SECURITY AT MACHINE SPEED

Auteurs:
F. Fransen
R. Kerkdijk
N. el Ouajdi

TABLE OF CONTENTS

1. INTRODUCTION

Across the world, overarching global trends dictate the security market. These trends are primarily driven by business developments like digital transformation, and technology developments such as the dynamic cyber landscape. Market participants have little control over trends like these. And yet they are compelled to adjust to them in order to maintain viability and protect or grow market share.

As the digital economy grows, it is essential to keep the safety and resilience of society in mind, and to protect its citizens and businesses. In recent years, companies—and in particular enterprises and SMEs—have embraced digital transformation and adopted ICT solutions to improve their operations. But the cyber landscape has evolved rapidly in the past few years. Current practices and solutions simply do not suffice to protect organisations from the persistence and sophistication of professional threat actors. Despite significant investment in cyber defence, most organisations are unable to keep pace with the ongoing evolution of threats and attack methods.

The Ukrainian Cyber Attack in 2015[1] and A.P. Moller—Maersk Cyber Attack in 2017[2] are examples of the huge impact these attacks can have on society, and the financial losses an organisation can suffer. The primary cause of the Ukrainian blackout was that an attacker (or group of attackers) managed to infiltrate the corporate IT networks of the targeted Distribution System Operators through phishing techniques. This interrupted the electrical supply of approximately 225,000 customers.

In June 2017, A.P. Moller—Maersk fell victim to a major cyber attack caused by the NotPetya malware, which affected many other organisations across the globe. As a result, Maersk's operations in transport and logistics businesses were disrupted, leading to financial losses of around USD 300 million. That includes, among other things, loss of revenue, IT restoration costs and extraordinary costs related to operations. Maersk's container ships stood still at sea, and its 76 port terminals around the world ground to a halt.

Meanwhile, the growing cyber landscape and changing IT architectures are driving the need for experienced security professionals. But the availability of these professionals is scarce. As it stands now, the widening gap between defenders and attackers will only continue to grow in the coming years.

This trend can only be stopped through a fundamental game-changer. TNO believes, that a combination of human expertise and technological advancements—like machine learning and Artificial Intelligence (AI)—hold the key. Specifically, that includes automating some security tasks that have traditionally been done by humans and designing better decision support and visualisation tools. These are the keys to improving the odds and protecting ourselves from the inevitable and continuous onslaught of threats.

[1] SANS/E-ISAC White Paper; 'Analysis of the Cyber Attack on the Ukrainian Power Grid'; 18-03-2016
[2] http://investor.maersk.com/news-releases/news-release-details/cyber-attack-update

2. THE NEED FOR AUTOMATION

As cyber attacks become more sophisticated, and their disruptive effects on business and society increase, large organisations that depend strongly on ICT have gradually elevated their defences. Strategies typically include an increased focus on security monitoring and incident response capabilities. This often includes dedicated Security Operations Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs). To further strengthen their resilience to cyber attacks, many organisations have subsequently complemented this with Cyber Threat Intelligence (CTI) and threat-hunting practices. While this has arguably increased defensive capabilities, threat actors have also been stepping up their game, and have consistently managed to come out ahead. Among many other sources, ENISA's Threat Landscape Report of 2017[3] expresses this clearly:

> 'The cyber security community is still far from striking the balance between defenders and attackers.'

and

> 'The increased defence levels and expenses cannot successfully reduce levels of cyber threat exposure.'

The Dutch NCSC reported similar observations in its Cyber Security Assessment for the Netherlands. The assessment shows that a principal cause of ineffective security is that defensive practices (as outlined above) tend to rely heavily on human effort and expertise. In today's complex ICT infrastructures, detecting and comprehending threat actor activity requires the digestion of large volumes of information, including all security events that occur in the organisation's infrastructure and threat intelligence collected from external sources. A human analyst will usually need some time to piece things together and prepare appropriate measures.

By contrast, advanced attacks are often automated to such a degree that they can (largely) be executed *at machine speed*. This imbalance has rather visible effects in operational practice, where the time needed to compromise a system is typically very short: seconds to minutes. Yet the time needed to discover a breach is more likely to be weeks, or even months. What's more, the actual containment of an attack may again take weeks[4]. As ICT infrastructures become larger and more complex, an analyst's workload will likely increase even further. Meanwhile, recent studies reveal an increasing shortage of qualified security staff[5,6]. So even if budgets allow it, SOC and CSIRT teams will have limited possibilities to simply expand their expert resources. To make a meaningful change, the most—if not the *only*—viable way forward is to *automate security (operations) duties*.

