WHITE PAPER

LACK OF CYBERSECURITY RESOURCES: WHAT SOLUTIONS?

GLIMPS

TABLE OF CONTENTS

Working from home and the complexity of IT systems:

a favourable context for cyberattacks

A little over two years since the pandemic began, it is time for an initial assessment. The roll-out of working from home, the use of the cloud, increasingly complex IT environments... Managing an information system (IS) requires larger-scale use of a new generation of tools, such as SOCs and SIEM.

The fundamental trend seen over the last few years remains in place: critical incidents within organisations are growing steadily. In 2021, 54% of French companies suffered attacks and ransomware expanded by 95% [Cybermalveillance.gouv.fr, 2022; CESIN, 2022; Stoïk, 2022]. All organisations and all sectors are affected, leading to major changes in the cybersecurity approach taken by IT departments.

A pandemic context helping to lower security barriers from 2020

How can we explain what looks very much like a cliff-edge? The context has often been mentioned – rightly – as an explanation for the change [Deloitte, 2020]. From the first months of 2020, the global Covid-19 pandemic led to working from home on a massive scale, and thus to greater use of the internet. In every home, there was a new intermingling of the professional and personal worlds. Companies had to review their organisations and overcome many barriers. The result was immediate: previously imagined as a castle, the information system (IS) saw its protective walls crumble and IT security became more fragile. As early as June 2020, the National Cyber Security Centre showed that 350 cyberattacks (phishing, direct attacks against organisations, infected websites etc.) had been recorded in Switzerland in April alone, compared with 100 to 150 previously. Comparable trends were seen across Europe and in North America, where almost one employee in two (47%) was caught by phishing attacks [Tessian, 2020].

Increasingly complex IT environments

This context had major repercussions for the technical evolutions that were still in their early stages in organisations at the time. The pandemic and the resulting changes in working practices helped to accelerate the trends that were emerging, related to the growing complexity of IT environments. New tools, new services, new applications... Organisations have made more and more use of specialist products in the quest to perfect their IT systems. This proliferation of new tools and applications has altered the strategic picture: now IT departments have to ensure the security of every component, or risk imperilling their whole IS... A real challenge, which 44% of companies see as fundamental [McKinsey, 2020]. Ranking second in the list of organisations' priorities (after data protection), this security has a considerable cost and requires companies to make major efforts. In nearly eight out of ten cases (78%), cybersecurity and IT experts agree that the security of remote workers is increasingly difficult to guarantee (Splunk, 2022].

Shortage of cybersecurity engineers

Observers know that the growth of the cloud has its part to play in the increasingly fine-grained and technical nature of information systems, not to mention their growing complexity (see box). This development is combined with a structural shortage of professionals. In France, the deficit in engineers specialising in cybersecurity led to the launch of a national government-backed plan launched in autumn 2021 [Les Echos, Sept.2021], shortly before the opening of the Campus Cyber in February 2022.

Leading global player Microsoft claimed recently that this lack of human skills constitutes the main obstacle in IT security. "We are short of nearly 15,000 cybersecurity experts in France, and we are looking for an extremely wide variety of profiles,» declared Jean-Christophe Pitié, COO of Microsoft France [Clubic, 2022]. The same trend can be seen in other countries across the world [ICS2, 2021] and is likely to become more deep-seated in the coming months and years. According to forecasts, the cybersecurity sector in France will see growth of eight to ten percent over the next five years [Les Echos, Sept. 2021].

Sophistication of attacks

The growing sophistication of attacks is the other major current phenomenon. Situational in nature, it is based on very advanced, continuous, clandestine hacking techniques used to reach the heart of the information system and remain there for a long time. While they particularly target high-value organisations (states, multinational groups etc.), these APTs (Advanced Persistent Threats) by extension affect all organisations, public and private, regardless of their size and sphere of activity. Their goal is to sneak out large amounts of valuable information over a long period through lateral movements that reveal the vulnerabilities of the IS from the inside. They are added to the long list of threats to business cybersecurity, with the human factor as an essential element...

