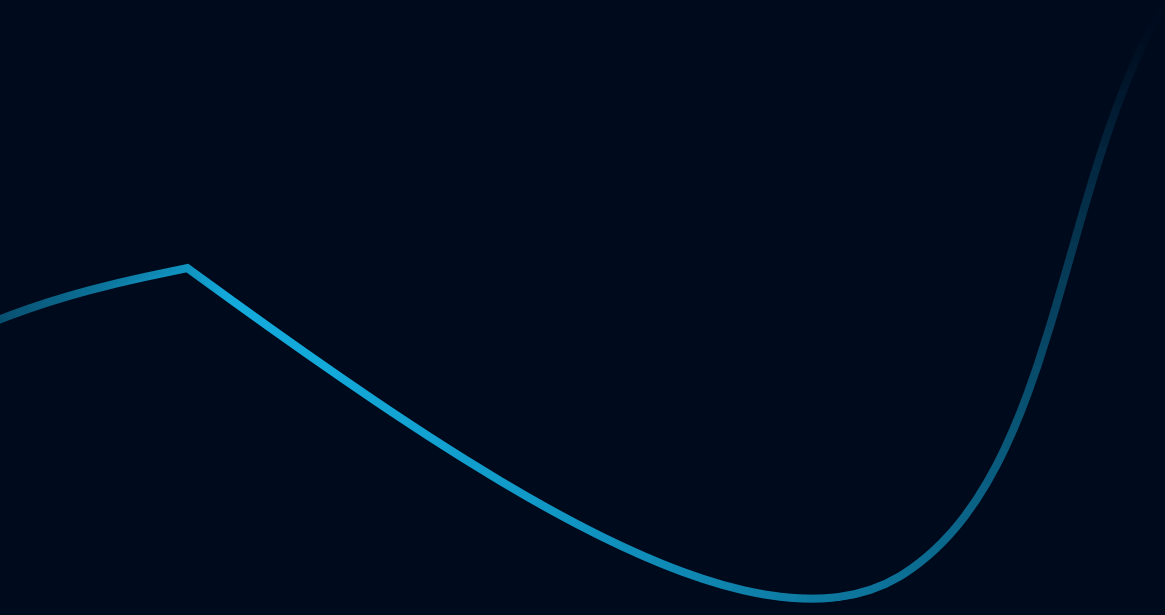
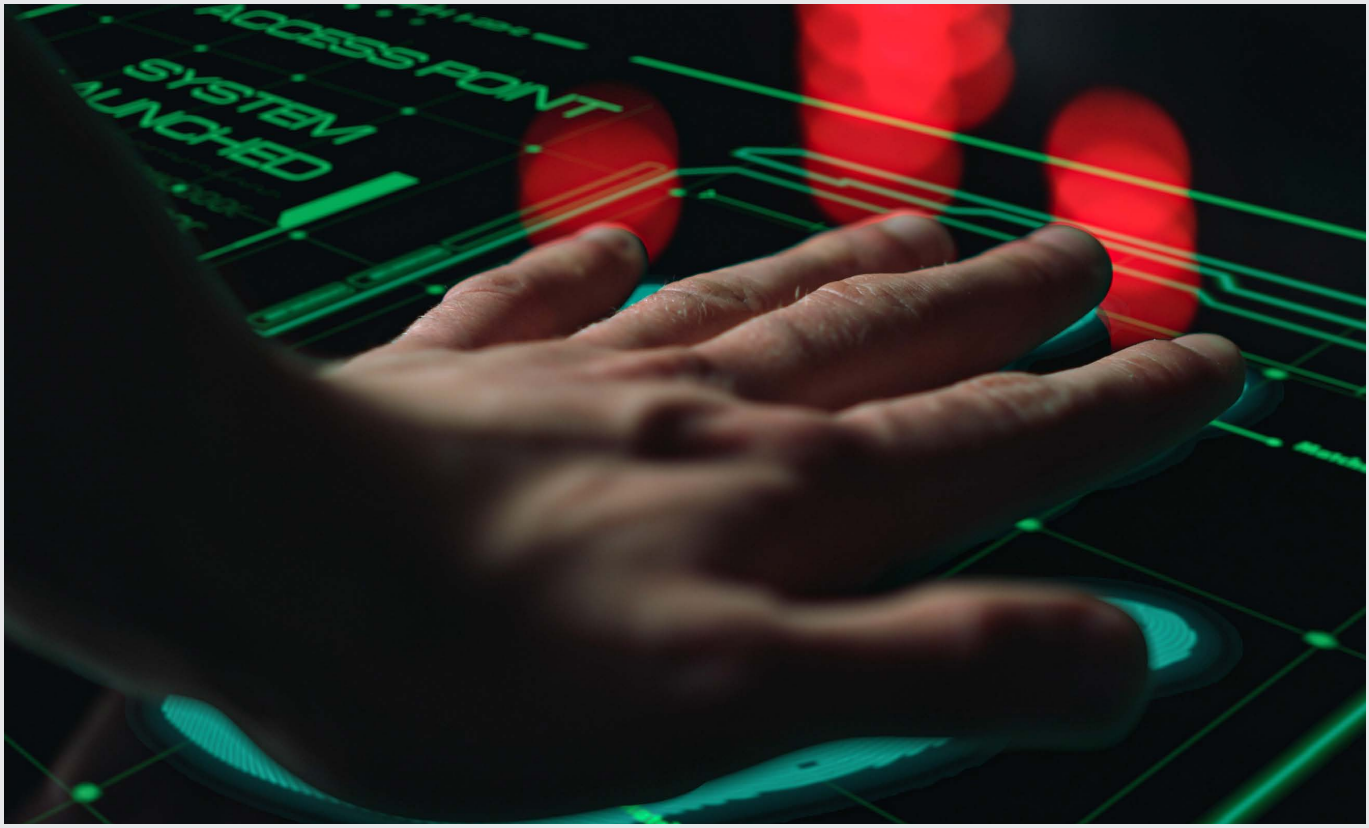
TRENDS IN CYBERSECURITY 2022

Secure an accelerated digital transformation

Capgemini



Trends in Cybersecurity 2022



Secure an accelerated digital transformation

Cybersecurity is a core business requirement, providing a secure foundation to transform your enterprise and support your business. How do you maintain oversight and control over your cyber risk program? How fast can you go back to business as usual when cybercrime hits your organization? And does your organization have a scalable approach to operating IT security?

Questions such as these are more relevant than ever. COVID-19 has permanently transformed the ways we do business and handle sensitive information. Technology and thought are changing rapidly; we now have to make sure these developments go hand in hand with a continuous focus on cybersecurity in all its guises. Current, unprecedented geopolitical developments make such a renewed focus even more critical.

Against this backdrop, we decided we needed a whole new trends report: Trends in Cybersecurity. This is the first edition. It contains the bundled expertise of our experts, tackling cybersecurity from all its viewpoints. Taken together, it serves as a body of insights that will hopefully help you give shape to your own cybersecurity strategies.

While writing the report, we were lucky enough to compare notes with Mauriche Kroos, Manager Information Security & Protection at Enexis. This management summary's short introduction of the contents of this report is accompanied by Mauriche's thoughts on the different topics we touch upon.

Perspective

To give you an idea of the scope of cybersecurity, we felt it would be a good idea to put it in perspective. Because you might be tempted to think of cybersecurity as an IT-issue, when in fact its impact is much broader than that. The opening article of this report attempts to paint this canvas, through an interview with TenneT's Associate Director of Safety and Security Gineke van Dijk. Her company's field of operation is where public sector, private sector, technological and geopolitical considerations meet.

Artificial Intelligence

With all the talk about AI nowadays, you might be tempted to think that AI's the answer to everything. Including every issue of cybersecurity you might think of. And as you'll read in our article, the uses of AI are many indeed. But its authors also have a word of caution: treat carefully. What are the basic considerations for any AI-driven approach? This article tells you all about it. In Mauriche Kroos' words: 'AI is very useful. For automation related tasks, for instance. And you can rest assured our adversaries are certainly trying to reap AI's benefits. This alone legitimizes investments in AI – we have to keep up with the bad guys. Along the way, though, we will have to find ways to deal with organizations' understandable reservations. And we'll have to find better ways to monitor AI's performance; it can be hard to find out whether our AI strategies are actually working as we intend them to.'

The business case for SOC

With a 50% increase of cyberattacks in 2021 compared to the year before, the business case for Security Operations Centers is basically writing itself. At the same time, SOCs are having a very hard time keeping up with threats, due to a shortage of skilled staffing. It's a paradoxical situation that urgently needs solutions. In the realization that labor market conditions aren't going to change any time soon, this article explains how we leverage technology to increase the effectiveness and scope of the Security Operations Center. Mauriche: 'It's highly probable that the implementation of an SOC will become a legal requirement for most companies, especially for those active in critical infrastructure. And rightly so. It should be a top priority for all of us; technology and the right processes and people to enable it, can help us make it happen.'

Cyber resilience as a continuous process

Cyber resilience is a team effort. And one that requires continuous attention. Technology alone doesn't cut it. In this article, the authors propose a way to organize and integrate cyber resilience, through three foundational principles: collaboration between your teams, judicious automation of tasks and processes and continuous improvement of your resilience

Tool complexity versus agility and vendor-independence

How quickly can your organization respond to outside threats? It all comes down to agility. And agility mostly isn't served by a complex IT landscape, consisting of many point solutions offered by different vendors. Such an IT landscape can be hard to manage, improve or adapt to newfound threats. A platform approach can be a good way to safeguard agility, integrating different process into a unified solution that is easy to manage or scale. On the other hand, best of breed solutions from beyond the platform can still be very useful. There are no easy answers, in other words, but this article still succeeds in providing some useful guidelines. Mauriche: 'These days, big vendors mostly compel us to purchase full-range capabilities, not point solutions. And of course this has big advantages. But on the other hand, tendering processes become more complex and more lengthy and expensive. Choosing a platform also means tying yourself to a single vendor, which is not always the best option from a client perspective. Integrating best of breed solutions becomes harder, as does retaining your independence. As always: buyers beware and your mileage may vary, YMMV!'

Organizing Information through Cyber Threat Intelligence

For companies, the question often is not if they will get hacked, the question is when. So when you're targeted, you'd better be prepared. And when the attack hits, do you know how to respond and stop it from happening again? In this article, the authors propose an analyst-centric methodology to prepare for and respond to cyber threats: Cyber Threat Intelligence. Through CTI, you can organize and secure an information position that allows you to stay on top of cybersecurity, and ahead of bad actors.

Dealing with ransomware: it's all about being prepared

Ransomware is one of today's most harmful types of cybercrime. In the first six months of 2021 alone, the world faced 304.7 million ransomware attacks; an increase of 150% compared to 2020. This article sheds light on some high profile, recent examples of ransomware – and the lessons that can be drawn from those incidents. Dealing with ransomware all comes down to preparation: with effective crisis management plants, a clear communication strategy and an organization-wide effort to educate and train your teams. And, just as importantly, you should come up with ways to keep the business running while all the lights go out.
Mauriche: 'It's not enough to simply recruit an army when someone declares war on you; you need to have that army in place in peacetime, too, and practice, practice, practice. It's the same with ransomware. Guidelines or strategies or scripts won't suffice. Companies need to regularly practice with all kinds of cybercrisis scenarios (including ransomware, data breaches and nation-state actor attacks), so that they are ready to deal with any situation.'

True security requires a new way of working

Start-ups, medium and large corporations have the same security challenges. They must react quickly against threats and known vulnerabilities in their solutions. Awareness of their landscape is paramount, and a complete overview of their environments and assets, threats and vulnerabilities, the resulting risks, and mitigation for each risk is a must-have. Full control is only possible by having the necessary processes in place; processes supported by technology for automated tooling within and outside the CI/CD pipeline. On top of that, companies must maintain a balance between standardization and flexibility. All in all, safeguarding a secure landscape may require a whole new way of working. A way of working that revolves around the right combination of people, processes, and technology.

SAP security should be approached as a cybersecurity issue

SAP's out-of-the-box cybersecurity capabilities primarily focus on identity and user account protection and data encryption. These key controls provide the first line of defense, but blind spots still exist. The average SAP landscape is vulnerable to advanced cyber threats – and such threats could potentially cause critical business disruption. Therefore, in a highly complex SAP environment, you should start approaching SAP security from a cybersecurity perspective. The SAP silo and cybersecurity silo should become as one. This article provides a detailed discussion of how you can realize this integration.

Navigating classified data in the public cloud

The Dutch public sector is making great strides in its public cloud journey. However, the ever-changing landscape of rules, legislation, and recent global developments can provide challenges, especially when it comes to processing state-secret classified data. This article gives an overview of recent developments, and indicates the limitations of public cloud when it comes to classified data. The public sector will soon have to make a choice: fully embrace public cloud, and accept the need for mitigating measures to counter its inherent vulnerabilities, or stick to private clouds that offer more security – but less opportunities to reap the potential benefits of cloud technology. Mauriche: 'We've been working with cloud native architecture since 2017. And it's been a good experience for us from a security perspective, providing us with the scalability we need, the cost advantages we seek and the time to market/time to change advantages we aim for. A chief piece of advice: don't become dependent on one single vendor.'

Securing business involvement in Zero Trust

Most of the time, Zero Trust is strictly regarded from a technology perspective. But this new standard for access management is far more than just an infrastructure challenge; it requires the involvement of the business to work as it's supposed to. Artificial Intelligence can help us to create policies for effective access control, but the access control decision itself should always be the business owner's prerogative. In the end, only the business has the knowledge and the (ethical) compass to make informed decisions. This is what Zero Trust allows us to realize: secure access through technology – with a human (and humane) touch. Mauriche: 'In applying Zero Trust, you should choose an integrated approach. A purely technological approach won't do. Business engagement is an essential part of its success.'

How automated cloud security can liberate the business

Moving workloads to the cloud at scale can enable new business models, shorter time-to-market, and more resource flexibility. It can also present unique challenges in being secure and compliant. Nevertheless, if automation is applied in cloud security, resources can be focused on innovation, business development, and growth without compromising data protection and control over information. This article goes over areas where automation can be applied and how to leverage automation to reduce risk and maintain a high-security posture.

Dennis de Geus,

Head of Cybersecurity,
Capgemini Netherlands

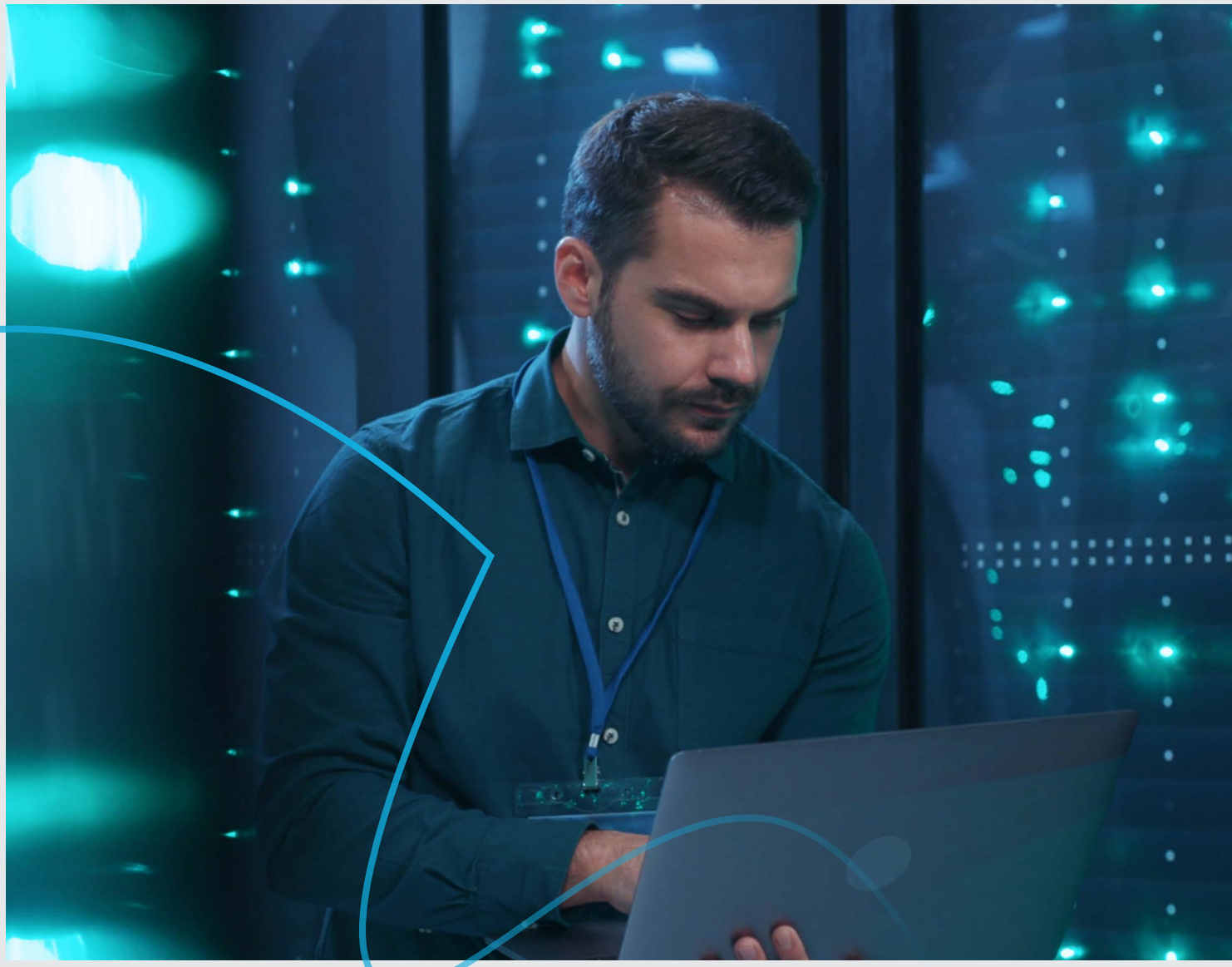
Mauriche Kroos,

GISO at Enexis

Content

Section	Title	Author	Page No.
	Secure an accelerated digital transformation	Dennis de Geus Mauriche Kroos	01
	The challenges of cybersecurity: a customer's perspective	Gineke van Dijk Dennis de Geus	06
Cloud			
	Data protection in the public cloud: a vision on the Dutch public sector	Manisha Ramsaran Ruben Tienhooven	10
Cyber Resilience			
	Combining colors and automation in IT security	Alex Verbiest	16
	Cyber resilience through platform-based approach, reducing tool clutter	Remco Vedder Jeroen van Hulst Sarah Dil Sebastiaan de Vries	21
	Cyber threat intelligence: painkiller or cure for cyber incident response?	Saskia Kuschke Erik van Dijk	27
	The ransomware epidemic and the importance of crisis management	Rachel Splinters Manouck Schotvanger Fokko Dijksterhuis	31
	SOAR - a technology to improve and speed up phising responses	Folkert Visser Stef Bisschop Sjra Maessen	35
Artificial Intelligence			
	The impact and considerations around AI-driven detection and response	Laura Adelaar Max Mol Niels den Otter Sebastiaan de Vries	40

Section	Title	Author	Page No.
Automation			
	Automation - a key component to secure cloud workloads at scale	Jean de Smidt Thijs Verkuijlen Rafik Nasiri	48
	Keeping your application landscape continually secure in a dynamically changing world	Barry Jones	54
	Securing the SAP landscape - Bridging Cybersecurity and SAP	Yogita Mahajan Rutuja Shedsale Ankit Arya Kriti Biswas Sagarika Ghosh	59
Zero Trust			
	Zero trust, a shift-up in security governance	Peter Hoogendoorn Paul Pelzer Jasper van den Vaart	66
	Publications		71



The challenges of cybersecurity: a customer's perspective

The fact that we're, for the first time, devoting an entire trend report to cybersecurity should tell you something: that cybersecurity is one of today's top priorities. Of course, this in itself won't come as a surprise, but what does surprise us all every now and again is the enormous impact cybersecurity can have on our organizations. Threat-wise, of course, but also from a threat-preventive perspective.

Traditionally, cybersecurity is regarded as an IT-focused field and is prioritized as such. At Capgemini, too, we come across many companies – both public and private - where cybersecurity is regarded as a technological issue. As a result, the significant impact a lack of security can have on the whole organization is often underestimated. As you'll read in the following, the true scope of cybersecurity goes far beyond just that of IT.

"There's always a risk of safety and security neglect, due to a lack of attention or prioritization. But on the other hand, there's also a risk of hasty, bad decision making, as a result of the increasing pressures and demands of the outside world. A lack of security costs money, but bad security also costs money. I have to make sure we keep on doing the right thing, at the right time. It's a responsibility we believe is or will be recognized by others with an end-responsibility for cybersecurity, especially in the critical infrastructure."

Energy transition

Current international developments once again show that cybersecurity must be a top priority. This is especially felt in the energy and utilities sector, where cybersecurity is an extra aspect to be addressed in already disruptive times. TenneT is a good example. As transmission system operator, the company is tasked with expanding the energy grid to support the energy transition, while making sure that services to current customers continue unimpeded. All against the backdrop of challenging geopolitical circumstances, increasingly strict rules, and regulations – and the company's own determination to do its part to safeguard the (cyber) security of its operations, that of the sector as a whole, the markets it operates in and the people it serves. We talk to TenneT's Director of Safety and Security and CISO Gineke van Dijk about the many ways cybersecurity impacts this crucial link in the electricity supply chain.

Heart

Operating at the heart of the energy transition, TenneT is a fundamental part of its success. The circumstances wherein TenneT is operating are evolving rapidly.
Gineke: 'Due to digitalization and geopolitical developments, the pressure on the transition process towards a CO2-neutral energy system is growing and its scope is increasing. We have to make sure that the energy system stays up, with 99,999% reliability – and at the same time, we have to transform and expand the energy grid rapidly. It's an enormous challenge. In the physical domain, but also in cybersecurity. Our sector has been on the radar of bad actors for quite some time.'

Holistic

Elsewhere in this report, the various technical aspects of cybersecurity enhancement are discussed. But that's not only what Gineke's role is about. She also has to make sure that cybersecurity remains a top priority from a more holistic viewpoint: "There's always a risk of safety and security neglect, due to a lack of attention or prioritization. But on the other hand, there's also a risk of hasty, bad decision making, as a result of the increasing pressures and demands of the outside world. A lack of security costs money, but bad security also costs money. I have to make sure we keep on doing the right thing, at the right time. It's a responsibility we believe is or will be recognized by others with an end-responsibility for cybersecurity, especially in the critical infrastructure."