[3] Threat Landscape Report 2017, ENISA, Final Version 1.0, January 2018, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

[4] 2018 Data Breach Investigations Report, Verizon, 11th edition https://enterprise.verizon.com/content/dam/resources/reports/2018/DBIR_2018_Report.pdf

[5] Cybersecurity Talent: The BIG GAP in Cyber Protection, Capgemini Digital Transformation Institute, February 2018, https://www.capgemini.com/resources/cybersecurity-talent-gap/

[6] Cyber Security Assessment Netherlands 2017: Digital resilience is lagging behind the increasing threat, National Cyber Security Center, August 2017, https://www.ncsc.nl/english/currenttopics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2017.html

3. CURRENT MARKET SOLUTIONS

Several cyber security vendors have already identified the need to automate security operations. This is evidenced by the introduction of so-called Security Orchestration, Automation and Response (SOAR) products. Also known as Security Automation and Orchestration (SAO) products, these solutions allow security operations teams to define *standardised* incident response *playbooks* and subsequently automate specific steps in the playbook to a greater or lesser extent. SOAR products can typically be integrated into:

- **Security monitoring solutions**, to allow direct response to security events occurring in the organisation's infrastructure,
- **Cyber Threat Intelligence platforms**, to follow up on new threat insights, and
- **(Technical) security controls**, to mitigate a threat or ongoing attack.

Playbook-driven security automation and orchestration will relieve SOC and CSIRT specialists from routine tasks, and will likely contribute to reducing the organisation's Mean Time to Detect (MTTD) and Respond (MTTR). However, the approach still relies on human experts to maintain applicable playbooks. This might become a complex and time-consuming task. Thus, while the advent of SOAR solutions is certainly a step in the right direction, security operations need to be automated significantly further to truly relieve the dependency on human expertise and effort for routine tasks.

A viable solution would include not only classical detection tools, but also tools that model ICT networks, calculate attack paths and model and estimate business impact. Ideally, a next generation of automation solutions would also support the actual analysis of complex threats and attacks in the context of an organisation's business and infrastructure. In the development of these solutions, machine learning and AI are almost certain to play a role.

These challenges can only be overcome by a mix of technical innovations. The aim of these innovations would be to improve insight and capabilities. Insight into how threats and cyber attacks propagate within an organisation's ICT infrastructure and the business impact of attacks. And capabilities for attributing attacks to known adversaries and effectively responding in an informed and (semi-) automated manner. Ultimately, we need to strive for self-protection. That involves the design of ICT systems and infrastructures that can anticipate, withstand and recover from emerging threats and ongoing attacks autonomously.

4. TAKING THE NEXT STEP

The idea of a self-protecting ICT system is not entirely new. In the early 2000s, IBM introduced it as part of its Autonomic Computing concept[7]. That concept, however, imagined a fully autonomous system with no human intervention. But it is unlikely that organisations will be able to allow full automation anytime in the near future.

Nevertheless, one key component of the Autonomic Computing concept may hold the key to improving cyber security today. The MAPE-K control loop consists of four functions with varying degrees of automation potential:

- *Monitor* – collect details (topology information, configuration properties, etc.) from managed resources and correlate them into symptoms that can be analysed.
- *Analyse* – perform data analysis and reasoning on the acquired symptoms to determine if any changes need to be made.
- *Plan* – create or select a procedure to enact a desired alteration in the managed resource.
- *Execute* – schedule and perform the necessary changes to the system.

In addition to these functions, MAPE-K identifies the ‘Knowledge’ component that is at the centre of the four functions.

There are, however, key areas in which expert human intervention still outweighs machine activity. For example, in understanding how a newly emerging threat affects an organisations’ infrastructure and business, and which Course of Action (CoA) would mitigate this threat or ongoing attack most effectively. A ‘human-in-the-loop’ solution, in which the latest technology is used to automate certain activities, can enhance the speed and quality of security decision-making. In this way, automation is used to provide essential security decision support, as indicated in the figure below.