Faced with this new context, companies are taking action. Deployed over the last few years, SOCs (Security Operations Centres) and SIEM (Security Information and Event Management) are among the solutions now being put in place. Offering businesses a new generation of detection, analysis and response features, they involve both technical and organisational issues within the company and relate to its global strategy.

The «cloudification» of information systems

Between 2019 and 2021, use of the cloud rose from 72% to 88% for both private and public organisations, and virtual offices gained four percentage points (86%). This raises major challenges in terms of security: the more complex the infrastructure, the more it proves vulnerable. This makes it harder to identify an attack, and even more so to respond.

According to an analysis by Kaspersky, six organisations out of ten estimate that the lack of visibility over IS infrastructure is the most common challenge they currently face [Kaspersky, 2020].

Cyberattacks: a cost for organisations

Growing in number over the last two years, cyberattacks are increasingly seen by businesses as the biggest threat to their activity. In 2022, one company in ten reported falling victim to ransomware, and 62% of the organisations affected admitted paying the ransom demanded [Hiscox Cyber Readiness Report, 2022]. In addition to the ransom amount, the Hiscox insurance company puts the average cost of a cyberattack at €51,000 for a medium-sized company. This amount includes both the direct costs (technical investigation, notifying clients, securing data following the incident, public relations, regulatory compliance, lawyers' fees, legal costs, improving cybersecurity systems) and indirect costs (business disruption or interruption, loss of intellectual property, loss of trust, damage to brand value, increased insurance premiums and cost of borrowing). The figure is of course higher for mid-market companies and still higher for major groups.

SOC: issues that are partly technical...

but mostly human!

Faced with increasingly frequent and increasingly technical malicious attacks, SOCs and SIEM offer global visibility over incidents. They also require organisations to consider major questions in terms of human organisation.

Repeated malicious attacks, complexity of information systems, growth of cloud technologies and working from home, globalisation of professional relationships... In the last few years, organisations have been opting for the deployment of SOCs (Security Operations Centres). The purpose of an SOC is to detect, analyse and intervene if a cyber incident occurs. To achieve this, the SOC employs a subtle coordination of technological systems and processes. It also relies on a dedicated human organisation and requires detailed thinking before deployment.

A combination of technological methods

The technical design of an SOC involves choices that need to be made about tools and the contracts to be signed. A whole set of questions arises at this stage. With regard to data collection, the tools that compose the existing IS need to be identified and located: IDS/IPS, firewall, data leak detection, encryption systems, antivirus, anti-spam, access control and authentication...

Each tool has its own role and its own security objectives. When it comes to supervision operations, a design study is required to refine the choice of the primary tool and its associated satellites. The goal here is to receive, sort, qualify, prioritise, monitor and process security incidents. These steps need to be adapted (and adaptable) to the specific situation in the organisation, whether it operates in the private or the public sector. In particular, they involve considering compatibility with the SIEM (Security Information and Event Management) solution in place, evaluating the ability of the SOC to prioritise incidents based on a scale of severity for the company, gauging the adaptability of escalation and communication pathways and planning exchanges and interactions with other SOCs.

These choices inherent in the technical tools are combined with others, associated with processes

and the rules governing information system security. Organisational in nature, these processes include crisis management, duty rosters and escalation. They guarantee that the SOC is integrated fully into the organisation's overall IT processes.

A specific human organisation

These processes necessarily depend on the underlying human organisation. Led by an SOC manager, teams are specifically dedicated to detection, analysis, response, reporting or preventing cybersecurity incidents. They generally consist of level 1 and 2 analysts, together with cybersecurity engineers (level 3).

Level 1 and 2 analysts could be seen as «hunters». Their everyday motivation is to flush out attackers via advanced investigations. They observe and interpret the alerts reported by the supervision centre, analysing SIEM security logs and network flows and establishing correlation rules to detect and manage incidents. These analysts also monitor threats and vulnerabilities (drafting alert bulletins) and carry out reporting and documentation activities (contributing to activity monitoring reports and the SOC's document library).