Rules and regulations

Of course, doing the right thing in itself is not something that's under discussion. The company isn't blind to current developments, and well aware of its own role and responsibilities. But even if it wasn't, regulators would force the company to keep its eyes on the ball. Indeed, the European Union is currently in the process of implementing a whole range of new, or tightened, rules and regulations.
Gineke: 'One of the European Union's responses to increased cybersecurity threats is a new set of reinforced regulations. Through NIS2 and the Network Code on Cybersecurity, the EU is really tightening its policies. The energy sector is on a tight leash. And we should be.' At Capgemini, we expect this growth in regulatory requirements will drive a CISO's agenda for the coming period.

Scope

The Network Code on Cybersecurity contains rules on cybersecurity aspects of cross-border electricity flows. NIS2 is a revised version of the existing NIS Directive on Security of Network and Information Systems. One of the big changes is its increased scope. Before, it was aimed at large, essential companies such as power companies and water companies; NIS2 also applies to (smaller) companies that are part of the same value chains. As a consequence, Third Party Security Risk Management increasingly requires attention. Taken together, the new pieces of legislation have higher requirements regarding data protection, infrastructures, and information sharing, along with stricter monitoring (and more severe penalties) from the EU. Complying with these rules and regulations takes up even more valuable resources – a fact that's exacerbated by the bigger role of chain responsibility.

A company like TenneT can only ever be safe if it collaborates with and supports smaller chain partners with fewer resources. As always, the chain is only as strong as its weakest link. Gineke: 'The new legislation is Europe's response to the changing landscape. For TenneT, it's becoming more vital each day to avoid becoming dependent on undesirable third parties. Making sure of this entails closely working together with other companies, public organizations, and governments. And as NIS2 points out, we have to strengthen our information sharing and collaborative efforts with other essential companies and organizations, but also with parties beyond that scope that are part of the same ecosystem. Collaboration-wise, there's a lot of room for improvement. Public organizations and government departments can step up in aligning with each other, and with companies such as ours, and vice versa. And apart from this: it's really hard to find qualified personnel, across the board. So how do we realize our own security ambitions, and secure compliance with legislation, while the people we need are so hard to find? This is a big worry for us right now.'

So, on the one hand, the scope of cybersecurity is increasing. And on the other hand, the supply of qualified personnel is tight, and becoming tighter. Plus, with the new legislation, it's easy to lose oneself in monitoring and reporting requirements. But especially for an asset-heavy company such as TenneT, there's another aspect that requires attention: the physical supply chain. A wide range of technology can have an impact on the grid, including modern (IoT-) infrastructure such as charging stations operated by other companies. TenneT hardly has influence on these systems. And although most cyber attacks seem to happen on IT systems, OT systems are vulnerable to the same threats. Gineke: 'someone working in OT may find it hard to imagine that his asset's downtime is related to a cyber situation. Our cyber teams, then, should not only be in contact with each other, but also with OT colleagues, sharing knowledge and information. And everyone should be aware of the cybersecurity perspective. Cybersecurity has expanded far beyond the traditional IT domain.' At Capgemini, we believe that CISOs should be asking themselves questions such as: Do we have a clear insight into the cyber risks across our value chains? What does my cyber staffing plan look like, and how does it impact my decision to do activities ourselves or to engage partners for certain activities? Governments, departments, grid operators and other chain partners alike should realize that, when it comes to cybersecurity, we're in this together. And as far as Gineke's concerned, it is high time that everyone involved gets together to reflect on their shared responsibility: safeguarding the cybersecurity in Europe, in the Netherlands, in every company and every household: "currently, collaboration leaves a lot to be desired. Departments, public organizations, governments – there's a great deal of fragmentation. Effective information sharing between relevant parties isn't a given, and full compliance with new legislation will be a big challenge – especially for companies newly added to the scope. If we are to safeguard commodities such as electricity, now and in the future, we will have to work together every step of the way, under the clear prioritization and direction of our governments."

About the authors:

Gineke van Dijk
Director Safety & Security TenneT TSO BV

dennis.de.geus@capgemini.com

Dennis de Geus
Head of Cybersecurity Capgemini Nederland B.V.

01

CLOUD

Data protection in the public Cloud: a vision on the Dutch public sector

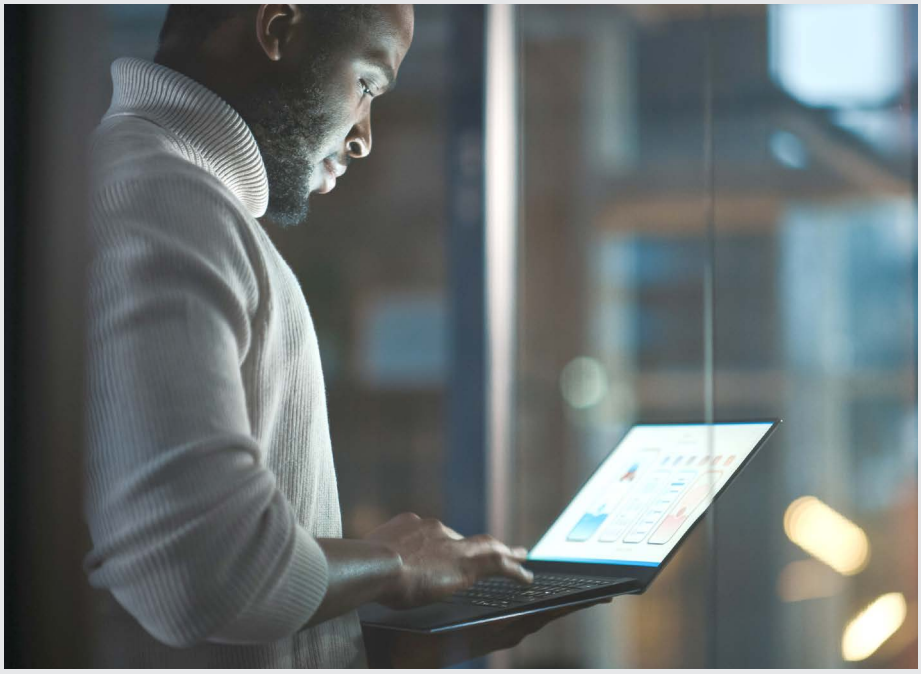
Highlights

- The public sector is increasingly embracing public cloud adoption.
- 2022 is a marking point.
- One of the biggest challenges is processing state secret classified data in the public cloud.
- There are several initiatives for European and national private cloud solutions.
- It is up to the Dutch public sector to decide what its future will look like.

01 Trends in Cybersecurity 2022

What are the most important data protection rules and developments regarding the use of public clouds for the Dutch public sector?

The Dutch public sector is making great steps in its public cloud journey. However, the ever-changing landscape of rules, legislation, and recent Mondial developments can provide challenges, especially when it comes to processing state-secret classified data in the public cloud. This article gives an overview of recent developments and provides insight into the data protection dilemma that the Dutch public sector currently faces: deciding to what extent its most sensitive data should be processed in the (public) cloud.



The big move towards the public cloud

In the coming years, most Dutch governmental organizations will fully embrace cloud services' adoption. A Gartner study shows that 63% of government cloud computing initiatives have succeeded over the past years[1]. Cloud services offer many valuable opportunities, from working (remotely) more efficiently to serving citizens optimally. Public sector organizations are increasingly opting for public cloud solutions. Public cloud 'hyperscalers' offer these solutions, such as Microsoft, Google, and Amazon, and offer great scalability/flexibility options to store and process data.
In general, processing data in the public cloud demands digital resilience more than the 'classic' on-premise concept. In all cases, (personal) data in the cloud must be handled securely and privacy-friendly, especially when it comes to sensitive data.

Because of several (political) developments over the years, the reluctance towards public cloud services gradually transitioned into its embrace by Dutch public sector organizations. Highlights include:

- In 2011, Minister Donner reported that only a small part of cloud service providers and offerings were on the right maturity level for the Dutch public sector[2]. The cloud applications existing at that time did not fully meet the specific wishes and data protection demands, for example, to store sensitive data.
- In 2019, an official advisory document about public cloud adoption was published[3]. This document explored the cloud policy of the Dutch public sector. It elaborated on data classification in the public cloud, stating that the use of the public cloud for data on the 'departmental confidential' level was not allowed unless specific conditions were met and that the processing of state secret classified data was not permitted.
- In 2019, 'Nationaal Bureau voor Verbindingsbeveiliging' (NBV) declined to confirm whether data processing in the public cloud could meet the conditions for data classification as 'departmental confidential'. However, in 2021, it changed its decision and advised that this data could be processed in the public cloud if several conditions were met to detect and prevent threats of state actors[4]. The processing of state secret classified data was still not permitted.
- In 2022, the Rijksoverheid will publish guidelines for the Dutch public sector to manage risks in relation to public cloud services. This clarifies the responsibilities regarding the adoption of data protection and security measures.

It can be concluded that the Dutch governmental organizations are offered more guidance and support to kickstart and continue their public cloud journey[5].

Overview privacy & security regulations

When processing data in the public cloud, various laws and regulations apply for the Dutch public sector at both national and European levels. This includes the following main regulations:

Data protection

In terms of data privacy, the General Data Protection Regulation ("GDPR") forms the baseline for protecting personal data in the public cloud. The GDPR is applicable to all governmental organizations within the European Economic Area (EEA) and describes the conditions for processing personal data and which criteria they must meet. It focuses on several privacy principles, such as limiting the processing of (sensitive) personal data and obligations in the context of data subject rights.

Information Security

In the field of Information Security, the Government Information Security Baseline ("BIO") is the most important framework. The BIO offers various measures, based on a risk-based approach, to ensure the security of information. For example, the BIO contains various measures for government agencies to maintain confidentiality, integrity, and availability of data. The BIO uses Basic Security Levels (BBN's) to keep risk management manageable, efficient, and transparent.

Depending on the BBN level, certain measures need to be implemented. See figure 1 for a complete overview.

Data	Authentication	Authorisation	Data Security	Public Cloud Storage
Publicly accessible information	None	None	Encrypted storage	**Possible**
Unclassified	Authentication ''low'eH2 / eIDAS: 'low'User-ID/ Password	Authorisation required (member of organization)	Encryption during transport outside the own network and encrypted storage of data. Manage own keys	**Possible with security measures BIO2020-BBN2**
Departmental confidential information Confidential	Authentication 'substantial'eH2 / eIDAS: 'substantial'2-factor authentication SMS/ token	Authorisation on specific role	Encryption during transport and storage. Manage own keys.	**Possible with security measures BIO2020-BBN2**
Personal data (processing standard personal data)	Authentication 'substantial'eH2 / eIDAS: 'substantial'2-factor authentication SMS/ token	Authorisation on specific role	Encryption during transport outside the own network and encrypted storage. Manage own keys.	**Consideration of type of application/system DPIA and security measures BIO2020-BBN2**
Personal data (processing special categories of personal data)	Authentication 'substantial'eH2 / eIDAS: 'substantial'2-factor authentication SMS/ token	Authorisation on specific role	Encryption during transport and storage. Manage own keys.	**Consideration of type of application/system DPIA and security measures BIO2020-BBN2**
Criminal and judicial (personal) data	Authentication 'high'eH2 / eIDAS: 'high'2-factor authenticationPhysical identification (passport, ID-card, issue reliable)	Authorisation on specific role	Encryption during transport and storage. Manage own keys.	**Consideration of type of application/system DPIA and security measures BIO2020-BBN2**
State secret confidential information	Authentication 'very high' Physical identification (passport, ID-card, issue physical)	Authorisation on 'need to know basis'	Encryption in transit and at intermediate stations via message security. Manage own keys. Minimise data transport. Only transport and storage in own network is permitted	**Not possible**

Figure 1: Overview of data classification, basic security levels and security measures in relation to data processing in a public cloud

Specific national rules and regulations

In addition to data protection and information security laws and regulations, governments are obliged to various other (legal) obligations. In practice, various laws impact the measures that governments should consider. For example, the Public Records Act ("Archiefwet"), Personal Records Database ("BRP"), Police Data Act ("WPG"), Government Information (Public Access) Act ("Wob"), etc.

Public organizations need to create a clear picture of the specific obligations that are relevant to them. The above laws are not an exhaustive list of all relevant laws and regulations.

State secret classified data and cloud computing

To fully reap the benefits of safely processing data in the public cloud, governmental organizations must align their data protection and security measures with the confidentiality level of the data. Currently, a lot is possible, except when it comes to processing state-secret classified data. As described above, it is not yet possible to process such data in a public cloud. State secret classified data can be defined as "official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated." Such data is not yet allowed in the public cloud, because active protection against state actors and organized crime cannot yet be sufficiently guaranteed. Special attention should be paid to Advanced Persistent Threats (APTs) - targeted cyberattacks in which a threat actor gains access to a network and remains undetected for an extended period of time. APTs are mainly conducted by state actors with political or economic motives, often aiming to steal state secret classified data or shut down (vital) networks at a certain point. This is the main reason for the Dutch public sector to be cautious with sensitive data processing in the public cloud; unlike private clouds, data is not under the full control of an EU member state itself. Therefore, how the Dutch public sector will process state secret classified data in a future-proof and secure way remains an important – and as yet unanswered - question.

The future of data protection in Europe – public or private clouds?

Since the legal basis for international data transfers between the EU and the US was suspended in the 'Schrems II' ruling of the European Court of Justice[6], there has been much uncertainty in the EU about the use of public cloud services for sensitive data processing activities. The 'hyperscalers' that currently provide cloud services to the Dutch public sector are all American organizations. The ruling stated that American legislation gives US intelligence agencies powers that are not compatible with the right to privacy of European residents, as described in the GDPR. As a result, EU member states were not only confronted with the information security risks associated with the powers of US intelligence agencies but also with compliance risks.

These additional risks intensified the discussions among EU member states as to whether they should better store sensitive data in 'sovereign' private clouds, as France[7] and Germany had already planned. In response, the American hyperscalers immediately developed cloud services to provide an answer to this data sovereignty issue, with which they claim to technically guarantee that (personal) data remains in Europe. Still, uncertainty remains among EU member states, with states questioning whether data sovereignty also implies sovereignty in the political sense; is the data truly European if an American organization is involved in these cloud processing activities?

Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.

The fear of losing full control of data processing activities has led to several European and national private cloud solutions initiatives[8]. Examples include the Capgemini initiative 'Blue'[9] for a private cloud in France and the European project 'Gaia-X'[10]. However, such initiatives are developing slowly compared to hyperscalers, and it has proven very difficult to match the quality of these US cloud services – including being innovative in information security and data protection. The above poses a dilemma for the public sector in The Netherlands and other EU members, where a choice must be made between:

- Using public clouds for sensitive data processing while increasing innovative capacity and accepting the additional sovereignty risks or;
- Using private clouds for sensitive data processing, embracing the (political) sovereignty to be completely independent but having less innovative capacity within the public sector.

Most Dutch governmental organizations will fully embrace cloud services' adoption in the coming years. The Dutch public sector can use public cloud services to process (personal) data up to classification level 'departmental confidential' but must use other means of processing for state secret classified data. Storing the most sensitive data in a public cloud comes with 'Advanced Persistent Threats' (APTs), which can pose a threat to national security. However, recent developments in the public cloud landscape might change this soon; public cloud providers seem to answer Europe's call for data sovereignty by building national infrastructures and giving governments almost full control of the data. Therefore, the Dutch public sector has a decision to make about the future of data processing: to either use innovative public clouds while embracing (mitigated) data and political sovereignty risks, or use private clouds that are less innovative but offer full sovereignty.

About the authors:

manisha.ramsaran@capgemini.com

Manisha Ramsaran

Manisha is a privacy consultant with profound experience with privacy & data protection related topics. Her law background and people-oriented focus make Manisha a dedicated sparring-partner with an eye for detail. She advices both public and private organizations with privacy-related matters.

ruben.tienhooven@capgemini.com

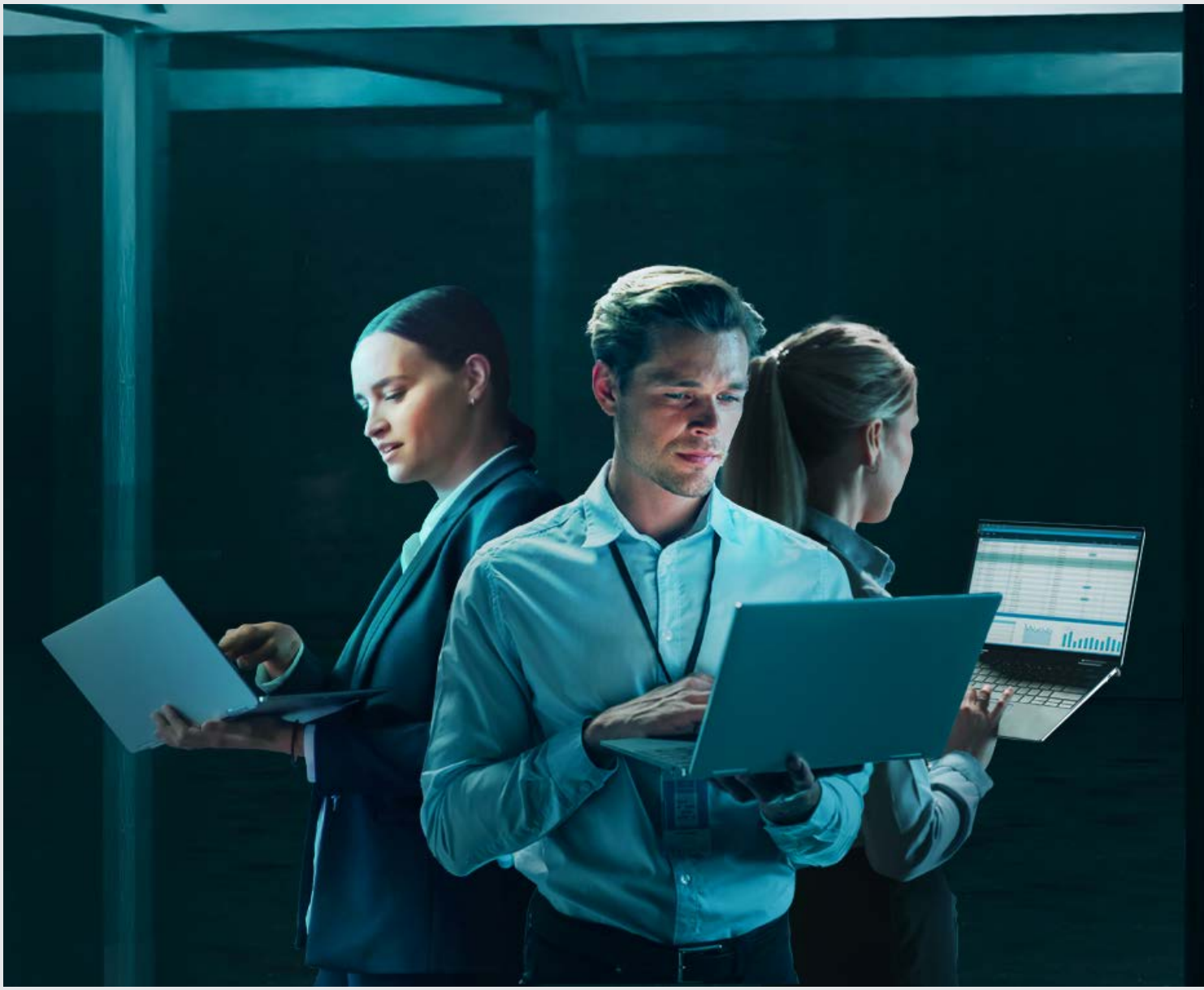
Ruben Tienhooven

Ruben is a senior data protection consultant with a focus on the protection of digital human rights and cloud computing. As a lawyer and IT specialist, Ruben knows how to bring both worlds of the cyber domain together.
In his work, Ruben knows how to translate requirements from legislation and regulations and the business into concrete actions and measures that can be implemented in practice.

1. https://www.gartner.com/smarterwithgartner/how-can-governments-scale-up-cloud-adoption
2. https://zoek.officielebekendmakingen.nl/kst-26643-179.html
3. https://www.noraonline.nl/wiki/BIO_Thema_Clouddiensten/Standpunt_AIVD_en_beleidsverkenning_BZK
4. https://www.noraonline.nl/wiki/BIO_Thema_Clouddiensten/Standpunt_AIVD_en_beleidsverkenning_BZK
5. https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2021/09/I-Strategie-Rijk.pdf
6. https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/
7. http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf https://www.bafin.de/EN/PublikationenDaten/Jahresbericht/Jahresbericht2017/Kapitel2/Kapitel2_7/Kapitel2_7_5/kapitel2_7_5_node_en.html
8. https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/
9. https://www.capgemini.com/news/capgemini-and-orange-announce-plan-to-create-bleu-a-company-to-provide-a-cloud-de-confiance-in-france/
10. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

02

CYBER RESILIENCE



Combining colors and automation in IT Security

02

Trends in Cybersecurity 2022

How can my organization build resilience against cyber-attacks, and who is responsible?

"Oh no, we have been hacked! How could this have happened?" – Every now and then, this question is asked by organizations that have fallen victim to cyber-attacks. Usually, this question is followed up by a second one; "Who within the organization is to blame?". Was it the Red Team for not finding the outdated software? Or was it the IT department for forgetting to place that "old system in the basement" on the inventory list? Perhaps both?

Highlights

- Resilience against cyber-attacks needs to be built and maintained.
- Welcome collaboration between your different teams.
- The “BAD” Pyramid.
- Use automation to support your resilience.
- Focus on continuous improvement.

Building your cyber resilience effectively yet efficiently asks for three things: collaboration between your teams, adding automation to the mix, and making it a continuous process.

There are different teams responsible for attacking (testing), defending, and building when it comes to IT security. The “Red” team focuses on attacking, the “Blue” team on defending, and the “Yellow” team on building. Each team has its own specific topic, yet they have a common goal: to build resilience against (cyber)attacks and safeguard business continuity. Building resilience against cyber-attacks is more than just keeping hackers out by performing penetration tests (performed by “Red” teams). It is safe to say that an attacker with sufficient time will be able to obtain access to your organization at one point. The question then is whether you will be able to respond properly to reduce the impact. A well-known concept called “Defense in depth” uses an approach of implementing multiple layers of defensive controls to protect assets. This is also applicable to the different teams; in case the Red team fails to discover a vulnerability in an application, the Blue team could still monitor the application for potential intrusions. If one layer fails, another one might still be able to protect the asset.