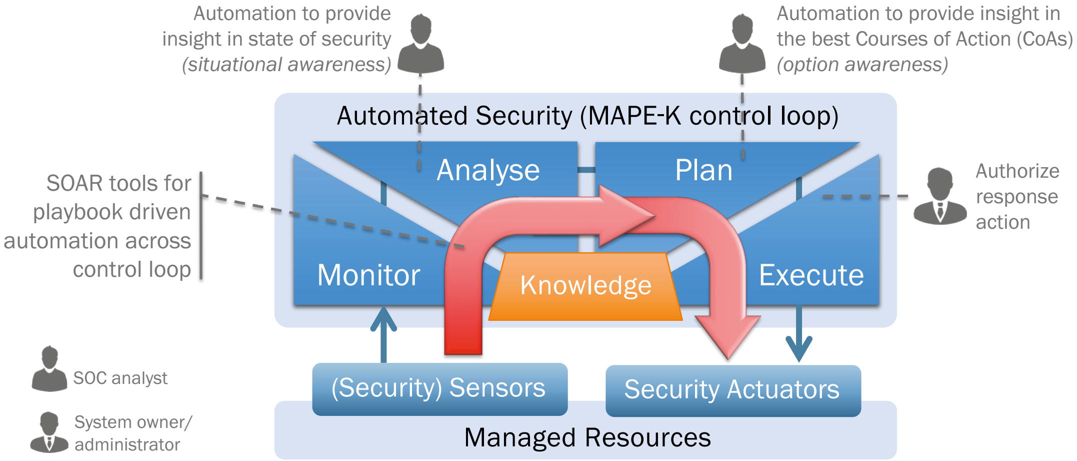
Automation to provide insight in state of security (situational awareness)
Automation to provide insight in the best Courses of Action (CoAs) (option awareness)
Automated Security (MAPE-K control loop)
Analyse
Plan
SOAR tools for playbook driven automation across control loop
Authorize response action
Monitor
Knowledge
Execute
(Security) Sensors
Security Actuators
Managed Resources
SOC analyst
System owner/ administrator

Figure 1. Conceptual figure of the MAPE-K model with a ‘human in the loop’.

[7] An architectural blueprint for autonomic computing (third edition), Autonomic Computing White paper, IBM-Corporation, June 2005, https://www-03.ibm.com/autonomic/pdfs/AC%20Blueprint%20White%20Paper%20V7.pdf

Each step in the MAPE-K loop is characterised by specific automation potential that can support human activities. Present-day market products already address some of this potential. In the ‘Monitor’ stage, for instance, SIEM and similar solutions are widely employed to automate the collection and correlation of security events occurring in an organisation’s infrastructure. What’s more, the SOAR products outlined in the previous section allow playbook-driven automation across the entire MAPE-K control loop. We envisage the concept of a *security decision support* environment that assists analysts by automatically assessing how attacks might propagate through an organisation’s ICT infrastructure and which potential CoAs could reduce the organisation’s exposure to such attacks most effectively. Such automation would greatly relieve the analytics effort required from human experts, and allow them to make more informed decisions on threat mitigation.

Cyber security is a concern for everyone. And the best solutions will come from widespread cooperation. TNO foresees public-private partnerships (PPPs) as a powerful means to achieve impact in automation of security operations and in security decision support concepts. These PPPs can manifest as programmes and long-term national alliances between research centres, knowledge institutes, government agencies, solution vendors and security service providers. They would be formed to undertake innovative, high-impact research around the automation of security operations.

5. TNO'S RECOMMENDATIONS

TNO's approach is to realise technology-driven *innovation in current monitoring and response products*. This includes innovation on advanced detection & CTI capability and on security decision support. The Security Decision Support concept will devise detailed models of enterprise ICT infrastructures and known attacker methods and subsequently (a) calculate and visualise how attacks could propagate through the network and (b) generate and assess potential CoAs that the organisation should consider in order to mitigate the threat. To achieve viable results, the infrastructure model needs to reflect the specifics of system and network configurations, the presence and configuration of security controls, communication flows permitted between nodes and assets, the presence of any unresolved vulnerabilities, and more. This poses something of a challenge, since organisations rarely possess an accurate and up-to-date inventory of all network devices and configuration data. In recent years, however, novel asset discovery tools have become available. As these evolve further, we expect that they can feed the Security Decision Support environment with much of the required infrastructure data.