Meanwhile, level 3 security engineers draw on more advanced expertise, relating to attack methods for example. These specialists are able to examine weak signals, carry out exploratory research into all the events they face and perform reverse engineering. As well as technical knowledge, they require strong people skills and analytical abilities.

The SOC manager takes care of the overall management of all the analysts. The manager is the keystone of the SOC's Service Level Agreements, guaranteeing that processes are applied properly (incident management, processing optimisation, change request follow-up), ensuring consistency and taking responsibility for the SOC's technical strategy. It is the SOC manager who defines and monitors performance indicators and sets up dashboards, leads reviews (weekly, monthly) and drafts activity reports and pre-formatted alert messages.

Far from being a basic «plug and play»-type process, installing an SOC within an organisation thus requires a high level of prior thought and a methodical approach. What governance will be put in place? Protective measures? Detection and response methods? Remediation and reconstruction in the event of a successful attack? All these major questions have to be backed by a high-level internal sponsor, because the deployment of an SOC is a large-scale cross-company operation. But above all, the human factor must be taken into consideration, given that the long-term everyday actions of the SOC teams are of crucial importance for the security of the company, and thus its long-term future.

Why SOCs and SIEM are necessary

In the last few years, the deployment of SOCs and SIEM have enabled the organisations adopting this type of response to guard against the expansion and growing power of the attacks they face.
SOCs provide a response to seven specific risks:

1- The growth of the attack surface: this is related simultaneously to the rise of the cloud, the increasing complexity of digital supply chains and ecosystems being stretched further by the multiplication of assets.

2- Expansion of the digital supply chain: by 2025, specialists forecast that 45% of organisations will face attacks on their software supply chains. This represents a threefold rise over 2021.

3-More sophisticated attacks on identity and access management: the misuse of credentials has become a primary method of attack. So far, organisations have been able to provide technical responses to improve the performance of user authentication, but the cultural question around behaviour remains.

4- Increasingly diluted cyber responsibilities: faced with an expanded attack surface, organisations are confronted with the dispersion of decision-making authority and responsibilities. This complexity leads to changes in the role of the CISO, turning them from a technical expert into an executive risk manager – a complete transformation of the role.

5- Human error: this remains a factor and a challenge that goes well beyond technical progress. In response, organisations are developing awareness raising programmes. The organisations with the most exposure go further still by investing in holistic behavioural and security culture programmes.

6- Suppliers: these players are now fully integrated into their customers' digital ecosystems, increasing efficiency and reducing complexity. However, this extension also increases risk and calls for globalised responses.

7- The cybersecurity mesh: this complex approach considers the overall architecture of the IS. It is a more integrated approach that aims to secure all assets, whether they are located on-site, in the cloud or in data centres.

Source: Gartner, "Top Trends in Cybersecurity 2022", mars 2022

«The SOC improves detection and response»

The first is a cybersecurity consultant; the second occupies the role of a cybersecurity architect. Lidao Bilesah and Mickaël Sardinha both work at CAPFI, an IT outsourcing company founded in 2005 to provide consultancy, IT and security infrastructure, data science and big data, digital engineering and finance. A view from the experts.

What is an SOC and how does it work?

Lidao Bilesah: There are several definitions of a Security Operations Centre. For us, it is a whole that consists of multiple elements. What we can say first of all is that an SOC is a technical solution that enables an organisation to improve its threat detection and response. It is also a set of processes that will increase its responsiveness when an alert occurs. The SOC also improves processes. And I would add a final element: the human factor. IT departments often forget or minimise this dimension. But it is the experts who manage the alerts.

Mickaël Sardinha: The SOC teams' technical solutions are not autonomous: they need someone to manage them and lead the team. IT departments have long been used to providing basically technical responses – there was a problem, so they deployed a firewall, for example. With SOCs, human resources are more important. I would even say that the human side has never been as important as it is now in terms of cybersecurity. The administration teams have to work with the teams responsible for alerts.

How do you explain such a major change?