Combining various teams’ expertise and experience can help organizations to continuously train their teams and further strengthen their resilience to (cyber)attacks. A popular combination is called “Purple teaming”, combining the skills and expertise of the “Red” and “Blue” teams. The “Purple” team is not necessarily an actual (separate) physical team but is about combining (see fig. 1) the red and blue teams through collaboration. The “BAD Pyramid”[1] gives a good visual representation of the various colored teams and how they can interact with one another.[2]

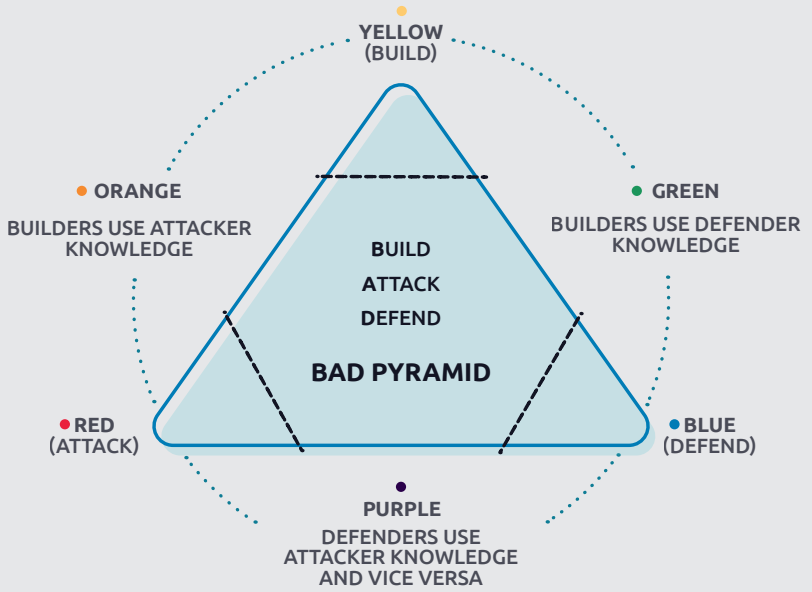


Figure 2: The Bad Pyramid
Daniel Miessler 2019Based on work by April Wright

A growing number of organizations already spent effort on “Purple Teaming” by collaborating on the prevention (e.g. penetration testing) and detection (e.g. SOC/SIEM) aspects. Some even bring in the Digital Forensics & Incident Response (DFIR) teams, which are sometimes also considered part of the “Blue team”. In the end, attacker and defender knowledge is valuable if you need to respond to an incident. However, it is less common for Red and Blue teams to collaborate with the “Yellow team”, which is responsible for the “building”-part.

When it comes to building systems or applications, having knowledge about offensive and defensive aspects in security is certainly valuable. The SecDevOps model[2] is a good example of this, as it weaves security into the entire development and deployment process. Keeping security in mind while building allows ‘Security by Design’, meaning that software and features have been designed to be foundationally secure. This generally results in solutions with fewer weaknesses to be fixed later. In addition, Security by Design lowers the costs for remediation as fixing issues in a later stage will generally take more time when compared to fixing them in the early stage. Other teams within the organization could also have a beneficial effect through collaboration. For example, organizations often have limited insight in (new) risks, such as newly found vulnerabilities in software. Collecting threat intelligence, which could also be performed by a completely different team, can provide organizations with valuable (new) insight into threat actors, techniques, tooling, and vulnerabilities, which can, in turn, support the other teams:

- Red team can perform new or refine attacks using the threat intel data.
- Blue team can improve their detection capabilities.
- Yellow team can implement (additional) security controls during the building process.
- Forensics & Incident Response team(s) can improve their incident response capabilities.

To defend against (cyber)attacks, you need to have insight into what needs protection. In other words, what does your infrastructure look like? What systems and applications do you have? Which data is stored where, and is that data of critical importance to the organization or not? Answering these questions will help determine what needs protection and what security level might be considered “sufficient”. This insight might not be readily available nor updated real-time. Especially highly dynamic organizations are facing infrastructure changes daily. The responsible IT department, which is (part of) the Yellow team, may not always be involved; more often than not, this results in an outdated overview of the infrastructure. Creating and maintaining an overview of the everchanging infrastructure aids in finding potential knowledge gaps within the teams when it comes to infrastructure visibility. How often do you hear about systems and applications that the internal IT department was not aware of? It is not difficult to imagine the security risks involved when this happens. The IT department has not included the system in their patch management process, and the Blue team is not monitoring the system. Perhaps even the Red team is unaware of its existence and thus has not tested (attacked) the system to identify potential vulnerabilities, leaving the organization vulnerable to (cyber) attacks.

Improving collaboration with automation

While creating an inventory of the infrastructure can be done manually, automation, such as ASM (Attack Surface Management) solutions, can be a supportive factor in this matter. These solutions continuously map your organization's infrastructure, including domains and networks, and provide an external attacker's perspective of the organization's attack surface. Looking at the bigger picture, automation can be used for many other purposes as well. Various tasks performed by the different teams could be automated, whether through simple scripts, small applications, or even through the introduction of machine learning (ML) and artificial intelligence (AI). For example, during penetration testing engagements, certain tasks are often performed multiple times, and manually. Such penetration testing tasks include enumerating systems and applications, abusing publicly known vulnerabilities with readily available exploit code, and abusing harvested credentials. By automating these tasks, the Red Team can focus on the more complex tasks and improve the efficiency and quality of the assessment. For example, implementing a Continuous Automated Red Teaming (CART) solution can help building resilience by continuously training your teams; (automatically) find weaknesses, actively exploit them, and further develop your detection and response capabilities/skills as these attacks are performed by simulating threat actors. Having the Red team actively exploiting weaknesses and using new techniques and tooling can also benefit other teams. The assessment details can assist the Blue team in improving their detection capabilities, such as by writing new detection rules. The process could also be automated so that the Red Team's attack details are sent to the Blue team, and that new rule sets are created and tested automatically.

Another example is fully automating the process of mapping your organization's infrastructure and Active Directory environment to take place continuously. These results can then be linked to fresh threat intel data, allowing you to identify new risks more quickly. Using automated tooling to crawl the (dark) web, collecting leaked credentials and mapping them automatically to enabled accounts from your Active Directory environment, and even resetting the password automatically, allows a fully automated detection and response process based on threat intel data.

Automation also helps during the development phase. A Secure Development Life Cycle (SDLC) is a development process integrating security throughout all its phases. This lifecycle supports the Yellow team in guaranteeing the solution's safety during each development phase. This includes determining the security impact of a new feature in the design phase, peer-reviewing code, and performing (automated) tests in order to identify vulnerabilities. Tooling can assist developers to identify vulnerabilities in their code real-time, for example, through plugins within their development environment. Another example of automation is Static Application Security Testing (SAST) tooling. These tools analyze source code or compiled code to identify security flaws. Using solutions like these can save time and effort, especially when compared to finding vulnerabilities in a later development stage. SAST tooling may not only help to identify vulnerabilities but also offer specific solutions for vulnerability remediation. New developments on the "Red" and "Blue" sides can be helpful to improve the tooling even further. It is safe to say that automation and the knowledge of both the Red and Blue teams are valuable for the Yellow team.

Resilience is built together

The key words for taking the next steps in building resilience are "collaboration", "continuous" and "automated". The necessary skillsets and processes need to be in place between the teams to continuously improve the organization's resilience against cyber-attacks. Effective collaboration between the different colored teams and automating as much as possible, can help organizations improve their resilience continuously while remaining time and cost-efficient. Because of the way resilience works, it might not be so easy to answer the question who or what is responsible for preventing an incident. An incident is often the result of several things that went wrong. In the end, everyone is responsible for your organizations' resilience. The rapid progress in (security) technology asks organizations to explore collaborations and keep themselves up to date, in order to identify new opportunities for improving the organization's resilience. The world and technology are changing rapidly, and (security) organizations should change accordingly.

About the author:

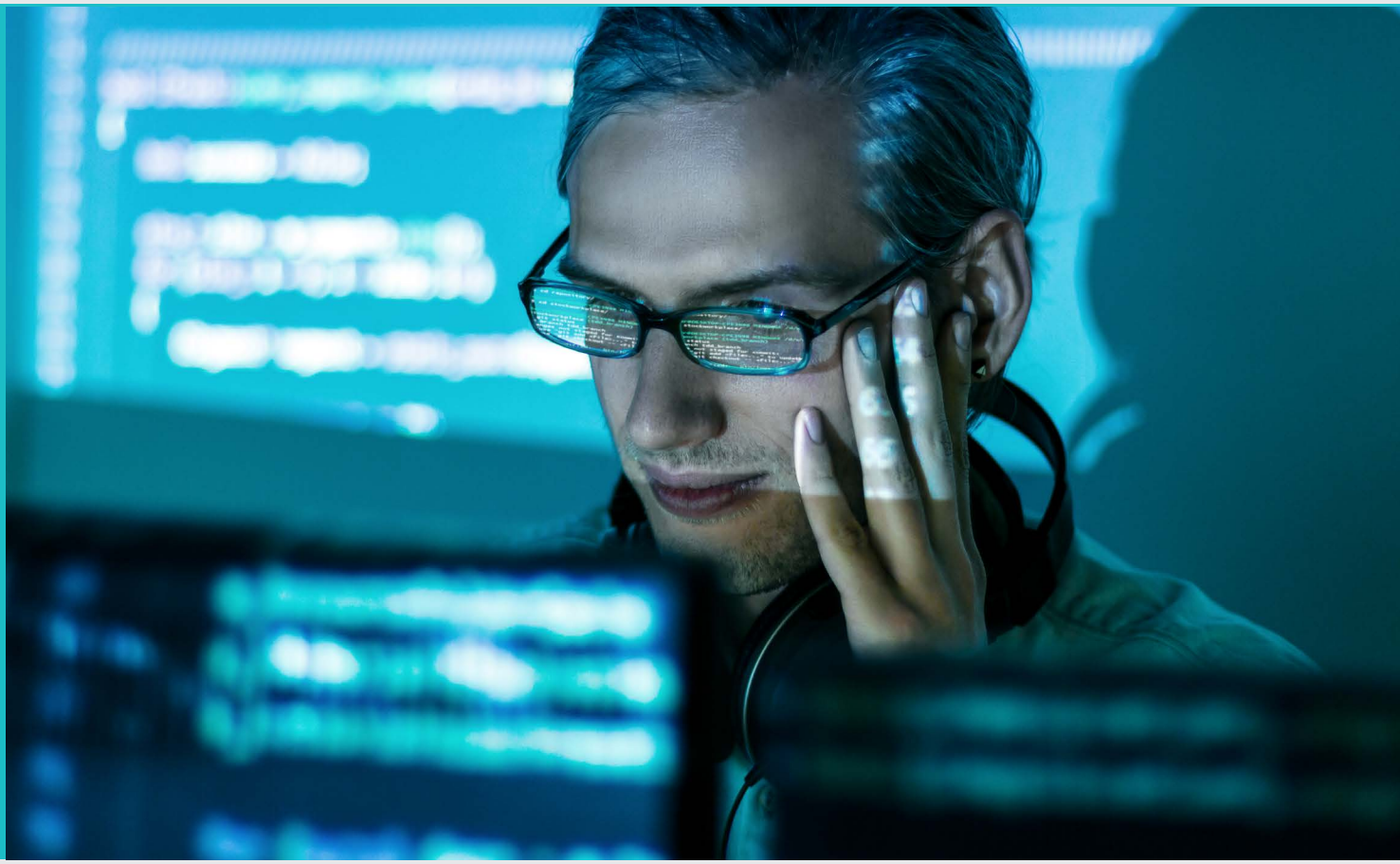
alex.verbiest@capgemini.com

Alex Verbiest

Alex is a cybersecurity consultant and ethical hacker with over 15 years of experience in the field of penetration testing and Red Teaming. He performs a wide variety of security assessments, both technical and non-technical, and leads a team of ethical hackers at Capgemini Netherlands.

1. https://danielmiessler.com/images/BAD-pyramid-miessler.png
2. https://www.capgemini.com/resources/secdevops/#:~:text=I'm%20delighted%20today%20to,processes%2C%20which%20DevOps%20makes%20possible

Cyber resilience through platform-based approach, reducing tool clutter



Every organization needs tools to support its business, but when every tool creates a new dependency, you lose the ability to adapt your landscape as needed. This loss of resilience results in lost business opportunities and increased security risk. So how do we escape this forest of tool clutter?

A new tool is brought to market every day, be it for patching, endpoint protection, or executive dashboarding. Today's tool landscape is as diverse as it has ever been. There is, however, a downside to all this diversity: increasing complexity, which reduces agility.

Agility is a measurement of how efficiently an organization's IT infrastructure can respond to external stimuli. If every new tool requires its own infrastructure, every infrastructure requires a team, and every team has its own wants and needs. The result is an IT landscape that is increasingly hard to adapt to new business requirements. So how can we reduce this tool clutter without losing much-needed capability?

Highlights.

- How tool clutter impacts your IT landscape.
- How AI impacts detection and response efforts.
- Specific considerations around dealing with false positives .
- The role of the SOC in AI-driven detection and response.
- How to find the right strategy for your organization.

Starting at the problem: the impact of tool clutter

With the need for capability growing, organizations implement more tools to help drive business processes, either to automate or improve their organization. This desire makes it highly enticing to implement a new tool for every challenge. Especially with organizations like Gartner mapping out the current offerings of "best of breed" tools – that is, tools that are the best at offering a specialized functionality.

However, while it sounds great to possess a proverbial trunk full of silver bullets, in practice you're going to need an even bigger trunk to keep everything organized. This lack of operational control makes the IT landscape harder to manage and can increase your organizations' security risk.

Collaborating between tool teams requires adequate translation of tool output and terminology. Information can get lost in translation, resulting in long and arduous discussions on what the actual state of the environment is. Making changes becomes complex because more and more stakeholders need to be involved, reducing the speed at which change can be adopted in the environment.

Therein lie the two main challenges in managing a tool-rich environment; information uniformity and tool alignment. Both are foundational elements of operational resilience, as an organization cannot adapt to change without them (see figure 3).

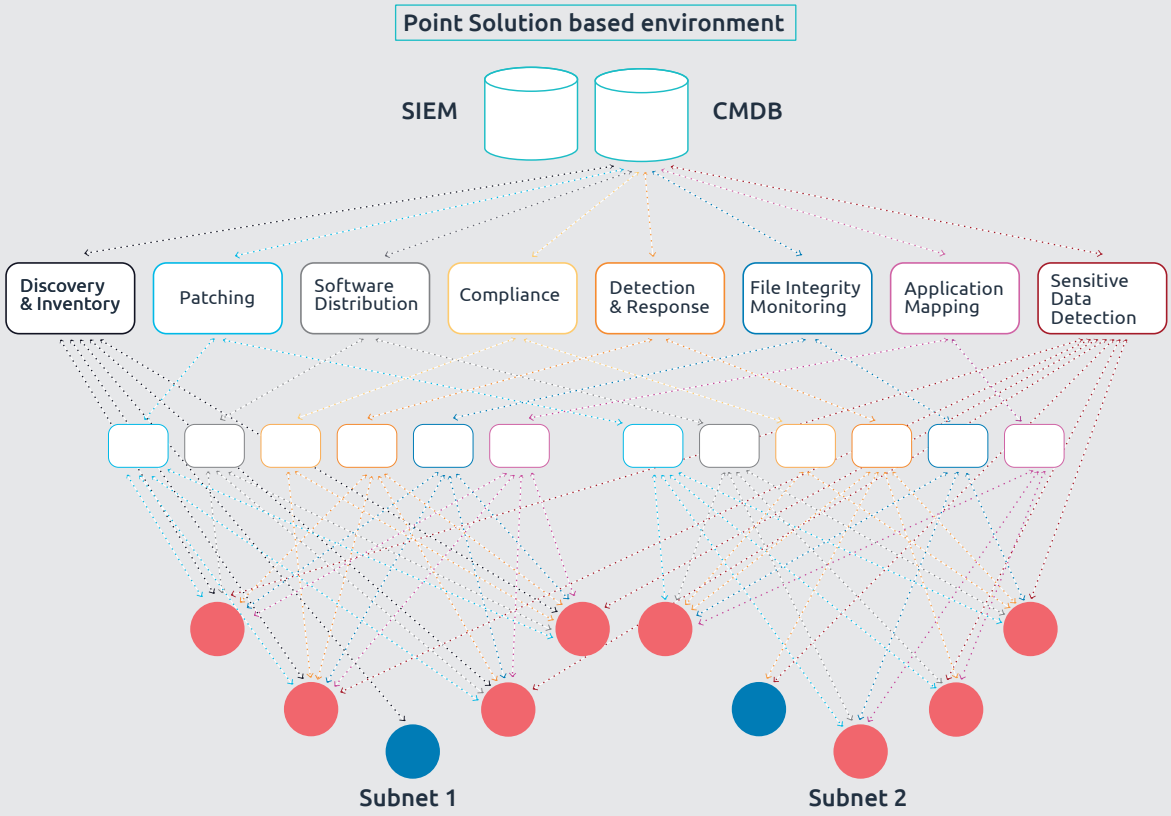
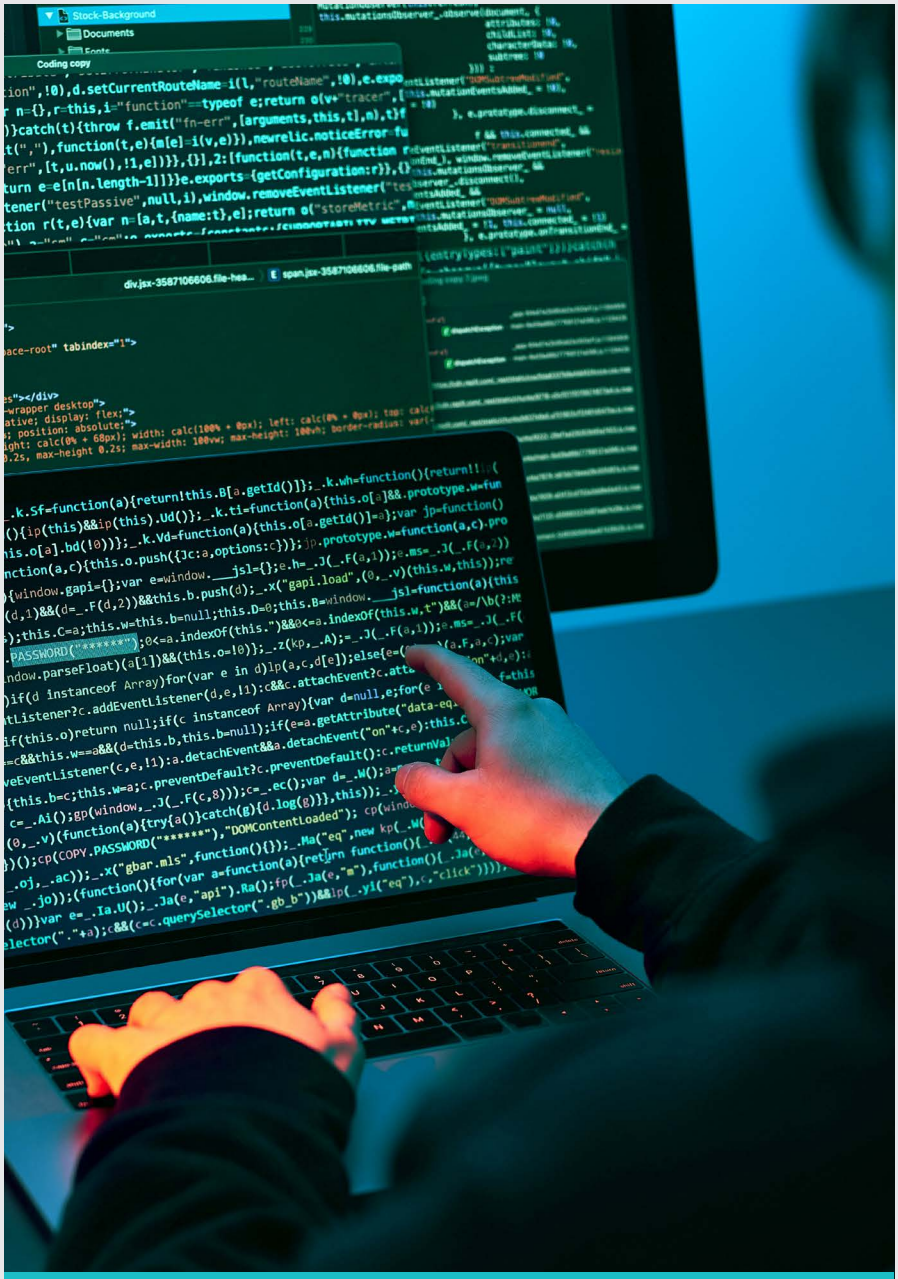


Figure 3: Point Solution based environment



Being able to make reliable decisions within IT requires reliable insight. Insight that is trustworthy, accurate, and complete.

Enhancing operational resilience

Being able to make reliable decisions within IT requires reliable insight. Insight that is trustworthy, accurate, and complete. If you don't have the whole truth, your decisions will be sub-optimal at best.

This is where most companies look towards a 'single source of truth' (SSOT). SSOT aims to provide central oversight and management of all data; it is the practice of structuring information models and associated data schema so that every data element is mastered (or edited) in only one place. This provides you with a single dashboard from which to govern your environment and all the tools therein. The SSOT approach resolves the challenge of information uniformity and provides you with an accurate picture of the status of your IT environment.

The challenge of tool alignment remains. Even with an SSOT approach, the problem persists; a disconnect between the requirements of senior management and those of IT management. While all data might be available from a single pane of glass, action must still be taken through different tools with different requirements. That translation from "big picture" to "key actions" is where things go wrong, where oversight gets lost, and where interoperability issues suddenly arise.

While there are many solutions to this challenge, not all are equally scalable or future-proof. This brings us to this article's key topic: the platform-based approach.

Platform-based approach

Opposite the point-solution approach on the tool spectrum is the platform approach (see figure 4). Where point-based solutions focus on being the best they can be in one specific area like vulnerability scanning, platform-based tools focus on the integrated capability to enable end-to-end delivery within a specific IT domain such as vulnerability management (i.e., vulnerability scanning, risk classification, and vulnerability remediation).