Meanwhile, we should also recognise that appraising the effects of a potential CoA is not solely a technical matter. Factors to consider also include the impact on business processes and the costs of executing a particular mitigation strategy. Thus, to allow viable decision-making, appropriate business impact indicators should accompany any technical attack and defence appraisal presented to the security analyst. To this end, the Security Decision Support environment will need to be made aware of core business processes and their dependency on specific ICT assets.

As a catalyst in PPPs, and with a focus on transitions or changes in ICT, TNO believes in the joint creation of economic and social value. We don't do that alone, but with companies, governments and a whole range of organisations. We develop knowledge not for its own sake, but for real application. TNO is already involved in the field of cyber security in various academic and industrial research consortia as a technology research partner. With a track record in the application of top multidisciplinary knowledge, smart solutions for complex problems and focus on entrepreneurship, TNO already coordinates different ecosystems in the field of cyber security both on a national and international level. For instance, a pan-European R&D project on automation in security operations , and an R&D ecosystem in the northern Netherlands in security operations[8]. Much of the research involves the use of machine learning for anomaly detection and AI-based Attack Detection. Many innovations are the product of pre-competitive collaboration.

[8] SOCCRATES project granted under EU H2020 programme (expected to start in Q2 of 2019)

6. WAY FORWARD: PUBLIC PRIVATE PARTNERSHIP

While none of this will be easy, we believe that extensive automation of security operations will play an instrumental role in reducing MTTD and MTTR. And ultimately, it will achieve a better balance between defender and attacker capabilities. Concepts such as self-protecting ICT infrastructures and automated security that provide analysts with decision support certainly have the potential to reduce an organisation's exposure to cyber threats. It can also provide support in developing cyber security experts' needed skills and knowledge. It will take some time before these new technologies are embedded in ready-for-use market solutions.

A PPP allows the expression of an in-depth view of each domain's needs and opportunities. With their combined strengths, research institutes, cyber solution vendors, R&D institutions and end-user organisations (critical infrastructure) can create a more innovation-oriented view. And together, develop new security measures both to prevent cyber attacks, and to detect and react to them. TNO covers part of the research costs, and the remainder of the funding comes from the partner(s). To stay ahead of the cyber attackers, this needs to be developed rapidly. There is an immediate need for intense and efficient cooperation between academia, research institutes, government, solution vendors and security service providers. If approached in the right way, such partnerships can lead to an increased knowledge position for:

- *the Dutch economy*: the South Holland region can profile itself as a region with a global economic impact that rests on a strong foundation. Namely, a strong cyber security infrastructure. In addition, South Holland is benefiting from an increase in the number of cyber security product and service providers, the number of start-ups, and more experts with in-depth knowledge of cyber security who are available for the labour market.
- *solution vendors and security service providers*: there is an opportunity for these to advance, promote and increase market share of their products and services. Companies can increase their innovative strength and competitive position and that the regional (digital) economy can continue to grow.
- *R&D institutions*: these will enrich their reputation for excellent cyber security expertise and as a place where nationally renowned researchers work on the theme of automated security. For academics, it also means more opportunities for training of students on cyber security. This increases the available number of cyber security experts.

A PPP will create economic and social value. By joining together, companies can increase their innovative strength and competitive position. The regional (digital) economy of South Holland can continue to grow, particularly in the area of cyber resilience. And organisations and society can benefit from the innovations created to keep them safe from those who attempt to attack them.

For every step we take to defend ourselves against cyber attacks, our attackers take two. Unless we increase the speed with which we identify, detect and protect against these attacks, we will continue to fall behind. The best progress takes place in collaborations, in which key stakeholders work together from their areas of expertise, in order to develop robust, pre-competitive solutions.

June 2019

For more information please contact:

N. (Noura) el Ouajdi
T +31 611 44 79 09
E noura.elouajdi@tno.nl

TNO innovation for life

TNO.NL

MISSION AND STRATEGY

TNO connects people and knowledge to create innovations that boost the competitive strength of industry and the well-being of society in a sustainable way. This our mission and it is what drives us, the over 3,200 professionals als TNO, in our work every day. We work in collaboration with partners and focus on nine domains.