Mickaël Sardinha: For me, I think the biggest change has been the move towards SaaS. To begin with, this posed important problems associated with technical solutions that weren't visible. A firewall doesn't detect anything when you're working in a café... The SOC will cover the maximum attack surface: SaaS, of course, but also mobile operations, such as smartphones and tablets. While still retaining the in-house operation!

So is the deployment of SOCs linked to the increase in the attack surface?

Mickaël Sardinha: That's right. A few years ago, so-called insider hackers were the most numerous. But the cyber world has grown much larger, especially due to the pandemic. That accelerated the phenomenon, together with the rise in mobile working and SaaS. There has been a clear increase in these services: file servers, mail servers, migration to Office 365... Organisations have discovered the convenience of giving up responsibility for maintenance. But that accelerated the growth of malware...

Lidao Bilesah: With the pandemic, we have also seen that digital transformation projects have focused more on the business dimension. Again, this has led to an expansion of the attack surface for cybercriminals. They have adapted to the new context, and in many cases they have concentrated on human vulnerability. Because there is always a weakness of this type in any organisation, and it can always be exploited! In response, defence teams have also reorganised. With an SOC, they have been able to adapt to the cybercriminals' new ways of operating, and exploit information about the strategies they have developed, their techniques and tools... For IT departments, this requires time, but also specific expertise and particular profiles with the latest knowledge about threats.

Has the switch to SOCs been easy for IT departments?

Mickaël Sardinha: We should first make clear that not all organisations have an SOC or SIEM. And then this all needs to be put into the context of the internet, whose scope has expanded incredibly in recent years. There are now 1.2 billion people with access to the net. Customers and web users are everywhere, and so are potential attackers. This explosion in the number of internet users automatically escalates the numbers of vulnerabilities, incidents and mistakes. A 14-year-old can easily find some malware and do serious damage to an organisation. This all makes it essential to set up whole dedicated teams, because there's a lot of work.

Lidao Bilesah: In this context, assembling a sustainable team within the IT department can be a long and painstaking process. Every company has its own internal culture, which doesn't always include cybersecurity – though it should. Recruitment has also become very difficult: there's a shortage of skills, and the process takes a very long time. It can last six to eight months, because there are plenty of vacancies and qualified profiles are rare. But once you've hired someone, the problems aren't over: you still have to keep staff up to date technically. And there are so many subjects for training: mobile, SaaS...

Would you recommend setting up an internal SOC or an external SOC?

Mickaël Sardinha: There's no clear answer to this question, because it depends on the company. You also have to look at the implications. An internal SOC is generally relevant for big organisations or companies with significant financial resources. Because an SOC managed by an in-house team inevitably raises questions about financial and HR management: as well as the essential professional training, you have to think about career development, holidays, sickness cover... When it's in place, this can be an attractive option for the company: the experts are quick to respond and know their risk matrix perfectly and the matrix is well targeted for the company's business applications. An external SOC, meanwhile, is aimed at different organisations and meets specific needs.

Lidao Bilesah: The advantage an external SOC can offer is the fact that the subcontractor can guarantee a full, consistent service 365 days a year, seven days a week. It will also be easier for the subcontractor to respond to certain issues because they will already have encountered them in other situations. An outsourced SOC can provide better reflexes, addressing processes and responses more quickly than an in-house team. This is the most obvious solution for SMEs and mid-sized companies, especially for government subcontractors.

SIEM, a pillar of the SOC

Since they began to emerge in the early 2000s, SOCs have undergone far-reaching changes. To respond to increasingly complex and elaborate attacks, operational security teams modernised in the 2010s.
SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation and Response) undoubtedly played a part in this evolution. Over the last decade, they have made it possible to industrialise surveillance by simplifying the analysis of multiple sources of security events (such as proxy servers, antivirus consoles and firewalls) and automating responses to security incidents. SIEM also enables the (many) events stemming from increasingly numerous devices and applications to be correlated. However, SIEM and SOAR require a heightened level of skill from the teams dedicated to operational security. Staff have to avoid the pitfalls of inadequate implementations of checks or incomplete knowledge of real threat scenarios.