One argument for implementing a platform-based solution is the central management of important business processes. Ultimately, the technology an organization uses should support, and be supported by, clearly defined processes and actions. How do we store data? When do we patch? How do we act on security incidents? While there might be point solutions with more in-depth functionality, platforms generally score better on integrating all different functionalities so as to manage business processes centrally (which can be crucial in getting the most out of your tool).

Using one platform centrally incentivizes looking at these interrelated processes from a holistic viewpoint. This holistic view tackles our first challenge; information uniformity. With all teams utilizing the same data source, you inherently create a SSOT.

This ties in with the second benefit of platforms; improved cyber resilience through reduced tool clutter. The clarity of central management from a platform makes it easier to turn management oversight into effective action simply because management and operations are looking at the same data. In short; SSOT by design.

This design enables for easier alignment between different stakeholders as the same stake on the technology layer is now shared. All players will want the same platform to be well-maintained and properly deployed, as this directly impacts their own operations. With this SSOT by design, we resolved our second fundamental challenge; tool alignment.

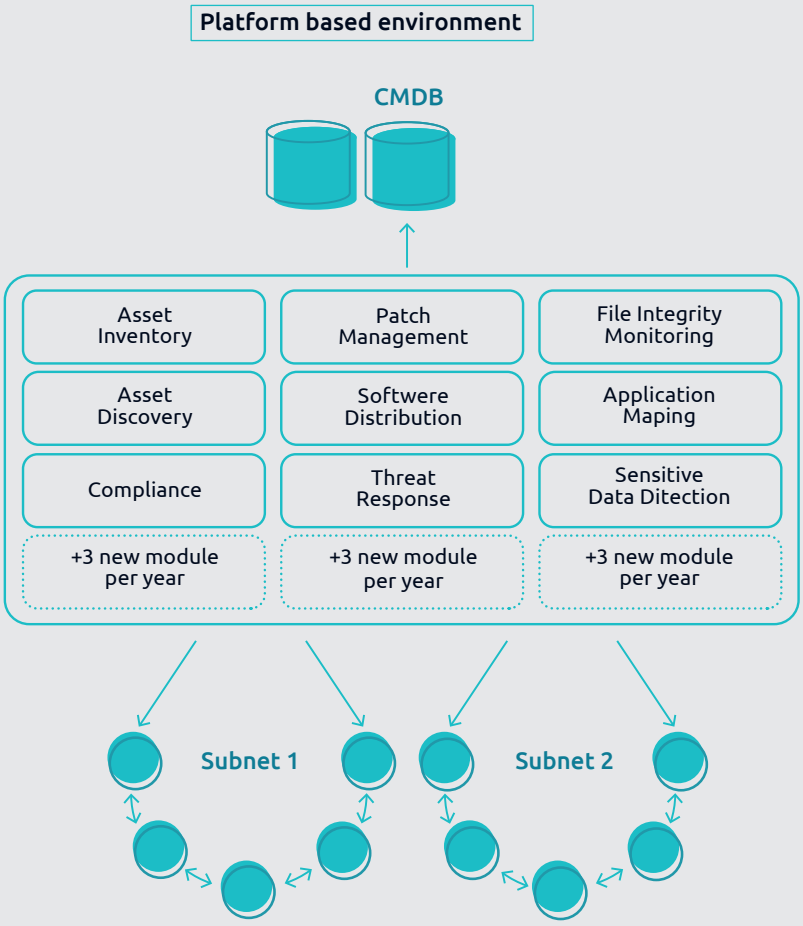


Figure 4: Platform based approach

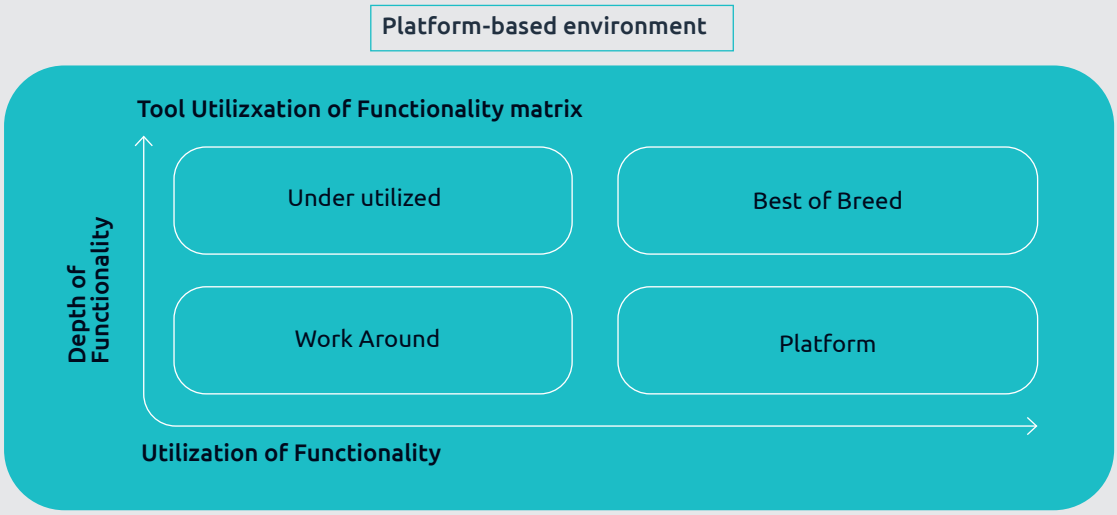


Figure 5: Platform-based environment

A pinch of salt

While in a binary comparison, it seems that a platform-based approach should be the universal standard, the reality is, as always, a spectrum. In reality, there is no single platform-based tool that can deliver every capability needed by an organization; even if there was, there would still be areas where the platform simply cannot compete with best-of-breed tooling.

This brings us to the main consideration of the platform-based approach. Where best-of-breed tools focus on one task and a platform focuses on many, sometimes you need more advanced capabilities to address the specific needs of your environment. Whether this applies to your environment or not, depends on whether the added functionality offered by a best-of-breed tool would be utilized to its full potential. While you don't need a trunk full of silver bullets, sometimes it's good to bring a little bit of kryptonite if the situation demands it.(see figure 5)

Strategic considerations

While different tools use different approaches, some general considerations hold true across all tool types.

Resilience knows many forms but generally pairs closely with functionality. If there is a need to change the existing tool for patching on a platform that also provides asset management, vulnerability scanning, threat hunting, and software deployment functionality, one may encounter interoperability difficulties. How do we swap out just one feature of a platform without losing our tool alignment?

This is an obvious challenge for the functionality of platform-based tools, but this same challenge exists at the process level with point-based solutions. How do we change a specific tool without impacting our information uniformity? This raises the question; where do you need the most resilience?

In general, we tend to prefer a combination of high tool alignment (making sure the capability never falters and teams keep working together) and just the right amount of functionality (why maintain data that you're never going to use?). But the final piece of the strategic puzzle is one we've not fully addressed, namely the question of capability requirements.

Capability requirements

In most cases, acquiring a new tool starts with a need for a specific capability. For example, the need to take stock of vulnerabilities or the need to deploy patches automatically. These requirements are generally not open for debate within the security world. If a need for more insight into security events is determined, there is usually good cause for it.

To compare the weight of these requirements with the need for information uniformity and tool alignment, you will need to start by quantifying the need behind the requirement. When we quantify these requirements, we can decide what it is we truly need. Do we need the in-depth, best-of-breed capability, or do we need to enhance our cyber resilience through information uniformity and tool alignment?

This question will require attention every time a need for a new tool or functionality is identified, so it is recommended to take the time to define a strategy around it.

Where to start

Starting with the transformation of an infrastructure cluttered with tools to a more manageable situation requires a structured approach. A clear vision and plan are needed to achieve the goals of the organization. Without this vision, the result will not be optimal for the organization and will not match the desired goals. While defining this vision, all parties should be involved to achieve the most valuable platform for your organization.

Next to a vision, it is important to get a clear overview of the current situation and tools that are in place. With this overview, you can identify and locate the weaknesses and strengths of your infrastructure. This will show where your infrastructure can be optimized. While doing this, make sure you create a diagram and not only a list. In this way, you can directly see where the tool clutters are in your infrastructure.

About the authors:

remco.vedder@capgemini.com

Remco Vedder

Remco Vedder is a cybersecurity consultant with knowledge and experience in the field of vulnerability assessments, offensive security and Endpoint Detection and Response Services. Currently, Remco is the Technical Lead for the Tanium Team and works for different Capgemini clients.

jeroen.van.hulst@capgemini.com

Jeroen van Hulst

Jeroen van Hulst is working for almost 3 years at Capgemini. He has a technical background and is currently working and specializing in Endpoint Detection and Response services. For this EDR service he operates as a team lead and SME for different clients and internal teams.

sarah.dil@capgemini.com

Sarah Dil

Sarah is a medior Security engineer focused on helping clients get the most of out their security tools. Working with Security Platforms like Tanium, she has in depth knowledge on a wide range of topics such as Software deployment, Patch management and Security Management.

sebastiaan.de.vries@capgemini.com

Sebastiaan de Vries

Sebastiaan de Vries is an experienced cybersecurity consultant specialized in XDR Services. Combining both technical and procedural expertise to bring his clients strong security solutions that drive effective business descision making while keeping the landscape secure.

Cyber threat intelligence: painkiller or cure for cyber incident response?

How does cyber threat intelligence benefit the cyber incident response process?

In the cybersecurity community, it is a generally accepted fact that a cyber-attack hitting an organization is a matter of when, not if. Entire fields and industries have built their livelihoods and capability around this one simple fact: when a cyber incident hits, what then? How do we investigate, communicate, remediate, and – most importantly – how can we stop it from happening again?

Highlights

- CTI is the business of understanding an adversary's capability, intent, and opportunity in relation to yourself.
- Every phase in cyber incident response can be supported by CTI.
- CTI should be applied holistically by considering tactical, operational, and strategic intelligence.
- CTI can be thought of as a form of preventive medicine - a proactive form of defense.
- Know thyself: CTI is a powerful tool when getting to know yourself as well as your adversary.

Cyber threat intelligence (CTI) is an analyst-centric methodology combined with innovative tooling for detection of and response to threats. At its core, CTI is the business of understanding an adversarys' capability, intent, and opportunity – what do threat actors want, and what is the myriad of tactics, techniques, and procedures (TTPs) they use to get it? Often, however, the challenge lies in understanding how CTI can be consumed in a way that truly benefits an organization; the threat intelligence has to be actionable for an organization. Is CTI the crystal ball that can tell you where an attack will happen before it happens or is it a feed of indicators of compromise (IOCs) that helps your security tooling detect threats that have already penetrated your infrastructure?

CTI can be categorized into tactical, operational, and strategic intelligence. Understanding these different categories and their intended audiences is key to understanding how CTI can benefit cyber incident response (IR) and beyond. Tactical threat intelligence is the most technical of the types and is often machine-readable – for example, these can be the IOCs that can be used to automate the detection of "known-bad" IP addresses, file hashes, URLs and so on. Operational intelligence takes a "big picture" stance, focusing on the threat actor's behavior and the full spectrum of operations. Understanding the modus operandi demonstrated by a threat actor in the past gives us a better chance of predicting their behavior and response in the future. Finally, there is strategic intelligence, which is focused on assisting leadership in decision-making when it comes to the organization's direction – it is intelligence that assists when considering risk management, business strategy, resource allocation, and budget prioritization.

For immediate IR, tactical and operational intelligence is the most applicable, whereas strategic intelligence plays a role in the long-term governance and decision-making around how cyber incident response is handled. In incident response, the National Institute of Standards and Technology (NIST) defines four phases of activities: preparation, detection & analysis, containment, eradication and recovery, and post-event activity (see figure 6). Let us examine how CTI can support each of these phases.

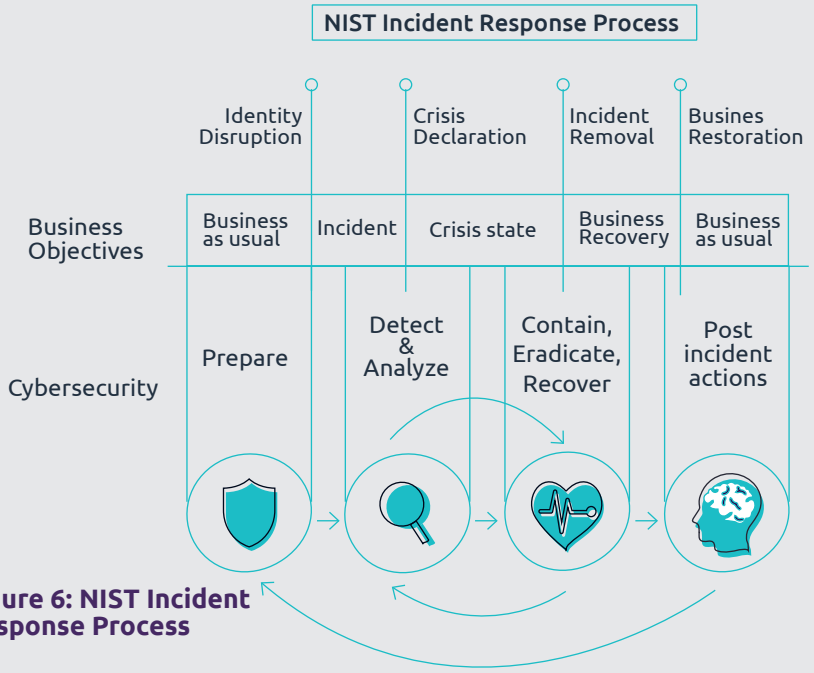


Figure 6: NIST Incident Response Process

Cyber threat intelligence (CTI) is an analyst-centric methodology combined with innovative tooling for detecting and responding to threats.

Imagine a grizzled detective is sent into the streets of Amsterdam. She has been tasked with catching a thief. Hopefully, prior to the thief burglarizing all of Amsterdam, preparation was carried out to ensure that the officer had all she needed to perform her duty to the greatest effect – a patrol car, a working radio, the correct training, and so on. In cyber incident response, this has generally involved having the telemetry, tools, and a trained team to investigate and respond to cyber incidents before the incident happens. In this phase, strategic and operational CTI is most useful in directing how the IR team prepares - for example, a general increase in Emotet-related incidents tells us we should especially be on the lookout for Emotet IOCs. This is a way for the IR team to ensure that they are trained to handle the latest and greatest and get to know their potential adversaries before facing them. In our detective analogy, this is equivalent to our detective having been briefed on the thief's regular hangouts and how they've historically been orchestrating their break-ins. She knows where to start looking for clues looking now.

Next comes the detection and analysis phase – or finding and investigating. Our detective has been dropped into the whole of Amsterdam, but luckily the intelligence from the previous phase has told her which borough she can start her investigation. A large focus of IR teams/investigators is on understanding how the threat actor thinks. The Cyber Kill Chain[1] is perhaps the most famous model used in CTI to illustrate the progression of a threat actor's campaign, and it is useful for the IR team to investigate with this picture in mind as well. In addition, tactical intelligence related to the threat actor's infrastructure (known command-and-control IP addresses or URLs in use by the threat actor, for example) and operational intelligence (e.g., this threat actor may prefer to use living-off-the-land techniques as opposed to prepackaged executables) provides additional sources of information to focus the direction of the investigation. This leads to a reduction in investigation time in a situation where every second counts. In other words, the detective knows from the provided intelligence exactly which types of tools the thief uses to conduct his break-ins – she also knows he prefers to break in through a window rather than the door, so she'll start investigating and collecting evidence there first to create a complete reconstruction of what happened and what was stolen.

Now that we understand exactly how the thief operates, we can contain them. The containment, remediation, and recovery phases kick the threat actor out of your infrastructure, fix what has been broken, and then return to business as usual. An important aspect of this activity is understanding the threat actor's behavior and how they may respond when they see defenders reacting to their presence, which can typically be gleaned from operational intelligence regarding this actor's TTPs. The detective knows how to approach detaining the thief – she expects him to react a certain way, which means there is a better chance of ensuring he (or his colleagues) does not come back to finish the job.

Finally, we have the post-event activity – a collection of activities centered around finalizing reporting, debriefing, and "lessons learned" exercises. This phase is dedicated to the wrap-up of the incident and works towards the improvement of the next response and prevention of this type of incident altogether in the future. All of the evidence (IOCs, malware samples, and more) collected during the previous phases and observations about the threat actor's TTPs can be aggregated and captured to improve future investigations. In addition, this intelligence (tactical and operational) can be fed into existing security monitoring solutions and threat hunt scenario development in a proactive approach to prevent future incidents of a similar nature.

It is tempting to distill a complex topic such as the consumption of CTI into simple terms such as “painkiller” or “cure”. CTI, in its tactical form alone, the use of IOCs for blocking and detecting attacks based on frequently changing technical information, for example, may seem more like a band-aid: temporary relief for a bigger problem. However, taking this type of CTI combined with operational and strategic intelligence provides a more holistic approach to investigating incidents and reducing the overall impact. Is CTI the “cure” to preventing any and all cyber incidents directed at an organization? Not quite – CTI is only as good as its audience’s requirements and understanding of its internal infrastructure. After all, you can only defend what you know you have and when you understand where your weaknesses and crown jewels are located. CTI is not a crystal ball: ultimately, it is a human-driven process, and much like traditional threat intelligence, humans miss things.

As such, the way to think about cyber threat intelligence is more like preventive medicine – a solid collection of routines and measures to reduce the risk of disaster and lessen the impact when illness does strike. A mature CTI program can give you some idea of what to expect in advance; which threat actors may be interested in you specifically? What malware do they like? What is the hottest flavor of exploit targeting certain vulnerabilities for this month? And then, when you do have an incident on your hands, your information position is better than what you otherwise would have had. When your investigators start piecing together the puzzle of how the intrusion occurred, they have a wealth of information at their disposal that allows them to pinpoint the attack vector (and perhaps even the culprit) more quickly, which reduces the dwell time of the threat actor in your environment in turn.

In the increasingly frenzied cyberspace arms race between threat actors and defenders, a good information position is more critical than ever. Cyber threat intelligence is the next step in ensuring that your organization – including executive leadership, the incident response team, security operations, all the way down to the end-user – stays on top of the game when it comes to being informed. After all, long before the advent of computers, Sun Tzu said it best: “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

1. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

About the authors:

erik.dijk@capgemini.com

Erik van Dijk

Erik is a Cyber Threat Intelligence consultant with ten years of military intelligence experience. He is leading and developing the CTI-team for Capgemini's Cybersecurity Unit in the Netherlands. Erik his focus is on the quality of the intelligence products and he is specialized in strategic intelligence.

saskia.kuschke@capgemini.com

Saskia Kuschke

Saskia Kuschke is a SANS-trained digital forensics and incident response analyst with experience in cybercrime investigation and incident handling. Saskia is part of Capgemini's ATHIR (Advanced Threat Hunting and Incident Response) team, working to build up incident response services capable of tackling enterprise-level cybersecurity incidents at scale.

The ransomware epidemic and the importance of crisis management

How to make an organization more resilient against a ransomware crisis?

During the first six months of 2021, the world faced 304.7 million ransomware attacks. With an increase of 150 percent of ransomware attacks in comparison to 2020, we can truly speak of a ransomware pandemic. Does your organization know how to respond when disaster strikes?

Highlights

- A dedicated cyber crisis management team is important.
- Incorporate a ransomware scenario in your crisis management plans.
- Think ahead about your communication strategy, channels, and messages.
- Be prepared for a lack of availability of your normal communication and collaboration platforms.
- The key to being prepared is to educate, train and exercise your team(s) in advance in a simulation or tabletop.

A dedicated cyber crisis management team

Your organization might have a general crisis management team, and it might have a team or even an entire department responsible for cybersecurity and incident response. However, during a ransomware attack, it often becomes evident that organizations do not know how these teams should collaborate in a dedicated cyber crisis management team. The moment a full-blown cyber crisis occurs, who needs to be involved is mostly unknown. Questions you need to address are: Do you upscale your incident response team? Do you include cyber experts in your general crisis management team?

Understanding the differences between a cyber crisis and a 'regular' crisis is important. Organizations often have a crisis plan or team in place, but that might not suffice due to the unique dilemmas you will face. During a cyber crisis like a ransomware attack, important decisions must be made which require both technical expertise and strategic decision-making. These decisions have to do with, for example, disconnecting systems or networks, negotiating with the hacker, whether to go public with information, and of course: are you willing (and able) to pay an extortion fee? While in essence a technical issue, a ransomware attack often has an impact and scale which severely disrupts the core of your business. Keep in mind that nowadays, multilevel extortion hacks are used more often. You might not only be dealing with inaccessible systems, but also with the theft of data that can be sold, exposed to the public, or used for other malicious purposes; all ramping up the pressure on your organization to meet the hacker's demands. The challenge here is that non-cyber experts need to make far-reaching and potential high-impact decisions about a technical topic.

To manage a crisis properly, it must be crystal clear which roles to involve and what the tasks and responsibilities of these roles are. This will require involvement from both your technical experts and your upper management, and you will need to describe who is involved in gathering the information and input required to manage the crisis and how the coordination and decision-making process will take place.

Ransomware guidelines and plans

Maastricht University, where hackers targeted all Windows-based systems with ransomware, did have plans for crisis management for major incidents (including ICT), but ransomware attacks were not included in those plans.[1] Forensic research shows that this attack started with two phishing emails that were sent when the hackers had been in the university systems for two months already. The attackers also effectively removed the backups. Maastricht University saw no other solution than to pay the ransom of 30 bitcoin, choosing not to put a halt on all student activities for more than a month. Maastricht University has learned from this incident and is now taking cybersecurity very serious by preparing themselves more against cyber incidents. This example illustrates that a ransomware attack is a specific type of crisis with unique dilemmas, requiring you to think about additions or changes to your generic procedures. Organizations often lack a crisis management plan specifically for a ransomware scenario, making it difficult to combat this unique challenge effectively once disaster strikes.

Organizations need to develop guidelines regarding crisis management for a ransomware attack that clarify what roles there should be, what the responsibilities of those roles entail, and which processes must be followed when this cyber-attack occurs. It can also be helpful to

include operational details such as contact information from key staff, and high-level infrastructure overviews such as network diagrams and system descriptions. You may also want to add where to find key information, and the contact details of your (or an) Incident Response provider. You do not have the luxury of time during a crisis, so you should think about what you can prepare in advance. Important strategic decisions that need to be made during a ransomware crisis can already be discussed upfront, for example:

- Do you know which business processes and crown jewels to protect or recover first?
- Who has the mandate to cut connections between networks or assets, and when?
- Are you willing to pay hackers? And if so, are you able to?
- How do you want to organize potential negotiations with the hacker?
- Do you want or need to inform or involve law enforcement and/or your accountant?
- Do you want to be transparent or evasive in your communication?