Towards an improved SOC 2.0 thanks to

the eXtended Malware Analysis Platform

In 2023, it is no longer enough to stick with the traditional versions of SOCs and SIEM. In response to current cybersecurity challenges, these solutions need to be consolidated with AI and Machine Learning, but also with solutions such as Reverse Engineering and the eXtended Malware Analysis Platform. Here's why.

With its historical focus on Research & Development, the French economy relies partly on the quality of its engineering. Dynamic and still with a low level of concentration, the sector receives a great deal of attention – and even protection. To guard the country's businesses against cyberattacks and continue to punch above its weight in industry 4.0, the government has recently accelerated its cyber strategy: by 2025, the sector is targeting revenues of €25 billion, three times higher than now [France 2030].

SOC 1.0: an architecture that has become obsolete

This modernisation should enable companies and public-sector organisations of all sizes in all sectors to accelerate the modernisation of their tools still further. The transition to SOC «2.0» is an integral part of this goal. Because many *Security Operations Centres* are currently based on an outdated architecture. Increasingly modern tools, new applications, IS complexity, multicloud environments and growing numbers of more powerful cyberattacks constitute a whole new reality. Working with now-obsolete detection methods, including solutions based on aggregating large volumes of logs and signature-based detection systems, «previous-version» SOCs require security analysis teams to multiply their exertions to extract data manually from a limited number of sources. The results are no longer worth the effort – they are inaccurate, remove all visibility for the SOC team and generate significant and unnecessary costs for the business.

AI and Machine Learning: automating detection

How can we detect ransomware attacks, which are increasingly based on surreptitious movements by cybercriminals within the same information system? With new SOCs and SOAR, detection is increasingly automated. Benefiting from artificial intelligence (AI) and Machine Learning, they are based on two main pillars: EDR (Endpoint Detection Response, or detection in workstations and servers) and NDR (Network Detection & Response, a solution that puts the security threat into context). These techniques provide a view of all the elements constituting the infrastructure, including both IT and IoT environments. With these new features and the automation provided by SOAR, latest-generation SOCs roll out a mesh of surveillance across all the assets in the physical environment and in the cloud. This more modern form of SOC enables teams to focus their attention on the attacker's methodology, and their behaviour more specifically, rather than the use of the attack (signature). This makes it possible to detect attacks that have never been seen before.

Concept code: recognising new threats

But however modern these new technologies are, they are still a long way from being able to detect Advanced Persistent Threats (APTs) or to uncover the sequence of actions that leads to damage to the IS.

To quote the specialist Olivier Gesny, innovation director at PR0PH3CY (formerly Silicom), in Revue Défense Nationale, *"Cyberdefence has to expand its capacity for action and perception if it is to meet attackers with greater scope for action on an equal basis"* [Revue Défense Nationale, 2019].

The eXtended Malware Analysis Platform is undoubtedly an element that already enables SOCs and SIEM to take a significant step forward in terms of detection and response (*see following pages*). What is unique about this tool is its global view over the whole information system, including the use of concept code. This technology plays a specific role by automatically identifying the «narrative» of a piece of malware, its grammar. «*We recognise new threats by the ways in which malware is coded*», explains Frédéric Grelot, Vice President for Research at the start-up GLIMPS and one of the engineers behind the invention.

[Infoprotection, March 2022]. «*To be more specific, we use Deep Learning to recognise, not new viruses themselves but their 'concept codes', i.e. the way the algorithm is coded: code for network communications, encryption, Bitcoin payments etc.*».

And it works! Faced with files that are both numerous and widely scattered, concept code offers centralised, relevant information that enables the eXtended Malware Analysis Platform to collect the significant details that will help security teams perform better.

Disassembling the code: the contribution of Reverse Engineering

Code conceptualisation is based on automatic Reverse Engineering. This involves disassembling the code, or translating it into understandable language, in order to identify its concepts. This process takes place in several stages, which are similar to the way a human learns to read, starting with learning the letters of an alphabet in order to form phrases and then learning the grammar. The end point of the learning process is the ability to assimilate the story being told, with all its different concepts and ideas.

Concept code: it's all about stories, including children's fairy tales!

The analogy between concept code and the fairy tales we tell children helps explain the characteristics of this new technology. Because although fairy tales tell the same set of stories (from Goldilocks to Red Riding Hood), they are adapted for children in all cultures and many different languages. This is where concept code is special: it focuses on the story being told, rather than the words and the grammar used to tell it. This means the technology can identify scenarios that are 80, 90 or 95% identical in several types of malware, despite them being written differently. The story is at the heart of concept code, in the same way as the story is the basis of the emotions children feel in response to fairy tales and legends.

Focus on a new concept:

the eXtended Malware Analysis Platform

Though they remain reliable in terms of detection, SOCs as automated solutions are proving more and more limited. A new tool is emerging: XMAP, or eXtended Malware Analysis Platform, in a more expansive version than the current sandbox environments.

Specialists know and use the many positive aspects of SOCs. Combined with SIEM and SOAR, Security Operations Centres collect and analyse data to enable corrections to be made. But in some cases these SOCs are poorly equipped with solutions, leading to holes in the detection safety net. Detection thus becomes too diverse... "*Today, an SOC has to collect files from all over the place - sandboxes, NAS etc.– and thus becomes dispersed. Alternatively, it will use multiple antivirus systems, which leads to significant costs for the business,*» warns Frédéric Grelot, an engineer at the start-up GLIMPS.

Malware Analysis Platform: a global solution

This observation calls for the development of a global solution: the Malware Analysis Platform. Its central feature is its ability to centralise solutions and data, giving the IT department comprehensive visibility over everything that is happening within the architecture of the information system.

To move towards this result, many IT departments are currently opting for the new solution of the sandbox. Referring to a tool that enables malware to be executed in order to observe its behaviour and extract indicators, this option offers security teams the option of dynamic execution. "*But the sandbox proves very expensive, requires long execution times and generates either very little information, or huge amounts. The result is that in the best case you are drowning in information, and in the worst you have too little...*» explains Frédéric Grelot.

The contribution of concept code to an eXtended Malware Analysis Platform

Ultra-rapid, comprehensive detection is still possible thanks to concept code. This emerging technology, which can be combined with a sandbox or an SOC, can detect the widest possible range of attacks in record time.

«With the SOC, we have a tool... but we lack reliability of detection and the global, inclusive dimension of an advanced analysis based on automation. All these elements are provided by the concept code solution,» continues Frédéric Grelot.

A feature of this new solution, which is associated with the notion of the eXtended Malware Analysis Platform, is that it systematically, reliably reports the information to the SIEM and SOAR (Security Orchestration, Automation and Response)systems to generate the analysis. The whole operation takes place in record time – four to five seconds, compared with several minutes (or even hours) for current solutions. As soon as detection takes place, the advanced analysis is ready! This speed can be life-saving for companies and public-sector organisations, especially in the current context.

Towards a dedicated detection and analysis role?

This shows how far detection and analysis are in the process of becoming the two themes of a distinct professional role, based on high-added-value automation skills and technologies. In this case, outsourcing these skills appears essential. Rather than referring to the partial, fragmented knowledge of a set of players scattered throughout the IT ecosystem, it seems increasingly obvious that the future will involve empowering a dedicated role centring on malware detection and analysis. This brings us to the concept of XDR, a tool for security threat detection and incident response based on the SaaS model.

Specific to each supplier and natively integrating a set of security products in a coherent system of security operations, XDR unifies detection and offers security teams *"flexibility, scalability and opportunities for automation"* [Forrester Research, Palo Alto Networks]. Based on partnership between a set of specialist players, this type of platform has recently been applied in France with the «Open XDR Platform», created at the time of the Assises de la Sécurité 2021 event (*see box*). Its chief benefit is the automated reception and processing of alerts.