Guidelines or plans do not have to be all-encompassing documents: the main point is that whatever you develop in advance will be useful in practice. This can either be a runbook or even a scenario flashcard with some guidelines on it that is accessible to everyone within the organization.

Prepared communication

A key challenge will be communication and thinking about what to say to employees, clients, third parties, the media, and other stakeholders during an attack. This can cause unnecessary delays in responding to questions and people feeling like they are left in the dark, which can have an impact on reputation or customer relationships. Therefore, it is important to be prepared in terms of both your stance on transparency/openness and the guidelines you want to have at hand, potentially even templates.

In case you do decide to prepare statements upfront, you only have to fill in the specifics during the crisis, making it easier for the communication department and customer-facing teams to know what to do and say. During the crisis, these teams will form the frontlines, so they need the right tools. Give them a document with frequently asked questions and authentic answers. How your company responds to the crisis can make a difference when it comes to damage limitation and customer relationships. Being proactive in crisis communication gives your company control of the situation at hand but determining how transparent you want to (or can) be depends on the context of your organization. Be concise and cohesive when talking to the stakeholders and the public and remember to also stress something positive, for example, the efforts of the teams working in the background or how you are now upgrading your security to the highest level.

The way of communicating often depends on the culture of an organization. When the ROC Mondriaan in The Hague was attacked with ransomware in 2021, with a subsequent data breach, they did not let the public know what kind of attack they were dealing with in their systems[2]. This resulted in uncertainty with students and lecturers, and even parliamentary questions. Other organizations have opted for a very open approach, like the Swedish company Volue, who organized daily live-streams with their upper management and CISO providing updates for their clients[3]. Whether during the crisis of afterwards, do keep in mind that sharing your experience can be of great value by serving as a warning and a lesson for other organizations.

Out-of-band Communication Zone

When your systems are being attacked by ransomware, it might be impossible to communicate via your normal channels due to plugs being pulled left and right or programs rendered unusable. Next to that, an attacker may also monitor your communications, bringing risk to the use of your usual ordinary channels.

To be able to collaborate as a crisis management team, it is important to have a backup place where you can do so. This can be an alternate website with functionalities or a zone outside the company systems where a new environment is installed with communication functionalities. Furthermore, it is essential to inform employees about what is going on. This can be done in simple ways such as WhatsApp, Signal, or Telegram groups, and you do need to prepare these groups upfront for them to be useful. There are also platforms and other programs on the market that can be bought for this purpose.

Next to having an out-of-band communication zone, it is important to identify key systems and follow best practices for backup. Half the time, organizations do not even know what their crown jewels are. It is important to identify and protect this high-level data. In 2021, the Dutch industrial group VDL Group was hit by a major cyber-attack that affected all 105 companies of the group[4]. VDL itself states that the cyber-attacks runbook came into effect due to adequate signaling, and the IT systems were immediately disconnected. Because they regularly made backups of their systems, a lot of data was protected.

Be prepared through education, training, and most importantly: exercising!

Although an organization can prepare itself for a ransomware crisis by developing plans, having a dedicated crisis management team, and having a communication strategy and backup zone, it is even more important to exercise consistently.

The most important thing is that the key stakeholders within the organization have some notions about the way of working during the crisis, facilitated with valuable instruments such as runbooks, guidelines, or templates. Key is that you don't want to waste too much time discussing topics or arranging measures you could have addressed earlier. It is also important to determine if your organization has the right (technical) capabilities to deal with a cyber crisis. An exercise allows the organization to develop 'muscle memory', having the relevant stakeholders being better aligned for when it does happen. These exercises can be done by e-learnings, small tabletop exercises, dilemma sessions, or an extensive crisis simulation.

An organization can improve its resilience against a ransomware crisis if attention is paid to preparation. This can be done by appointing a dedicated crisis management team to ensure clear tasks and responsibilities. It is also important for an organization to have guidelines regarding a ransomware crisis to act adequately when the situation calls for it. By having guidelines or templates that relate, among other things, to communication during such a crisis, an organization can be better prepared. In addition, it is good to have an out-of-band communication zone when the organization is attacked. In sum, you can actually undertake quite some activities to be better prepared for a ransomware attack. This preparation is key, but of course in the end we all hope you will never need to put preparation into practice.

About the authors:

rachel.splinters@capgemini.com

Rachel Splinters

Rachel is a cybersecurity consultant with a specialization in Crisis and Security Management within the cyber domain and focuses on developing cyber crisis exercises regarding the public and private sector.

manouck.schotvanger@capgemini.com

Manouck Schotvanger

Manouck is a cybersecurity consultant at Capgemini Netherlands. She specializes in crisis and security management within the cybersecurity domain and focuses on business continuity and crisis management regarding the public and private sector.

fokko.dijksterhuis@capgemini.com

Fokko Dijksterhuis

Fokko is the lead of Capgemini's cyber crisis management stream, in addition to which he is specialized in cooperation in the cybersecurity domain on a cross-organizational and international level.

1. https://www.maastrichtuniversity.nl/cyberaanval-een-overzicht
2. https://www.volkskrant.nl/nieuws-achtergrond/grote-cyberaanval-treft-roc-mondriaan-studenten-en-medewerkers-kunnen-niet-bij-bestanden~ba55c62e/?referrer=https%3A%2F%2Fwww.google.com%2F
3. https://www.volue.com/news/volue-after-the-cyberattack
4. https://www.vdlgroep.com/en/news/vdl-groep-back-in-business-after-cyber-attack

SOAR - a technology to improve and speed up phishing responses

How can we use SOAR to grow SOC capabilities and keep up with the rapidly growing and changing threat landscape?

How do we keep our SOCs effective now and in the future? The threat landscape keeps changing, and skilled security analysts are scarce, leading to an increasingly high workload. Could we leverage technology to accomplish the required growth of SOC capabilities?

Highlights

- A rapidly growing and changing threat landscape leads to a shortage of skilled staff.
- The need for SOC capabilities continues to grow.
- SOAR can be leveraged to deal with phishing.
- Full automation is an utopian goal.
- Automation helps SOCs, but it's not a holy grail (yet?).

Keeping up with the rapidly growing and changing threat landscape

The challenge of a modern Security Operations Center (SOC) is to keep ahead of the rapidly growing and changing threat landscape. For 2021, Checkpoint observed a 50% growth of Cyber-attacks compared to 2020 [1]. These trends lead to an increasingly high workload for SOCs and a shortage of skilled SOC staff.

An excessive workload for SOC staff can lead to a short-term focus on the immediate response to security alerts. Worst case, there is not even time to respond to every alert in a timely manner at all. This allows attackers to stay undetected and cause additional damages, which could have been minimized if responded to immediately. Furthermore, the short-term focus prevents SOCs from maturing to create and improve processes and standard operating procedures. This will only increase the time and effort required to respond to security alerts, resulting in a downward spiral.

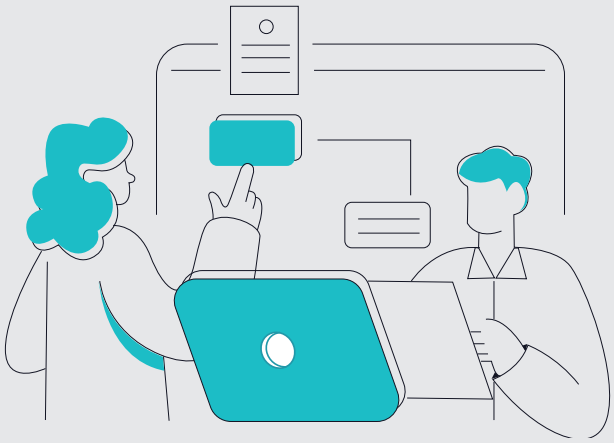
Dealing with phishing further increases SOC overload

One of the oldest cyber threats, and still evolving, is phishing. It impacts every organization by attacking its people, often referred to as the weakest link. Mitigating against phishing attacks is vital for organizations to protect themselves, their employees, customers, and suppliers against the negative impact of cyber-attacks. The large volume in which (possible) phishing emails can be reported and the often repetitive and manual tasks to analyze them adds more workload to the already overburdened staff [2].

Using technology to grow SOC capabilities

Both trends lead to the need for organizations to develop their SOC capabilities. When it's not possible to accomplish this growth by finding the right number and type of people, we need to make smarter use of scarce resources by using technology.

SOAR (Security Orchestration, Automation, and Response) refers to technologies that enable organizations to collect inputs monitored by the security team (Gartner, 20223)[3]. It allows organizations to streamline security operations and to perform automated responses.



Leveraging SOAR to deal with phishing

Phishing is one of the areas where SOAR can improve the effectiveness and efficiency of the SOC. This can be explained by SOAR's two main components: Orchestration and Automation. Orchestration refers to streamlining or standardizing your processes into digital workflows. Having proper and well-thought processes is one of the key success factors for an effective SOAR. Implementing a SOAR also forces organizations to define workflows if not already done. On the one hand, orchestration will lead to quality improvement, as every phishing report will be handled in a standardized, agreed-upon way. On the other hand, this standardization will open the doors for SOAR's second main component, automation.

When starting with automation, every task of the digital phishing workflows should be analyzed for automation possibilities. Some practical automation examples:

- Enriching artifacts (e.g., URLs, IPs) with extra details or reputation information from online sources;
- Reporting URLs to phishing databases (e.g., Microsoft, Google, Phishtank);
- Performing Notice and Takedown Requests (NTD) to bring down a malicious domain or URL.

These examples can often be considered repetitive and time-consuming tasks when analysts need to perform them manually. Analysts need to gather the artifacts, visit all the online sources, run searches, gather results, create emails, etc. With SOAR, these searches can be automated, and the results are presented in one single console. Response actions can also be automated and initiated from that same console, e.g., by using a pre-configured email template to perform NTDs.

Thanks to this orchestration and automation, fewer analysts are required to handle the same volume of phishing reports and deal with attacks. By automating the initial analysis, SOAR reduces response time, allowing analysts to spend their precious time on more complex matters.

A common misconception

It is a common misconception that the full phishing response process can be automated, and that analysts will become redundant. As seen in the previous paragraph, there are great possibilities for automating tasks. However, analysts are still crucial to analyze the information and make a judgement call. One of the reasons is that corporate and online security tools still contain false positives. Automatically initiating your response actions based on that (false) information can lead to all kinds of negative consequences.

How to start using SOAR for phishing?

Below is a conceptual overview that offers a number of necessary steps when you want to use SOAR to deal with your phishing reports (see figure 7).

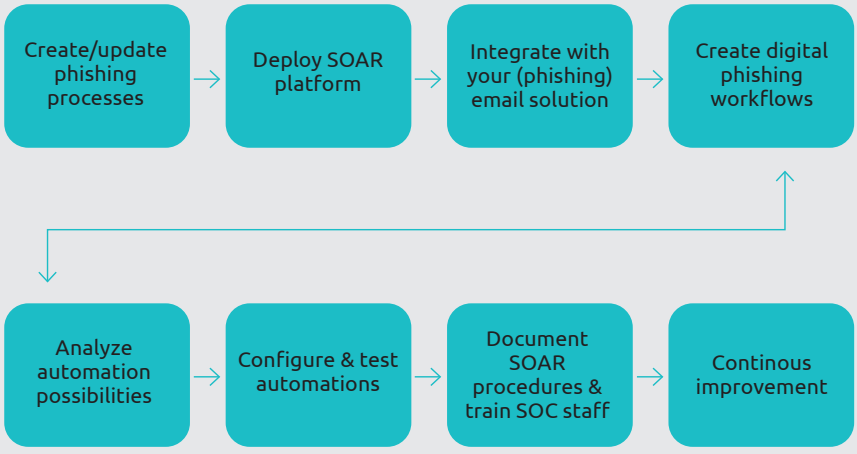


Figure 7

Why implementing SOAR can be challenging

Implementing SOAR can be challenging and requires a certain level of maturity on all levels of the People, Process, and Technology triad.

In terms of people, it's very important to have people from both operations and development on board. Working closely together with the people who know the processes and who are the future users of SOAR, will greatly impact the success of the implementation. Furthermore, technical people are needed who have experience with the SOAR platform and have automation skills, like programming and scripting.

The second key success factor is to have proper processes and documented standard operating procedures. Without this you can't successfully orchestrate and automate. The documented breakdown of activities identifies the opportunities for automation.

The final success factor is technology. First, you need a SOAR tool that fits your purpose. For instance, if you want to migrate your phishing processes to SOAR, you will need a platform that supports connecting to your security or phishing mailbox. The second aspect is maturity. This is less important when looking at phishing alone, but if you want to handle alerts from other security toolings like a SIEM or EDR, a certain level of maturity of those tools and their content is needed to get valuable and actionable alerts in SOAR.

SOAR increases SOC effectivity

Using SOAR in a successful way will lead to the growth of your SOC capabilities, making it more effective and ultimately saving time. This saved time releases your analysts from simple and mundane parts of response activities, allowing them to focus on adding true value. Furthermore, SOAR provides quality and compliancy assurance by proven process execution through orchestration. Additionally, using automation allows for the decrease of both the response time and overall duration of the response to a cyber-attack. As a result, you reduce the window of opportunity for hackers and reduce the risks of being hacked.

Recent developments in both Artificial Intelligence Engines and Machine Learning Algorithms point towards a future where the human role in an Orchestrated and Automated process will continue to decrease in size. This opens up time and opportunity to develop new services. Chaining Orchestrated and Automated processes will add to that decrease in human involvement.

What if a future SOC Operating Model fully incorporates Automation, Artificial Intelligence Engines, and Machine Learning Algorithms? What additional protection could such a SOC provide for your organization?

About the authors:

folkert.visser@capgemini.com

Folkert Visser

Folkert Visser is working in Cyber Defense for over 17 years. He has worked as an incident responder, SOC manager and SecOps lead. Folkert currently focuses on Cyber Defense Operations within the CSU.

stef.bisschop@capgemini.com

Stef Bisschop

Stef is working in cybersecurity for over 5 years. As a security analyst and consultant in the cyber defense field, he is specialized in deploying and working with a variety of security technologies like SOAR, SIEM and EDR.

sjra.maessen@capgemini.com

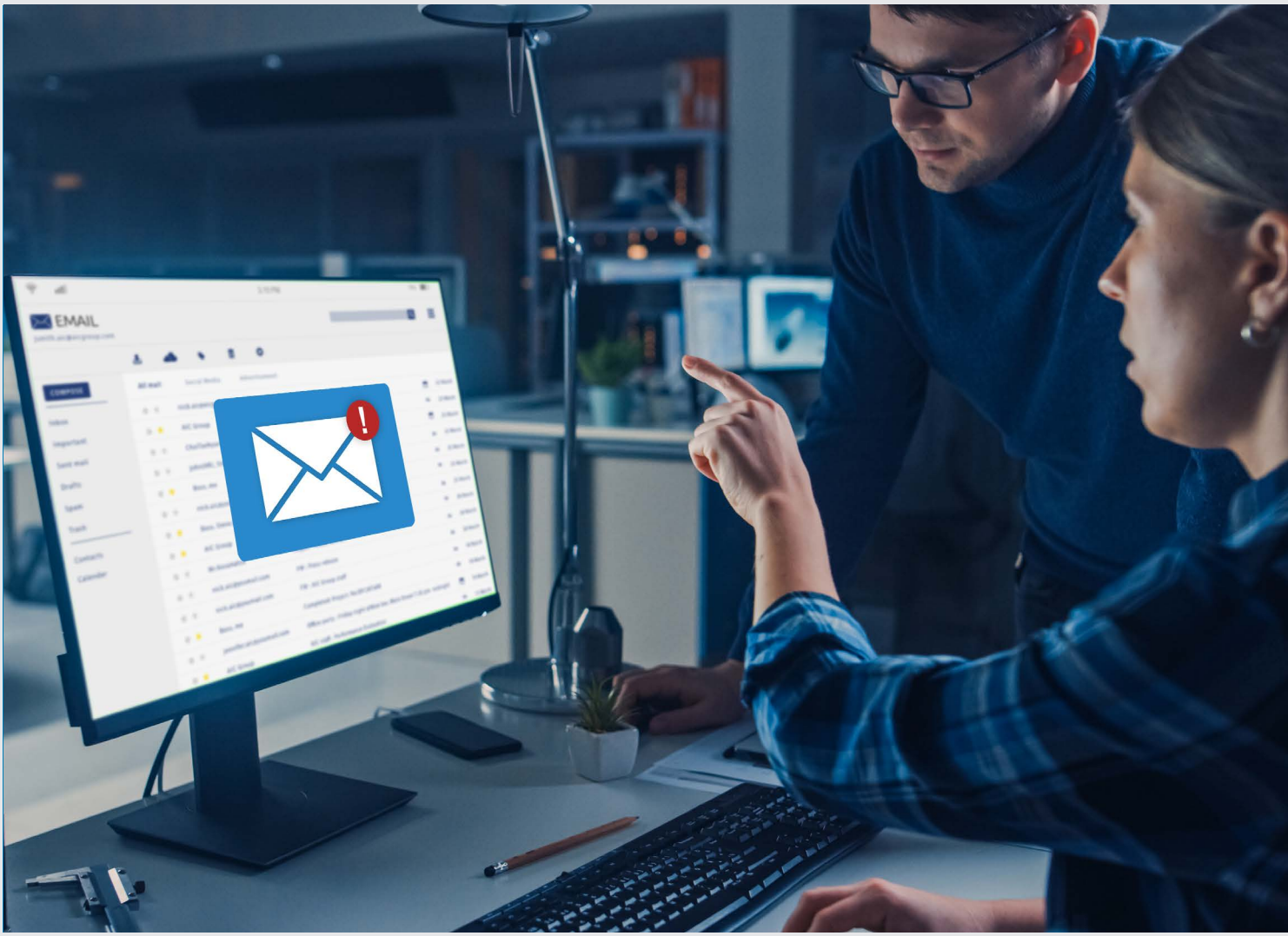
Sjra Maessen

Sjra Maessen is a seasoned security project manager working for years in IT and security. The last years Sjra managed several security projects in multiple security domains (SOC/SIEM, IAM , IT/OT Security).

1. https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/
2. https://newsroom.trendmicro.com/2021-05-25-70-Of-SOC-Teams-Emotionally-Overwhelmed-By-Security- Alert-Volume
3. https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar

03

ARTIFICIAL INTELLIGENCE



03

Trends in Cybersecurity 2022

The impact and considerations around AI driven Detection and Response

With the new wave of AI-driven detection tools, what requirements do you need to consider in finding the right tool for your landscape?

With more and more AI-driven tooling flooding the security tool space, it is becoming harder and harder to find the right tool for the job. With AI-driven analytics and AI-led security response, there are many options with massive potential benefits for your organizations' cyber resilience and security.

Highlights

- How detection and response works.
- How AI impacts detection and response efforts.
- Specific considerations around dealing with false positives.
- The role of the SOC in AI-driven detection and response.
- How to find the right strategy for your organization.

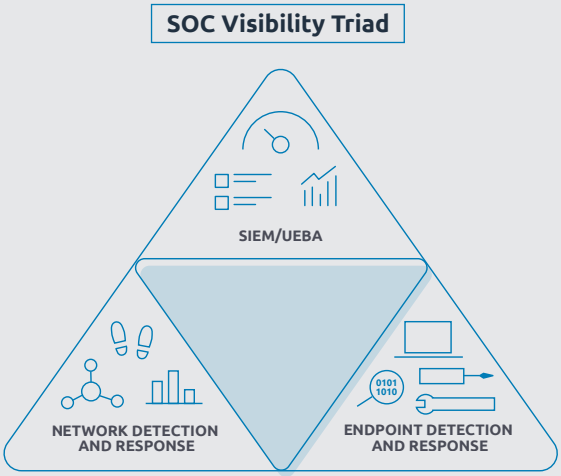


Figure 8: SOC Visibility Triad

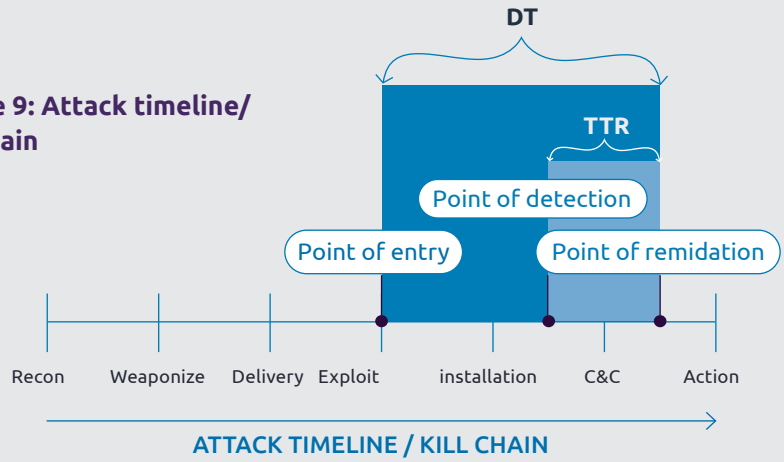
How does detection and response generally work

To answer which scenario fits AI best, we first must consider what forms of detection and response are viable for AI intervention and how this fits into the landscape. In this article we will consider Endpoint Detection and Response (EDR), and Network Detection and Response (NDR), both physical and virtual. When looking to where these capabilities fit in the grand scheme of things, the Gartner visibility triad shows us that they form the foundation of your SOCs visibility.(see figure 8)

EDR pertains to devices like servers, laptops, workstations, and mobile devices. This is where data is processed or where people perform their duties. Therefore, all interventions are done on the device itself, such as putting a file in quarantine, for example

NDR is network-based and looks at data in transit to identify malicious activity, acting by isolating a machine from the network or locking a user account as some response options.

Figure 9: Attack timeline/ kill chain



However, is AI the right fit for every scenario? Or are there times when human interaction would be better? With Man and Machine fighting for the leadership position in today's tool landscape, let's go back to the basics and start with the fundamental considerations needed to find the right tool for the job. And hey, we might learn something new along the way.

When looking at both EDR and NDR we define two key metrics.