A more efficient human organisation

This level of specialisation and technical complexity can only have a beneficial effect on in-house IT teams. Confronted with increasingly elaborate ransomware, using tools with multiple entry points and subject to a growing plethora of information, IT engineers are required more and more to rely on time-consuming manual solutions with highly uncertain results. Sometimes deprived of resources and subject to high levels of stress, they can relieve their daily workload with solutions based on Reverse Engineering, concept code and AI. «*It's clear that IT departments can save a lot of time by relying on artificial intelligence and Machine Learning,*» concludes Frédéric Grelot. *"These new solutions apply human thought to truly consolidated, globalised, comprehensive data. They enable the organisation to respond better to incidents.*» Ultimately, they can also represent significant budgetary savings while ensuring optimum protection.

Concept code: a scientifically valid technology

The concept code technology was recently described in a scientific paper [C&ESAR, 2021]. Written jointly by Frédéric Grelot, Marie Salmon and Sébastien Larinier, the article compared two methods of binary analysis: manual analysis by experts from the ESIEA digital engineering school, and automatic analysis by engineers from the start-up GLIMPS. Ultimately, the automated search and the concept code technology were validated by the manual academic approach: the comparison showed that automation using reverse engineering is not only reliable, but also much quicker than the conventional approach.

Open XDR Platform: a complete cybersecurity offer in France

During the Assises de la Sécurité 2021 event, several French players announced the launch of the Open XDR Platform. A trusted platform in the field of extended detection and response, it is based on collaboration between seven participants and constitutes a sign that the French cybersecurity ecosystem is working hand in hand to confront the major threats affecting organisations. The participating players include HarfangLab (ANSSI-certified EDR solution), the French National Information Systems Security Agency (ANSSI), SEKOIA.IO (a Cyber Threat Intelligence building block), Pradeo (Mobile Application Security Testing), Vade (email filtering), Gatewatcher (Network Detection & Response), Wallix (access security) and GLIMPS (eXtended Malware Analysis Platform). According to Grégoire Germain, the founder of HarfangLab, «*the building blocks are independent and customers can choose them to suit their needs*" [Lemondeinformatique.fr]. Ultimate goal: to offer a trusted platform to private companies and public organisations.

GLOSSARY

Concept code:

Code conceptualisation is a recent technology that involves automatically identifying the narrative of a piece of malware. Once it has been disassembled through Reverse Engineering, the code delivers up the story it contains, going beyond the numbers that constitute its words and their grammar. Concept code can thus be used to establish that a story is 5%, 10% or 15% identical to another, enabling the spread of malware to be stopped in its tracks.

EDR:

EDR (Endpoint Detection & Response) software is a security solution designed for «endpoints» (physical devices communicating with networks). It overcomes the deficiencies of certain antivirus systems by detecting unknown attacks and initiating automatic corrections. Advanced features enable EDR to carry out remote investigations.

Artificial intelligence:

AI is a set of technologies that work together to enable machines to perceive, understand, act and learn with levels of intelligence tending towards that of humans. It includes several strands of technology, such as Natural Language Processing (NLP) and Machine Learning (ML).

Machine Learning:

Machine Learning is one of the themes of Artificial Intelligence, a subcategory of AI aiming to automate the process of creating analytical models. Machine Learning enables machines to adapt autonomously to new scenarios. One example of its use is the intelligent management of Big Data, which is a vital asset in malware research.

NDR:

An NDR (Network Detection and Response) solution deals with security threats by putting them in context. To do this, it analyses network traffic and inspects communications in real time. Threats are thus detected and dissected, especially risky activities or abnormal behaviours. This solution can prove useful if an organisation's alarms are poorly contextualised.

Reverse Engineering:

A technique by which a system can be disassembled. In the field of computer systems, this study and analysis can be applied to malware. Software Reverse Engineering involves disassembling the machine code of malware to reconstitute the original source code as it was written. With this source code, Reverse Engineering can identify the malicious content of a program.

GLOSSARY

SaaS:

Standing for «Software as a Service», this term refers to an application solution hosted in the cloud and operated by a third party outside the organisation (private company or public body). This model includes a multitenant architecture that enables users and applications to share the same infrastructure and code base, with maintenance being centralised. SaaS facilitates personalisation, software updates and better access. It eliminates the costs of acquiring equipment, supplies, maintenance, licensing and support.