Dwell time (DT) is the time an attack has gone undetected (see figure 8). While this is hard to keep track of and requires extensive analysis to quantify, comparing current alert volumes to industry-wide benchmarks can give insight into how good your detection strategy is.

Going a step beyond detection, AI-driven response can be critical in reducing your security teams' time to response (TTR). A properly trained AI can act with expedience when it sees a true positive, stopping any attacker in their tracks. This is the metric most reports focus on.

How does AI get involved in this?

The general rule of thumb is that AI is faster than human thinking. We prefer to use this to benefit either the volume of analysis (DT) or the speed of response (TTR). From this perspective, it appears as if speed is the one true metric. Unfortunately, it's a little more complex than that.

Key challenges come from dealing with change. While AI technology is faster in most cases, it generally works from a baseline. Either a baseline of your environment to define "normal" or a baseline of attack methodologies to define "Evil". Artificial Intelligence (AI) achieves this by leveraging technologies like deep learning. This allows AI to learn what is considered "normal" in the context of the environment. Superior to rule-based filtering, this approach can adapt to changes in your environment with minimal to no human guidance.

Therein lies its downfall. Deep learning requires change to your environment, not your policies and procedures. This means that if you are making changes to your environment, there will be a period where you are getting more false positives as the AI attempts to learn this new normal.

The general rule of thumb is that AI is faster than human thinking. We prefer to use this to benefit either the volume of analysis (DT) or the speed of response (TTR).

The impact of false positives

This challenge of handling false positives is not unique to AI. Both AI-driven and human-driven solutions face the challenge of reducing false positives.

When AI is mainly used to facilitate analysis and reduction of dwell time, a benign detection results in time spent investigating something that wasn't a security incident, as the intent behind the event was not to cause harm. While this feels inefficient, it can still provide benefits in securing the environment. A system administrator doing his job outside the approved process might still require addressing.

However, when AI is focused on automated response and reduction of the time to remediation, a response to a benign detection could disrupt normal IT operations. As an example, if the IT Operations teams are attempting to patch a system vulnerability, but the AI sees this change as malicious, the patching process will be disrupted and in-operable, until the AI has been re-calibrated to exclude these operations.

Differentiating between attackers and admins

We often tell clients that there is little difference between the actions of an attacker and a system administrator. Both are trying to do their job, but an attacker has a vastly different objective than a system administrator. This is what we refer to as "intent", or "context". When security analysts talk about the calibration of detection and response capabilities, this usually refers to filtering out false positives based on newly acquired operational context.

This is an ongoing activity. As businesses and processes change, so does context. Attackers will develop new methodologies that require proper understanding by security teams.

A key consideration to prevent both scenarios is to have specific procedures in place to implement such exclusions to the AI's response to these types of false positives. But the root cause lies in understanding the context of the detection.

While some AI-driven tools provide services that keep the AI up to date on the latest attacker methodologies, it is important to keep in mind that no service can pro-actively ingest your own operational context without your organizations' participation.

What about the SOC?

How your SOC fits into the dynamic of AI, is completely up to you. If you are looking to enhance the team element of your SOC, either because your analysts are overburdened by events or you are simply lacking the manpower to provide full coverage, AI can be a powerful component in decision-making processes. By focusing more on filtering out benign alerts, you help your team to focus on what needs attention.

If you are looking to enhance your facility, and with it your capability, considering AI as a preventative measure might be more suited to your environment; leveraging the speed of action AI brings in automated remediation of detections.

Whether your SOC is a formal part of your organization or just a team of security specialists doing their best, a good strategy will go a long way.

Man versus Machine

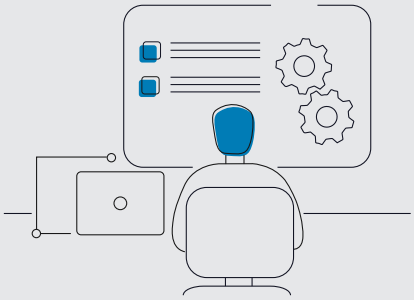
Using only AI will not solve all problems. A synergy needs to be defined between Man and Machine. Defining this strategy requires identifying the areas that matter.

These areas are often closely related to your security strategy. Take, for example, your organization's risk appetite or need for forensic evaluation of an incident. A low-risk appetite organization may favor a more aggressive AI in response to a security incident (improving on TTR by responding with greater speed); a more analysis-focused organization may prefer first to gather all the desired artifacts, improving on DT by learning about all the steps used by the attacker and not just the final stage.

Does this mean AI is or will be the golden solution? No. While AI can greatly reduce workload and increase your organization's security posture, it will still need human intervention to guide it through the messy process of understanding context before it can work on its own.

What strategy is right for me?

As stated, DT and TTR are the key metrics. This goes for all organizations, and how to go about improving those metrics is custom. Dialing the AI to the highest setting can automatically remove anything detected, which means an instant response to any potentially malicious event. This will also guarantee disruption to your other IT processes and maintenance due to an over-aggressive response to false positives.



Circling back

While there is much more to be said for and against AI-driven detection and response, the most important takeaway should be that the fundamental requirement for effective use of AI solutions is strategy. Without an appropriate security strategy, your AI solution is just going to be an expensive trinket in your security team's toolbox.

AI offers great potential by responding faster than its human counterpart, potentially reducing dwell time and time to remediation, while a strong integration with IT Operations seems mandatory to avoid business disruption.

Human-driven has been tried and tested for many years now and has shown to be reliable in a wide range of situations. The question, however, remains if it will remain so in the future.

Currently, there is no one-size-fits-all solution regarding the use of AI-driven detection and response technology. With landscapes rapidly changing and many organizations facing never seen before challenges in both the IT operations and IT Security operations domains, we might simply be past the idea of one-size-fits-all. But one thing we can say for sure, AI-driven solutions have a lot to offer. The only thing left is to figure out where this offer fits best in your environment.

About the authors:

laura.adelaar@capgemini.com

Laura Adelaar

Laura is a cybersecurity consultant with a background in communications. She is focussed on endpoint protection solutions combined with AI.

max.mol@capgemini.com

Max Mol

Max Mol is a cybersecurity consultant with a passion for designing security monitoring solutions. He has worked with Microsoft security products and currently leads the NDR team with a focus on AI driven technologies.

niels.den.otter@capgemini.com

Niels den Otter

Niels den Otter is a cybersecurity consultant specializing in Network Detection and Response. His technical background enhances his capabilities within this realm and allows him to support the core processes of the NDR team.

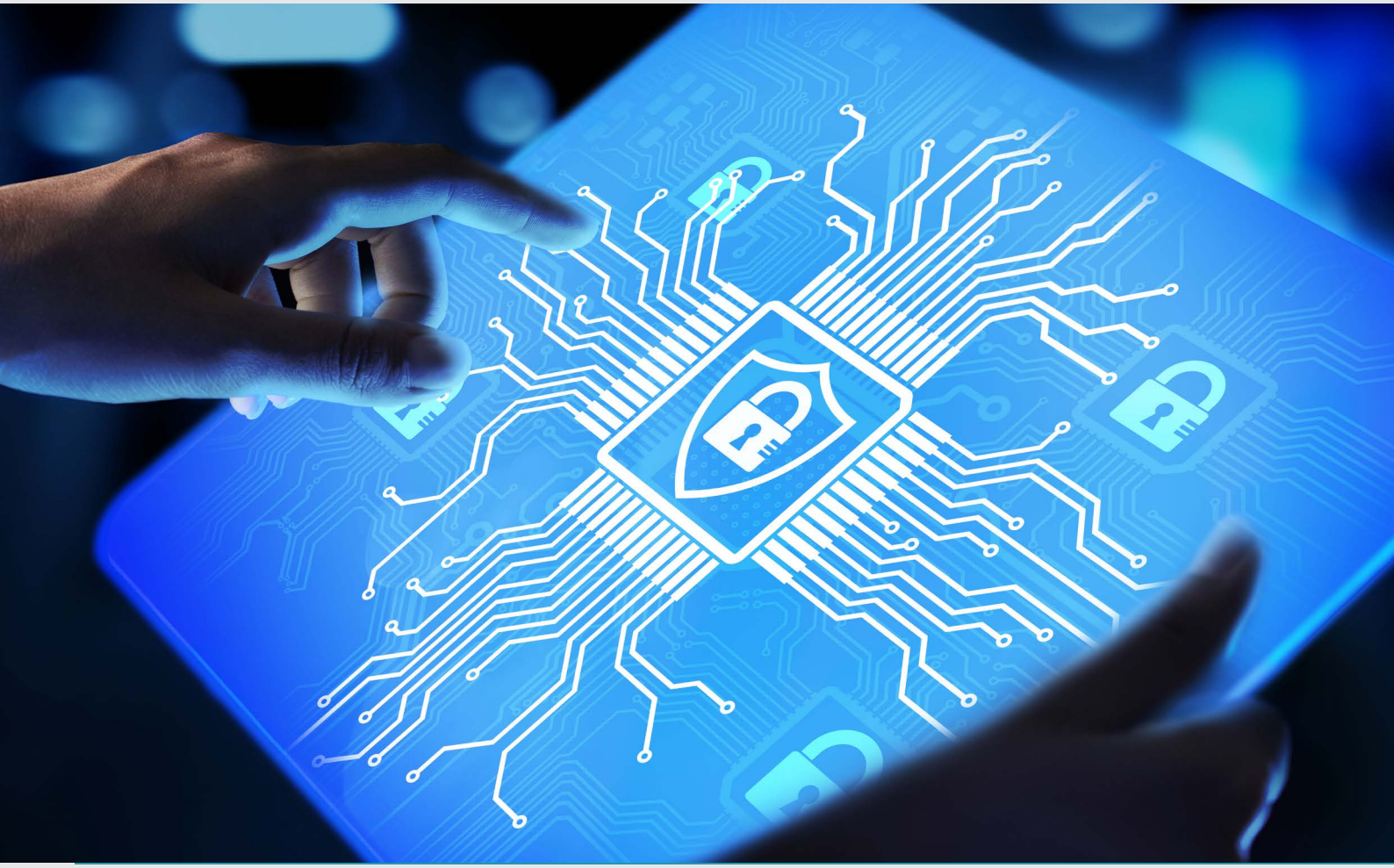
sebastiaan.de.vries@capgemini.com

Sebastiaan de Vries

Sebastiaan de Vries is an experienced cybersecurity consultant specialized in XDR Services. Combining both technical and procedural expertise to bring his clients strong security solutions that drive effective business descision making while keeping the landscape secure.

04

AUTOMATION



04

Trends in Cybersecurity 2022

Automation: A key component to secure cloud workloads at scale

How can enterprise organizations leverage automation to secure cloud environments at scale?

Moving workloads to the cloud at scale can enable new business models, shorter time-to-market, and more resource flexibility. It can also present unique challenges in being secure and compliant. Nevertheless, if automation is applied in cloud security, resources can be focused on innovation, business development, and growth without compromising data protection and control over information.

Highlights

- Platforms, apps, and security operations can benefit from automation.
- Security automation works best when processes are well defined.
- Automation should complement and not hinder DevOps processes.
- Several automation strategies can be leveraged to improve security.
- Automation integrates with people to solve evolving cyber challenges.

In this article we will go over areas where automation can be applied and how to leverage automation to reduce risk and maintain a high-security posture.

With the emerging threat of global cyber-attacks on cloud infrastructure, and the increased speed at which organizations move their workloads to the cloud, comes the challenge of maintaining a high-security posture at scale. A key component in addressing this challenge is leveraging automation to improve and maintain the security of a cloud environment. Due to large-scale environments, common security challenges can be addressed with automation strategies.

Large cloud deployments include workloads that use the same or similar underlying cloud services. If these workloads and services are configured and operated (semi-) manually by different DevOps teams, the risk of misconfiguration is prevalent and amplified by the sheer volume of workloads. This risk results in many resources that must be continuously reviewed, reported on, discussed, remediated, and retested. The same is applicable when new resources are created, which takes time.

Furthermore, public cloud providers' number of services and features is constantly growing. Each new service will have a unique attack surface, security pitfalls, and best practices. When an organization opts for a multi-cloud environment, this variety and volume increases the complexity of maintaining and controlling security posture. In an environment where many different cloud services are being used, an organization needs to continuously generate and iterate guidelines for the DevOps teams to accommodate the proper security of existing resources and ensure the safety of new services.

Lastly, DevOps teams growing in number and size also contribute to complexity. Organizations have pockets of people with cloud security knowledge, but they are not equally distributed across DevOps teams. The unequal distribution of skills and expertise ultimately translates to an unequal distribution of security maturity across the organization. When a team is afforded a high level of autonomy but doesn't have sufficient cloud security knowledge, it could compromise the security posture of an entire enterprise environment.

Automation can be used to deal with the increased complexity of the (partly manual) operation of large-scale cloud deployments and overcome the challenges of unequally distributed expertise. The application of automation can impact many different areas such as platform, application, and operational security. However, leveraging automation works best in areas where processes are well defined, and security strategy is aligned with business goals.

In the following, we describe several approaches to security automation that an organization can adopt. Combining one or more approaches can ensure that automation is consistently applied across different security aspects in an environment.

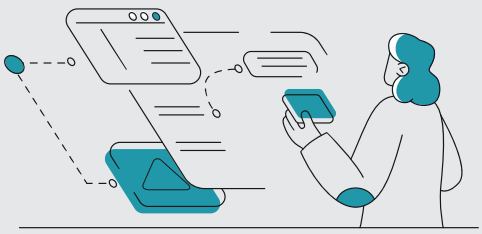
Policies and guardrails

Popular cloud providers such as AWS, Azure, and GCP deliver capabilities to enforce security policies and the desired resource configuration state of the cloud control plane. These policies act as guardrails to the environment, programmatically enforcing certain rules to ensure proper governance. These capabilities could also be used to describe the desired security state for a resource. When a resource deviating from the desired state is deployed, it is remediated, and its configuration is automatically changed to the desired secure state. This reduces the challenges of configuration drift and manually fixing misconfigured resources. It is important to test policies and configurations extensively and communicate changes to DevOps teams as it could affect their development processes. Transparency enables DevOps teams to troubleshoot more effectively.

Automated security testing and scanning in the continuous integration/continuous delivery (CI/CD) process

A significant portion of security and policy-assurance testing can be automated and performed continuously in the DevOps process. When security or compliance issues are raised early in a development life cycle, they are relatively easier and cheaper to fix. Traditional security and assurance testing methods cannot keep up with the speed and agility of the DevOps team deploying and running workloads on cloud platforms. Automated assessments of application source code and infrastructure as code for vulnerabilities, misconfigurations, or compliance issues, are vital in ensuring the security of products and services shipped by DevOps teams. An additional benefit of automated security testing is the educational value of the output from scans. Good tooling informs users why specific findings are security or compliance issues, and these explanations are an opportunity for developers and operation engineers to educate themselves.

Security scans can integrate into the CI/CD process to perform many different automated checks. This includes scanning third-party software libraries for known vulnerabilities, looking for sensitive information such as credentials and secrets residing in the source code repository, statically analyzing code for bad coding practices, and scanning the application code for common vulnerabilities or misconfigurations. Additionally, automated dynamic testing of an application deployed in a test environment allows finding runtime-related security issues before the application is released. The results



Automated access controls built from sound security guidelines are less susceptible to manual misconfiguration.
This significantly improves governance in the environment and limits the risk of excessive permissions being assigned at scale.

of the automated scans should be fed into a vulnerability management system to track security issues and progress across an organization. Traditional penetration tests are still necessary. Some problems are context-specific and require human intervention but automating security testing could limit the number of new issues identified during a penetration test and give developers time to address common security issues.

Automating access control

Distinct workloads of DevOps teams should be separated logically within the cloud environment. Members of DevOps teams should only be assigned permissions to operate within the scope of the workloads they are responsible for, following the principle of least privilege. Furthermore, members should only have access to service accounts that operate within a limited scope. Some environments will have shared infrastructure and cross-functional teams, which can also be accommodated when designing access controls. Manual processes such as creating logical workspaces for teams, onboarding members to the environment, assigning access to workloads, and expanding shared infrastructure should be translated into automated processes. Automated access controls built from sound security guidelines are less susceptible to manual misconfiguration. This significantly improves governance in the environment and limits the risk of excessive permissions being assigned at scale.

Pre-built modules and templates

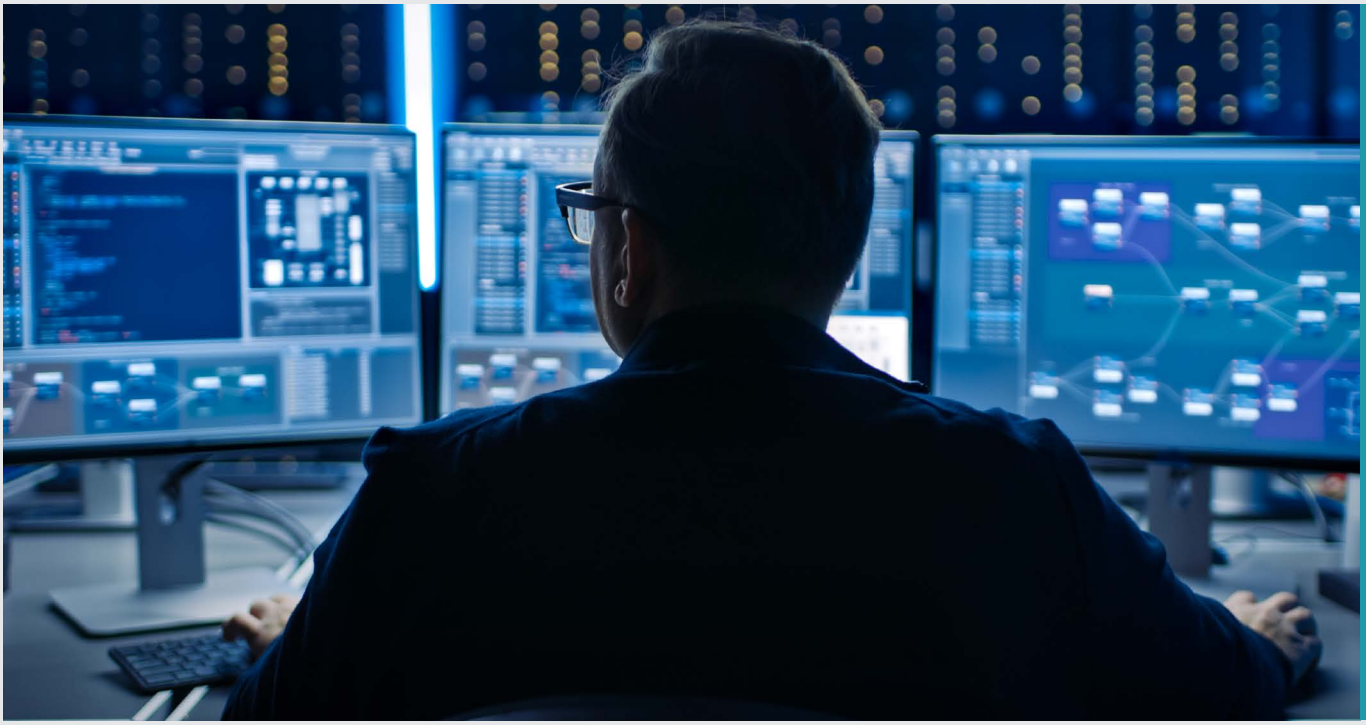
Pre-built modules and templates can be used to automatically configure the secure configuration of cloud platform resources, and DevOps teams can deploy predefined resources where secure configuration is baked in and automatically configured. The downsides of this approach include less flexibility for the DevOps teams and additional overhead for authoring and maintaining these modules and templates. Organizations with low-risk tolerance and strict security guidelines can opt for this approach to stay compliant and minimize security drift.

Automation in security monitoring

Logging and monitoring solutions in large-scale environments will generate many logs and alerts. Introducing automation in security operations and monitoring could help programmatically detect, investigate, and remediate cyber threats. By introducing machine learning into the monitoring solution, it could be used to limit the false positives and filter out noise to reveal important incidents. This reduces the volume of logs that analysts need to triage through and could be used to prevent alert fatigue. Incident response can be automated by automatically blocking communications to targeted attacks from known bad infrastructure. Security automation can accelerate the turnaround time from detecting to responding to a cyber-attack, reducing the time window for an attacker to successfully exploit vulnerabilities in the environment.

Host and container hardening

Several tools can be used to automatically restrict the functionality of a device to reduce its attack surface. Hardened controls can automatically be applied across multiple devices and configured from a single control pane. This can ensure that repeatable, secure configurations are consistently applied across an estate. These tools are commonly used to restrict the capabilities of applications and the underlying operating system, access to privileged



functionality, file permissions, and network access on containers and hosts. DevOps teams might find that certain restrictions severely hinder legitimate functionality; in that case, discussions are important to understand business needs. The balance between security and usability must be carefully weighed when automatically enforcing this defence-in-depth strategy.

Automating OS patching

Most public cloud providers offer managed or PaaS services that offload the responsibility for patching the underlying infrastructure to the cloud vendor. Although they do not eliminate security responsibility, they ensure that the underlying OS stays up to date, enabling DevOps teams to spend more time on development. However, some development use cases still require infrastructure where DevOps teams can access the underlying OS, and organizations are responsible for keeping this infrastructure up to date. Update management can be made easy by using cloud-native automation tools to ensure that important security patches are deployed continuously, with minimal disruption to workloads. These patch orchestration tools can be tweaked to specify categories of patches such as critical or security updates, suitable times when these patches should be performed to minimize workload disruption, and the types of operating systems included in the automated process.

As the automation strategy matures and automated controls become more effective at enforcing the desired security state, the probability of known misconfigurations and vulnerabilities surfacing should reduce in the environment. Furthermore, automated processes can be extended for novel threats by programmatically identifying and containing such threats and securing resources at scale. As more components become automated, security teams can shift effort from

repeatable operational activities to researched focused activities such as exploring the security of new technologies relevant to the organization. Furthermore, as DevOps teams mature in their understanding of cloud security, the balance between autonomy and automation can be fine-tuned. Investing time to automate cloud security will play a key part in building a cyber-resilient organization with a long-term vision. We advise you to think about how your organization can use it today, to future-proof the security of your cloud infrastructure.

Most public cloud providers offer managed or PaaS services that offload the responsibility for patching the underlying infrastructure to the cloud vendor.

About the authors:

thijs.verkuijlen@capgemini.com

Thijs Verkuijlen

Thijs is a cloud security engineer specialized in Azure cloud security. His main focus is on codifying security controls and coming up with new and innovative ways to improve the customers security posture in the cloud.

rafik.nasiri@capgemini.com

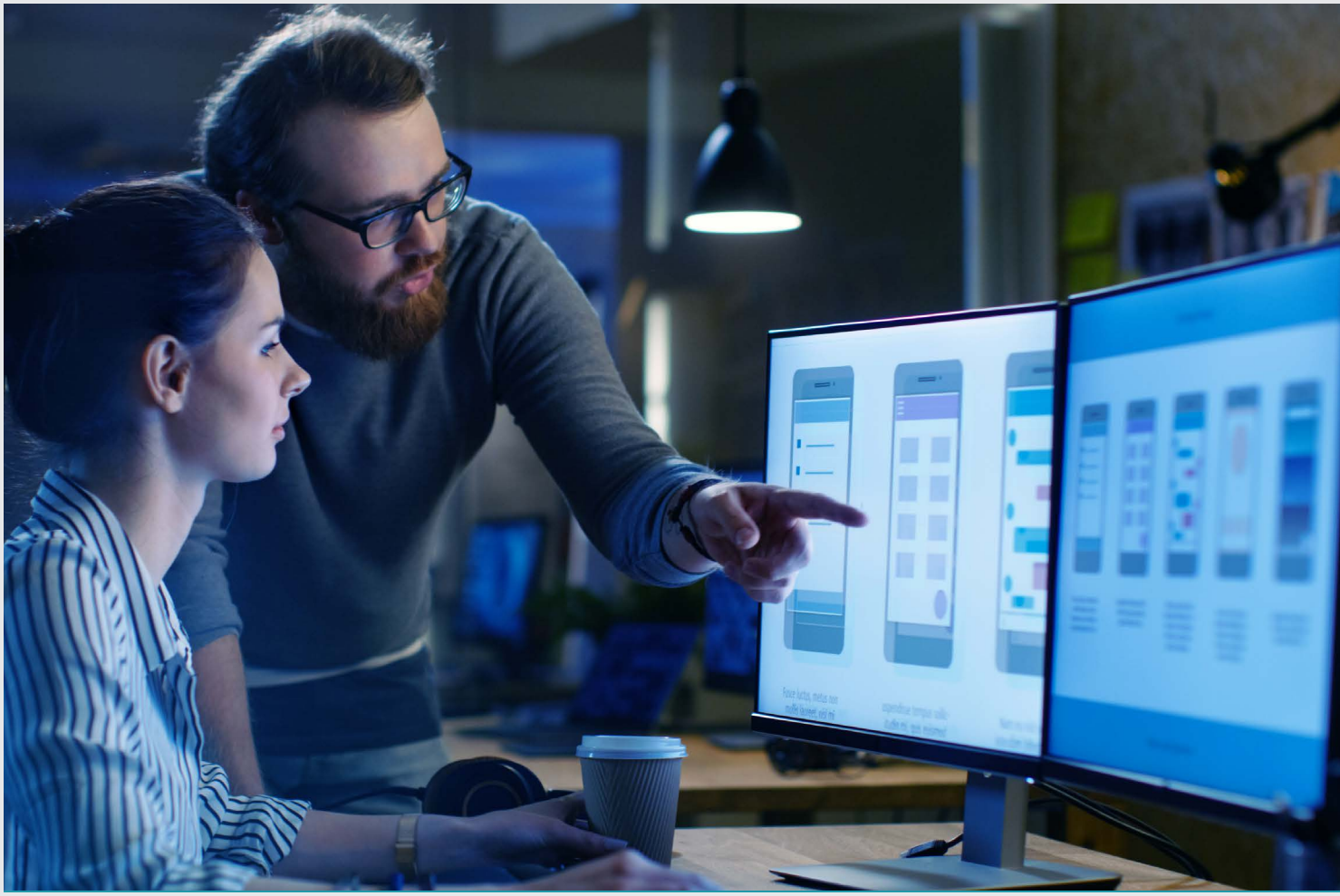
Rafik Nasiri

Rafik is a SOC analyst working with Azure Sentinel. He is a part of a SOC team that ensures that the network of several customers is monitored for suspicious activity and provides response to several incidents within the SOC.

jean.smidt@capgemini.com

Jean de Smidt

Jean is an experienced cloud security engineer and penetration tester. He works closely with organisations to secure infrastructure, access controls and networks in large cloud environments.



Keeping your application landscape secure and innovative in a dynamically changing world

How can people, processes, and technology work together to support innovation and security of assets in a new way of working?

People, processes, and technology work together to support the parallel activities of implementing secure solutions and reactions to unexpected events. Cloud solutions are becoming the norm. Cloud application and infrastructure are typically developed in CI/CD pipelines. Development of security controls exists on

Highlights

- Cloud adoption and agile are stimulating collaboration between security, infrastructure, and development teams.
- Achieving full control requires knowing your assets. Strategy, tactical and operational levels must be aligned.
- Security must be part of all development and production support.
- Do not assume that you are protected.
- Security must not block innovation.

the border between software and IaC development. Therefore, development of security controls is part of the CI/CD pipeline. Security staff must also recognize and respond to security events in real-time.

The challenge is to build an integrated set of processes and tools to optimize the speed, effectiveness, and efficiency with which security staff can build and maintain security solutions.

Current way of working

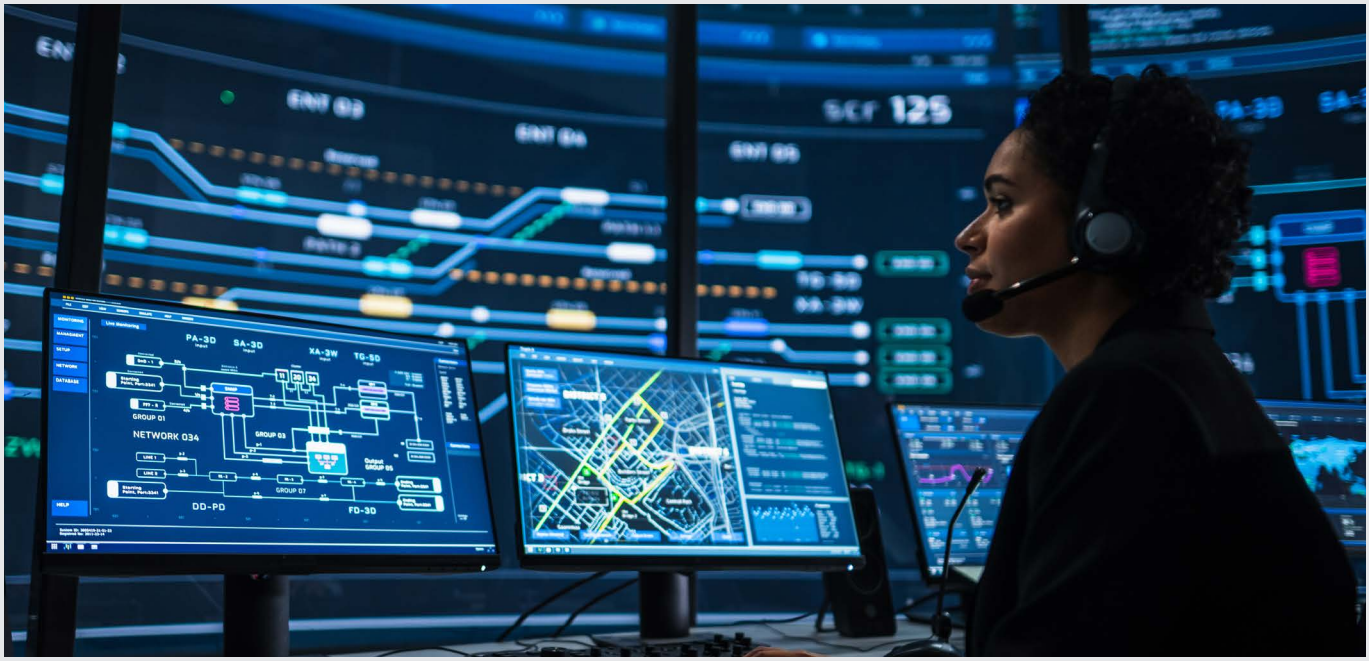
Different sized companies have different approaches to generating business. A small start-up will typically focus on generating income quickly or satisfying investors with the potential to create income. A retailer makes sure they stay ahead of their competitors by reacting quickly. Large corporations are less dynamic when they have a large customer base and generate enough income regularly.

Small companies focus on one or a small number of solutions, and large corporations manage many solutions as part of their application landscape. Regardless of size and market share, they must all become profitable and conform to laws. Therefore, their security policies require clear alignment between strategy, tactical and operational levels.

More and more solutions are being developed for the cloud. Each solution is composed of small software services working together, and cloud solutions are typically developed in CI/CD pipelines. Solutions are developed with standard services provided by one of the main cloud providers, such as Amazon AWS or Microsoft Azure. Development includes the use of standard computer languages like Java and JavaScript but also infrastructure development with Infra-As-Code templates such as Terraform.

Start-ups, medium and large corporations have the same generic challenges from a security perspective. They must react quickly against threats and known vulnerabilities in their solution. Awareness of their application, infrastructure, and data landscape is paramount. A complete overview of their environments and assets, threats and vulnerabilities, the resulting risks, and mitigation for each risk is a must-have. Built-in control with PDCA must be implemented within and outside the CI/CD pipeline. Full control is only possible by having the necessary processes in place. These processes are supported by technology for automated tooling within and outside the CI/CD pipeline.

Maintaining the balance between standardization and flexibility is a must for every organization. They need to combine people, processes, and technology to be in full control of their security. Automated tooling is becoming more common in representing technology. The challenge for start-ups and small companies is developing and maintaining their unique selling point and keeping it secure. Challenges for large corporations are to have full control over their own internal and outsourced developments, maintain their application landscape and be in ownership of innovation. Typically, these challenges and full control of security are not currently met as they should be.



An ideal way of working

An ideal way of working is to have security policies which are aligned with enterprise and IT architecture, security architecture, the structured implementation of security controls, and incident management. Security architecture protects the application and data landscape. Structured implementation of security controls provides a mechanism to achieve a secure architecture. Control of security against a framework indicates where there are gaps and security exists. The more you are prepared, the less you will be negatively affected by unforeseen events.

Defining the IT architecture, security architecture, and security policies must include tooling, processes and roles, responsibilities, and tasks for security people and the teams. New developments and existing production solutions must be continually protected.

Developed applications, third-party software, middleware, operating systems, and your network can all be attacked by unexpected events. It is therefore important to be prepared for attacks from threats that are known and new, zero-day attacks. Automated scans must be used to report on vulnerabilities. A process must exist for combining the manual and automated effort to remove vulnerabilities with solutions. Zero-day attacks must be dealt with separately because there are no available solutions.

Threats exist against asset vulnerabilities in each company's landscape. Protection against threats usually requires threat modelling. The result shows where we are missing protection. It provides focus on priority of protection for the business.

Each solution includes people, process, and technology. Security people implement or manage the controls represented by policies, compliance standards and frameworks. They use manual and automated processes to develop and maintain PDCA process or life-cycle. Technology is used to support repeatable and automated measurement and control. Frameworks, such as CIS , are necessary to indicate where we are missing security controls.

Tools representing technology are an essential part of business support.

Increasing automation with tools is a must-have. AI is an important part of the tooling world. Examples are network monitoring and learning to spot suspicious network traffic. Quantum computing is on the near horizon. One important example is quantum cryptography, which will significantly impact the data encryption world.

Roadmap to an ideal way of working

A generic roadmap can combine strategic top-down and agile bottom-up for all company sizes. Development of applications and infrastructure do not have to waterfall wait for comprehensive documentation on security. Security policies, standards and frameworks must be used as a guideline to determine where we have control and where there are gaps. Agile implementation of security controls can support strategy when the controls are mapped to frameworks and mapped to standards and company policies and strategies. This sliced approach allows one or a limited number of controls to be implemented but not all at once. A prerequisite is that each control implemented must be registered against the framework and standard to register coverage. An example is application security covered by secure software development and continuous vulnerability management on VM operating systems addressed by the infrastructure team.

A continuous agile approach for each security control will increase knowledge, experience in people, and provide input for improvements in processes and use of technology. It will also provide input upward to strategic and tactical decisions, improving the PDCA process within and between the different strategic, tactical, and operational levels.

A fundamental part of this approach is secure software development see figure 10 & 11. It must be supported by and integrated with infrastructure development, and together they must be supported or be directly involved with solving incidents in production.

Application development should, therefore, conform to secure software design. Vulnerability scans must be regularly executed by tooling on applications, third-party software, and operating systems. Automatic patching and upgrades or quick turnaround should be used. PDCA must be implemented in the agile iterations to ensure that the necessary changes have been made. These are only part of the full set of required controls.

Tooling is a necessary and important part of all developments and automated controls. Continuous research should be performed on the existing solution to determine improvements or replace existing tooling. Therefore continuous research must be performed on all tools, from portfolio and license management to production scans. These will provide input on gaps or overlaps in using tools or better alternatives and new developments.

Technology provides the ability for a business to find new opportunities and change. Security and infrastructure development can provide the ability for business to survive and innovate.

An example of the process for secure software development is as follows:

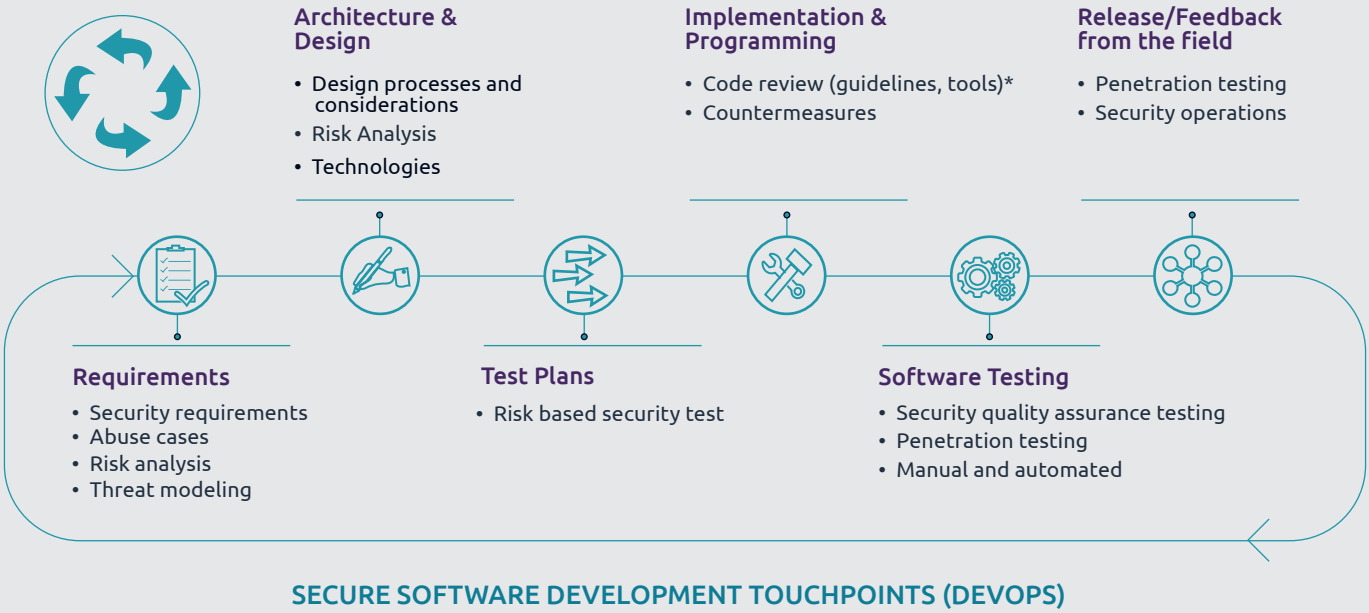


Figure 10: Secure software development touchpoints

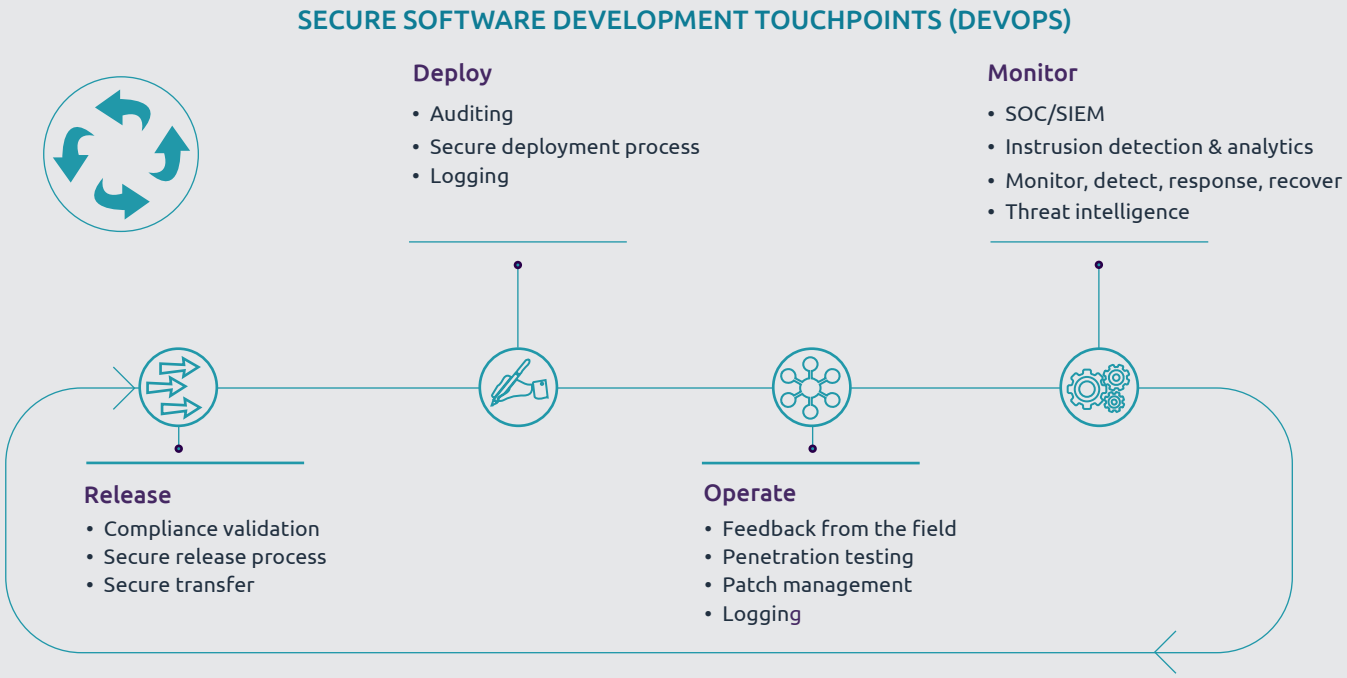


Figure 11: Secure software development touchpoints

The new way of working dictates that people, processes, and technology must combine to provide efficient, effective, and secure support for business objectives. Each development CI/CD pipeline secured before deployment. Each production deployment should be continually measured for vulnerabilities. Threat modeling and follow-on actions must be part of each standard process.

Secure PDCA must be enacted between and within the strategic, tactical, and operational levels. PDCA between (and within) strategic, tactical, and operational levels should be continually improved. Security decisions at all levels will become more transparent and real-time. Development, infrastructure, and security members must work closely together in an Agile manner so that new developments and existing deployments are kept safe. This Agile approach will allow for quick repairs of faulty decisions, mistakes, and external effects. It will support implementation of solid, secure solutions by iteratively building on small successes.

A new way of working requires not just PDCA on all levels. It requires full continual transparency on the link between strategic requirements, policies, compliance against standards, frameworks, and implementations. A new mindset of transparent and continual improvement is required. This means that people, processes, and technology must work together optimally, effectively, and efficiently to support security for business and continual innovation.

About the author:

barry.jones@capgemini.com

Barry Jones

Barry is a managing consultant with more than 30 years of varied IT experience. He is CISSP and CEH certified. Barry is working and researching on operational PDCA of security in AWS and Azure Cloud solutions. His focus is the alignment between strategic, tactical, and operational levels. This requires alignment between policies, standards, and frameworks. Full control is achieved from an Agile approach. His objective is to maximum automation of tooling and minimize manual effort. Secure software development is one of the important elements of his approach.

Securing the SAP Landscape - Bridging Cybersecurity and SAP

How to face key challenges on cybersecurity risks in our SAP Landscape?

The SAP landscape has become an integral part of intelligent enterprises as SAP applications provide businesses with a seamless way to manage their various departments effortlessly. With the digital economy creating opportunities for companies to transform and scale, SAP encourages customers to move to SAP S/4HANA and reap the benefits of a flexible, scalable cloud-based system.

However, recent cyber threats in the complex SAP landscape prove that continuous monitoring to identify and secure threats and vulnerabilities is needed. This article describes the challenges and the tools to identify and mitigate vulnerabilities.


Matching Password

Highlights

- Gain insight into vulnerabilities and threats in the SAP application and database, including security (and compliant state).
- Prevent attackers from bypassing the segregation of duties (SoD) and authorization controls.
- Handle risk of unsecure code or configuration and setting up continuous reporting on SAP cybersecurity posture.
- Maintain controls in a compliant state within the SAP landscape and enforce security baselines for SAP ECC or SAP S/4HANA landscapes.

Classic and extended Security in SAP Landscape

Since SAP has a lot of built-in facilities in line with recommendations for secure application in on-premises (e.g., encryption, authentication etc.), the industry has not invested much in identifying and remediating inherent vulnerabilities inside existing configurations. The result is a potential to disrupt critical business and even lead to critical events like data theft and data deletion. It has become - in these changing SAP environments - very important to identify new threats and weaknesses in SAP security configurations. SAP vulnerability remediations for mission-critical systems must be prioritized. This would improve productivity, efficiency, and compliance, while reducing risks, costs, and time to investigate, identify, and remediate.

The focus on native (out-of-box) cybersecurity provided by SAP is primarily on protecting identities, user accounts and data encryption. These key controls provide the first line of defense, but blind spots still exist. Critical SAP vulnerabilities exposed to modern-day advanced cyber threats, if unmanaged, could lead to cyber-attacks causing critical business disruptions. Therefore, in a highly complex environment, it is advised to have dedicated automated tools instead of manual checks on vulnerabilities, risk levels, business impact, and methods to remediate or mitigate such risks. Let us take you along the challenges for the current SAP landscape, and the possible solutions to mitigate those challenges in the current and the future state in, for example, the S/4 HANA projects and secure Migration to cloud.