SOC:

A Security Operations Centre is a platform for supervising and administering information system security. It includes tools for collecting and correlating events and intervening from a distance. It consists of the technical equipment and the dedicated staff needed to guarantee the supervision of IT security and to intervene as quickly as possible if an incident or attack occurs.

SIEM:

Security Information and Event Management enables the management of events and information about an organisation's security. Based on comparing events with rules, analysis engines, indexing and analysis, SIEM represents a new generation of detection, analysis and response functionalities for all organisations. Historically, SIEM is the tool used by SOCs to monitor an organisation's infrastructure.

SOAR:

This term stands for Security Orchestration, Automation and Response. As the name suggests, it refers to a tool for orchestrating and automating responses to IT security incidents.

XDR :

This acronym (standing for eXtended Detection and Response) refers to a tool for collecting and correlating data located at several levels: email, endpoint, server, cloud and network. XDR thus enables threats to be detected more quickly and saves time on investigating and responding when the security analysis is carried out.

BIBLIOGRAPHIC REFERENCES

BOERO Alexandre, « *Il manque plus de 15 000 experts de la cybersécurité en France* », Clubic, 21 juin 2022
https://www.clubic.com/pro/entreprises/microsoft/actualite-427680-il-manque-plus-de-15-000-experts-de-la-cybersecurite-en-france-microsoft.html

CESIN, *Baromètre de la cybersécurité des entreprises*, 7e édition, année 2021, 17 janvier 2022
https://www.cesin.fr/actu-7eme-edition-du-barometre-annuel-du-cesin-enquete-exclusive-sur-la-cybersecurite-des-entreprises-francaises.html

CYBERMALVEILLANCE.GOUV.FR, *Rapport d'activité 2021*, 8 pars 2022
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2021

GARTNER, *Top Trends in Cybersecurity 2022*, mars 2022
https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

GESNY Olivier, « Capter l'IA de demain au regard des enjeux de cyberdéfense », *Revue Défense Nationale*, 2019/5, n° 820, pp. 38-42
https://www.cairn.info/revue-defense-nationale-2019-5-page-38.htm?contenu=article

GRELOT Frédéric, LARINIER Sébastien et SALMON Marie, « Automatisation de l'analyse des binaires : de la collecte source ouvert à la Threat Intelligence », 16 novembre 2021, salon C&AESAR 2021.
URL : https://conf.researchr.org/details/cesar-2021/call-for-papers/14/Automatisation-de-l-analyse-de-binaires-de-la-collecte-source-ouverte-la-Threat-I

HISCOX Assurances, *Rapport 2021 sur la gestion des cyber-risques*, avril 2021
https://www.hiscox.fr/courtage/blog/rapport-hiscox-2021-sur-la-gestion-des-cyber-risques

BIBLIOGRAPHIC REFERENCES

KASPERSKY, *A Resilient Cybersecurity Profession Charts the Path Forward*, (ISC)2 Cybersecurity Workforce Study, 2021
https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

MOTELLA Clotilde, « Le coût réel d'une cyber-attaque pour votre PME », SFR Business, 19 octobre 2021
https://www.sfrbusiness.fr/room/securite/cout-reel-cyberattaque-pme.html

PALO ALTO NETWORKS, « What is XDR ? », 2018
https://www.paloaltonetworks.com/cyberpedia/what-is-xdr

PERELAFOUINE, « La transformation du SOC », 20 juin 2022
https://perelafouine.com/la-transformation-du-soc/

PWC, « La cybersécurité fait face à une pénurie de talents constante »,
https://www.pwc.fr/fr/decryptages/securite/la-cybersecurite-fait-face-a-une-penurie-de-talents-constante.html

STOÏK, « La tendance à l'aggravation de la cybercriminalité se confirme », 28 avril 2022
https://www.stoik.io/cybersecurite/chiffres-cles

Web : https://www.glimps.fr/en/
Linkedin : https://linkedin.com.company/glimpsre
Twitter : https://twitter.com/GlimpsRe
Email : contact@glimps.re