Security challenges in SAP Landscape

The primary goal of cybersecurity is to ensure the confidentiality and privacy of information, the correctness of data, and access to authorized users. Yet, these cybersecurity goals are not easy to achieve, and cybercrime statistics overall are alarming. Cyber threats and incidents have increased due to the pandemic in 2020 to and have increased even further in 2022 due to geographical tensions in the Ukraine.

Organizations are generally focused on securing components like OS, Web stack, and Database. However, they are unaware of the specific vulnerabilities in the application layer (e.g. database systems, user data and identities). Merely a missing patch update can become a prime target for attackers on the hunt for sensitive data. Wrong configurations in the SAP application can even compromise the access of, for instance, critical accounts. A critical account is the only superuser in the system with unlimited access authorizations.

The IDC survey on cybersecurity in 2021 reveals that 64% organizations have reported a breach in their ERP systems including SAP in the past 24 months. IDC research further suggests that ERP systems, such as SAP, are under increased attack for material data.

The above scenarios are just some examples of components for which the existing approach of SAP application security teams does not suffice. No wonder, then, that the idea is gaining traction that SAP application security should be included in the cybersecurity Scope.

Solutions to solve challenges in SAP landscape

The SAP landscape is a popular target for cybercrime because it stores and processes a lot of sensitive information, from social personally identifiable information, supplier data and customer data to financial data like payment information and sales orders.

The best solution to meet challenges and remediate vulnerabilities in the SAP landscape in your organization is to bring together the existing SAP and cyber expertise – SAP Basis, SAP Security, SAP GRC and cyber vulnerability management. The integrations ensure a complete coverage of the broader SAP Landscape: SAP Roles Security, SAP Application & Database Security and SAP Hosting Security. [see figure 12]

To integrate the cybersecurity and SAP landscape silos, you should be very clear on different aspects of cybersecurity and how each aspect helps to remediate the drawbacks of SAP application security.

The SAP landscape demands a comprehensive security and industry specific approach because of multiple important security aspects and considerations:

- Use SAP Security Baselines (SB) to understand the highlights and best practices for securing SAP solutions. Every organization should align SB in the process of selecting the right SAP security controls;
- Use SAP HANA Security Framework to understand SAP's technical holistic security guidance for on-premises and in the cloud;
- Make security patching an imperative – annual system upgrades are not sufficient. SAP releases a lot of security patches and many of these patches are not included in the service pack upgrades;
- Assess SAP vulnerability risks on a regular basis, using suitable tooling like Onapsis and MS Sentinel SAP Threat Monitoring;
- Consider that SAP security is more than Segregation of Duties (SOD) and default authorizations – attackers can bypass the SOD and built-in authorizations controls to gain privileged access to SAP;
- Integrate SAP security monitoring with a corporate SIEM solution. SIEM solutions help companies to use real-time intelligence to respond to internal and external cybersecurity threats;
- Ensure the use of the "Golden Content" best practices in your specific industry.

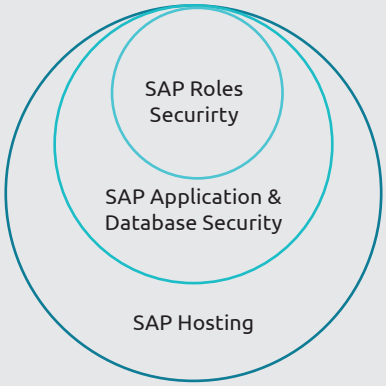


Figure 12

The above security aspects comprise the minimum set of capabilities to protect the SAP landscape. Once businesses have the much-needed assurance that their business processes are safe and secure, they can invest their energy and time in their core business areas.

A practical approach to get a good insight in SAP vulnerabilities is to find out the feasible automated solution to conduct a vulnerability assessment. Additionally, you should think about implementing management solutions which can readily integrate with different incident management tools. Keeping the strategy of "thinking ahead" in mind, the preventive solution is not to trust others to keep your physical and virtual assets safe, but to take control of security yourself.

Example Risk Score 10 Vulnerability

The Onapsis Research Labs and SAP Product Security Response Team (PSRT) joined forces to discover and patch three critical vulnerabilities that affected Internet Communication Manager (ICM), a core component of SAP business applications. The individual ICMAD vulnerabilities were identified as CVE-2022-22536, CVE-2022-22532, and CVE-2022-22533 — the first of which received the highest possible risk score, a 10 out of 10. The other two received scores of 8.1 and 7.5 respectively. As a result, the U.S. Department of Homeland Security's CISA issued a Current Activity Alert.

Both SAP and Onapsis advise impacted organizations to prioritize applying the Security Notes 3123396 and 3123427 to their affected SAP applications immediately. If exploited, these vulnerabilities, dubbed ICMAD (Internet Communication Manager Advanced Desync), enable attackers to execute serious malicious activities on SAP users, business information, and processes — and ultimately compromise unpatched SAP applications.

It is an important and urgent message for your organization, that in order to meet the business need to be in control over your SAP Landscape, you urgently need to bridge the cybersecurity and SAP silos in your organization.

Combining and integrating SAP & cyber competences yields two main benefits:

The **SAP Landscape will be part of the overall cybersecurity strategy**, underlying plans and security automation initiatives. For example, it would be possible to implement a specific SAP vulnerability management solution that has the capability to integrate with different popular incident management tools (E.g., SNOW, JIRA), which can ensure the end-to-end workflow while abiding with service level agreements.

Secondly, from an SAP competence perspective – **security requirements will be fully included in the SAP World**. That SAP World could be implementing automated controls in your existing ECC landscape, integrating security requirements in the Blueprint of your S/4 HANA Green Field implementation and/or assessing vulnerabilities before migration to cloud.

Next steps in this integration journey of SAP & Cyber is to start integrating Security & Compliance requirements in your SAP approach. Automation will make – your Security & Compliance life in SAP landscape a lot easier!

About the authors:

kriti.gourab.biswas@capgemini.com

Kriti Gourab Biswas

Kriti is experienced in working with clients from Middle East, Western Mediterranean and European countries in the Domain of SAP authorization and authentication for more than five years. He played key role in designing security structure of some big clients. Currently he is focussed in developing new solutions for SAP vulnerability management.

yogita.mahajan@capgemini.com

Yogita Mahajan

Yogita is SAP Security GRC certified consultant and has 15 years of experience in SAP Consulting, Implementation with a specialization in SAP Security and GRC AC 10.1, GRC AC 12.0, Onapsis Vulnerability Assessment and Management, skilled in Business Process, SAP NetWeaver, SAP NetWeaver Business Warehouse (SAP BW), SAP Implementation, GRC 10/10.1/GRC 12.0, HANA and Azure Migration support, SSO implementation. Worked for different Manufacturing, Automobile, and medical industries from the region of US, CA, UK, and NL.

rutuja.shedsale@capgemini.com

Rutuja Shedsale

Rutuja is a certified SAP Security and GRC architect at Capgemini with over 9 years of experience. She specialises in advising and implementing security solutions for the customers taking into account the industry best practices for cloud and on-premise environment.

ankit.arya@capgemini.com

Ankit Arya

Ankit is SAP Security and GRC consultant having 10 years of experience in various leading consulting roles with emphasis of Audit, Risk and Compliance Management. Ankit designed and implemented comprehensive business-driven security models for various SAP ERP products in compliance with audit requirements.

sagarika.ghosh@capgemini.com

Sagarika Ghosh

Sagarika is a SAP Security Consultant with 7 years of experience, having specialization in SAP ECC Security, GRC AC 10.1, GRC AC 12.0,SAP BW Security, HANAStudio, S/4 HANA, FIORI, Successfactors, Concur. Sagarika has implemented GRC Security models and designed Successfactors RBP concept for business.

05

ZERO TRUST

Zero trust, a shift-up in security governance

Highlights

- Zero trust developments increase business involvement.
- The shift from technology-centric to identity-centric will intensify.
- Besides identity and roles, context and behavior are also input for granting access.
- AI will play a major role in converting complex patterns to logical business decisions.
- Similar conditions can lead to different access decisions.

05

Trends in Cybersecurity 2022

How does zero trust affect business decisions regarding access governance?

Most of the time, zero trust is addressed from a technology perspective and the NIST SP800-207 is a good standard. In general, the components as described in the basic zero-trust construction are used, and technology is provided to deliver these components. In a zero-trust environment, attribute-based access control is the main principle governing access decisions. Various attributes of the identity will describe the context of the identity and a business-defined policy will grant or deny access. This policy will shift from a technical policy to a business-oriented policy, putting business owners in the driving seat of access control by defining

SPOILER ALERT

The threats will decrease over time while business driven access management will increase.

those policies. But will this shift affect the risk of unauthorized access? What will be the role of the business in granting users access to data?

In limiting user access, two main principles have always driven the composition of user access rights in profiles, roles, or groups. The main point has always been to only provide the minimum set of access rights to users; “Need to know”. This is to prevent users from engaging in fraudulent activities and prevent adversaries with stolen user accounts from being able to do much damage. Using zero trust principles, the number of possible decisions increases, allowing business users much more flexibility. In the basic zero-trust construction (see figure 13), the basic principles are depicted. A user uses a device, and through that device, services are accessed. The Enforcement Point receives the request through the access network and decides on a number of criteria to either grant, revoke or limit access. Apart from using the attributes for direct access decisions, a few of the attributes can also be used as proof of authentication and the trust level of the authentication. Behavior analytics as an example can either be used as proof that an individual is authentic but also as additional proof that the individual is not behaving rationally enough to grant (critical) access. As an analogy, a car driver may have a valid driving license, but his behavior may show that he is too tired to drive safely. In the zero-trust environment, a similar individual may be rated as authentic, but behavior analytics will show he is in an absent state of mind. Based on this analysis, his access will be limited to only standard application use; he will not be allowed to engage in customer interaction. This has some interesting ethical angles that need to be discussed. A car deciding what actions are allowed for a human, implies human behavior is tracked and becoming visible to party or parties without explicit consent. The deciding algorithm may be wrong, end-responsibility can be unclear, people can feel manipulated. Those ethical aspects are not well known but could heavily influence the use of this technology.

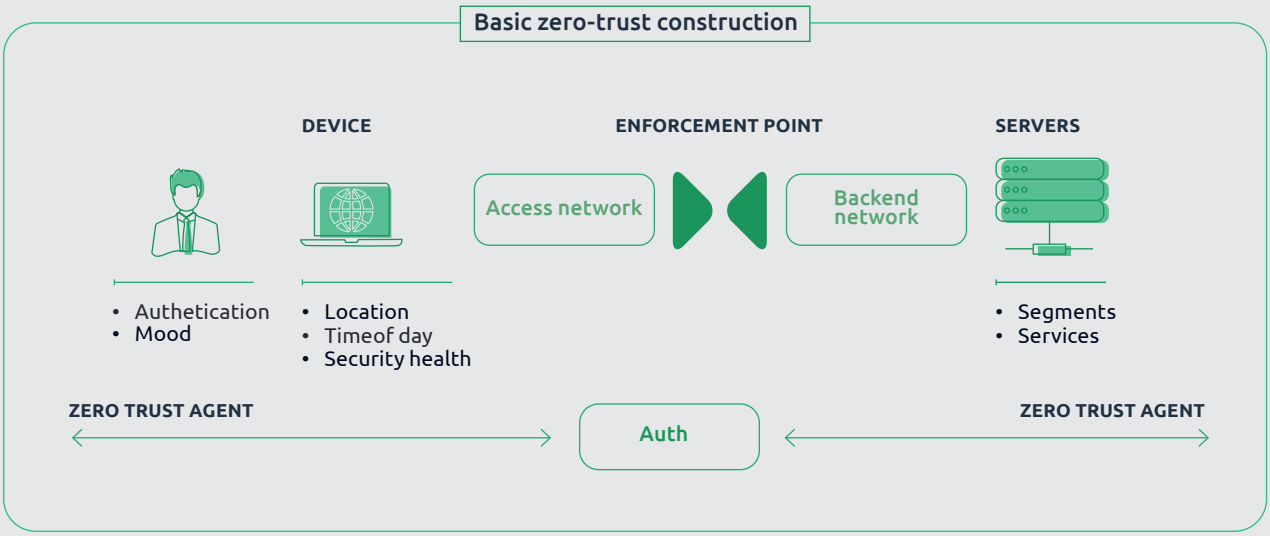


Figure 13: Basic zero-trust construction

In theory, granting access rights is not too hard, but the sheer volume of applications and the granularity of possible authorizations can make it difficult. A midsize company can easily have 600 applications, varying from modern cloud-based and commercial applications to homegrown legacy systems comprising about 50.000 different access rights that need to be neatly organized, all in line with the aforementioned principles. Granting appropriate access rights in such an environment requires adequate business-driven authorization schemes to decide which access is required to be able to execute required tasks, and which risk profile is acceptable.

The infrastructure that supports the applications mainly consists of systems that are predominantly connected by the networks that are in the same area (e.g., a cloud environment or a local network). Having access to one system will – implicitly - provide access to the same network area and subsequently to all systems in that same area. This poses a threat of lateral movement of access rights, which can be solved by splitting networks into several parts (network segmentation). In the optimal situation, there is a segment for every application (micro segmentation). Such an infrastructure provides options to restrict access to an application on a network level.

Granting access rights always starts with an assessment of attributes. In a zero-trust environment, more attributes of a user are assessed than would traditionally be the case, including attributes such as:

- the user (only user id/password or stronger using tokens, fingerprint).
- the security of the device being used (patch level, security features, hardened).
- the time of day (within business hours, overtime range, nightly, weekend).
- the network being used (private owned, public).
- the location (office, home, public place).

Assessing all those elements will result in a risk score. This score is then compared with the vulnerabilities of the requested access. Based on the outcome, the right level of access can be tailored.

The access conditions which are needed to validate if access to applications or data can be granted, require a good understanding of business use cases. An example might clarify this. When the access risk is between 3 and 4, a financial transaction is only allowed up to a limit of 500 euros and only to existing relations.

Granting, limiting, or even denying access to employees, clients, or business partners is not to be taken lightly. On the one hand, the work that needs to be done requires sufficient access; limiting or denying access without a proper reason can lead to serious loss of revenue. On the other hand, granting access can pose risks that also can lead to serious damage.

To determine the right access, business rules need to be considered. This will be new to business managers, and a well-designed zero trust architecture will aid business managers in achieving this decision-making process.

To illustrate how this works in practice, we have provided a few examples:

Ursula is using her company laptop and logs in from the hotel room. She uses the company smartphone as her Wi-Fi hub. Her risk profile could look like this:

1.Authentication: good, user id/ password combined with token-based VPN.

2.Device: good, company-managed device, not compromised.

3.Time: good, it is 15:00, so normal working hours.

4.Network: good, traffic routed over a reliable network facility.

5.Location: moderate, hotel room means confined space, but adversaries might have visible access.

6.Required Access: CRM application for entering vulnerable client-specific information but no specific deal information; compromise will lead to minor losses.

Ursula can access the application. When the Wi-Fi suddenly switches to the Hotel Wi-Fi network, access to the CRM application is denied, and she can only access her email and standard office applications.

This example is reasonably straightforward and can be realized using static rules.

A more complicated scenario requires an Artificial Intelligence functionality to help convert the dynamic risk profile to a dynamic functional business profile.

Ursula is abroad to close a deal with a new customer. She succeeds, receives the formal approval-email at 20:00 and happily enters the new customer in the CRM environment and subsequently wants to enter the deal information in the financial system.

Now the risk profile changes to:

1.Time: moderate, it is 20:00, within overtime working hours range.

2.Required Access: CRM application for entering vulnerable client-specific information including deal information, compromise will lead to a moderate loss, access to the financial system can lead to major loss.

In this case, the AI engine recognizes the usual behavioral pattern for Ursula entering a new client. Considering the overall risk posture, the AI requests her to do a "Step-Up" authentication to really make sure it is Ursula. When she enters the correct information, the AI grants her access to the financial application, which allows her to enter the new client information but denies her access to all other financial information.

This approach supports the conversion of complicated technical-oriented risk profiles to business decisions of granting/revoking access at an appropriate granularity level.

Although this seems like a reasonable approach, a complication can arise when a decision to deny or grant access is challenged. An audit trail of all decisions and the reason for those decisions needs to be available to answer the challenges. This could prove to be difficult in such a rapid changing environment where microsegments are constantly being changed and AI engines are learning behavioral patterns all the time. This could easily lead to different outcomes given the same scenarios. Solving this 'challenge' situation requires thorough knowledge of zero trust concepts and the business, including legal regulations.

Zero trust architecture-based solutions are getting mature, and it is time to reap the benefits at business level. An emerging trend shows technology leaders are becoming aware of the advantages that the zero-trust architecture can bring. AI engines can help create clear decision-ready policies out of a complex manager to fully understand the conditions and risks that they run pursuing commercial business goals.

The underlying mechanism in a zero-trust environment with the aid of AI will ensure that these conditions will not put the customers or the business at risk while at the same time ensuring that commercial targets can be achieved.

About the authors:

peter.hoogendoorn@capgemini.com

Peter Hoogendoorn

Peter Hoogendoorn is an IAM solution architect at Capgemini with a passion for innovative answers to modern questions. He has a background in information security and IAM. With 20+ years' experience he is leading the IAM centre of excellence and bring sustainable IAM solutions to Capgemini clients.

paul.pelzer@capgemini.com

Paul Pelzer

Paul Pelzer is a security architect at Capgemini with a strong background in infrastructure. He uses his experience (+30 year) to help customers to create their infrastructure in a secure way and keep it secure during its usage. His activities cover technology, processes, and organization.

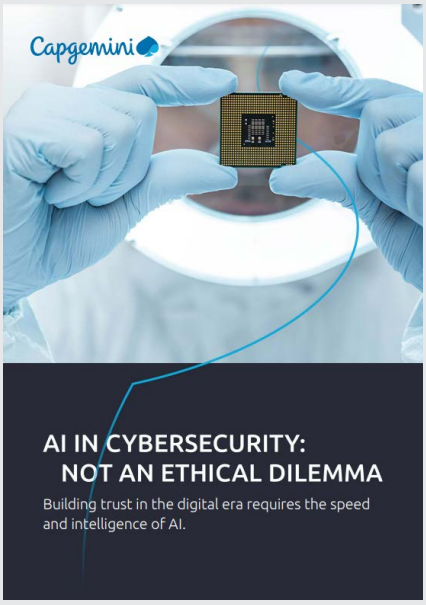
jasper.vander.vaart@capgemini.com

Jasper van der Vaart

Jasper van der Vaart is a security architect with a background in Physics and computer science. He is an innovator, capable to design simple solutions in complex environments.

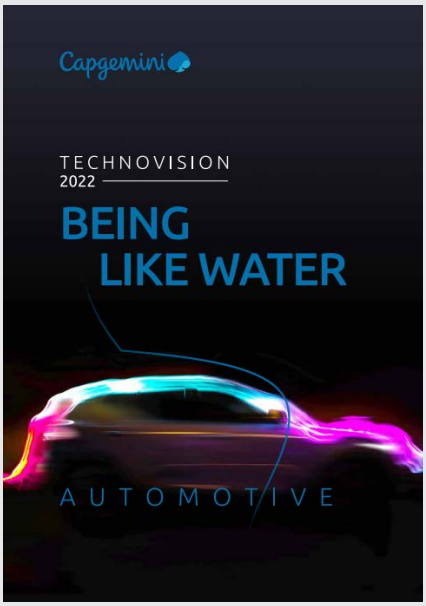
Publications

In addition to the Trends in Cybersecurity report, we publish other reports, studies, and white papers that may be relevant to you. Below you will find an abbreviated overview. To complete overview can be found at www.capgemini.nl



AI in cybersecurity not an ethical dilemma

The debate about the ethical implications of applying AI to business processes is legitimate and important. We have all experienced both the benefits and the unintended consequences of AI in our day-to-day lives. The thought of applying this powerful technology to the protection of our personal information and our corporate data should give us pause. This paper takes a closer look at why companies must harness AI as the first line of defense, and why the use of AI is not only ethical but morally imperative.



TechnoVision 2022 – dive into automotive innovation

Being like water covers a multitude of disruptions that are shaking the automotive industry. Customer expectations are changing. Products are evolving. Ecosystems are growing. Technology continues to redefine drivers' relationships to their cars. And cultural disruptions reflect the need for manufacturing companies to embrace the very different world of software development. TechnoVision for Automotive 2022 dives into each of these areas with up-to-date details on a host of developments in the automotive world.

Trends in Public Security 2021-22

How safe do citizens in the Netherlands feel today, and how should organizations in the security domain respond to changing threats and new technologies? The changing needs of citizens come at a time when new technology is exploding onto the market with a fully digitalized landscape fast approaching. More efficient and effective ways of ensuring public security using data and information are being sought. Intelligence-led operations are leading the way for the future – which will be particularly useful in the world of cybercrime where a single perpetrator is able to harm hundreds of victims within a matter of hours. With intelligent solutions comes speed, and this is a crucial aspect of public safety whether in the physical or online worlds.

Future role of the CISO: Basement or Boardroom

The research highlights how the role of the CISO and the way in which they are perceived by the business is changing. This road map shows how CISOs, business managers, and transformation leaders can build on that change in perception and establish security as a business enabler; it also looks into how Covid-19 presents an opportunity to pull these various business units together under a “trust purpose,” the effect of which will persist in your organization for a decade.

Colophon

This report has been prepared in collaboration with

Barbara Timmer, Bart van Riel, Dennis de Geus, Marieke van Putte, Matthijs van der Wel, Mohit Sikka, Natasja Pieterman, Nicolas Castellon, Rudi Gorsic, Storm Poot and Thomas de Klerk

Advice, design, and production

Marketing & Communication
Capgemini Nederland B.V.
Johanna Achterberg &
Arindam Dey

Capgemini Nederland B.V.

Postbus 2575 – 3500 GN Utrecht
Tel. +31 30 689 00 00
www.capgemini.nl

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of 325,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fuelled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2021 global revenues of €18 billion.

Get the Future You Want | www.capgemini.com

For more details contact:

Capgemini Nederland B.V.
P.O. Box 2575, 3500 GN Utrecht
Tel. + 31 30 689 00 00
www.capgemini.com/nl-nl

1A-001.22