PUBLIC-PRIVATE PARTNERSHIP AUTOMATION OF SECURITY OPERATIONS

TECHNICAL EXECUTION PROGRAMME

December 2020

DEVELOPMENT OF A MODULAR SECURITY PLATFORM AND TECHNIQUES FOR THE AUTOMATION OF THE SOC IN A PARTNERSHIP BETWEEN SECURITY COMPANIES, PUBLIC ORGANISATIONS AND TNO FOR A DIGITALLY SECURE NETHERLANDS.

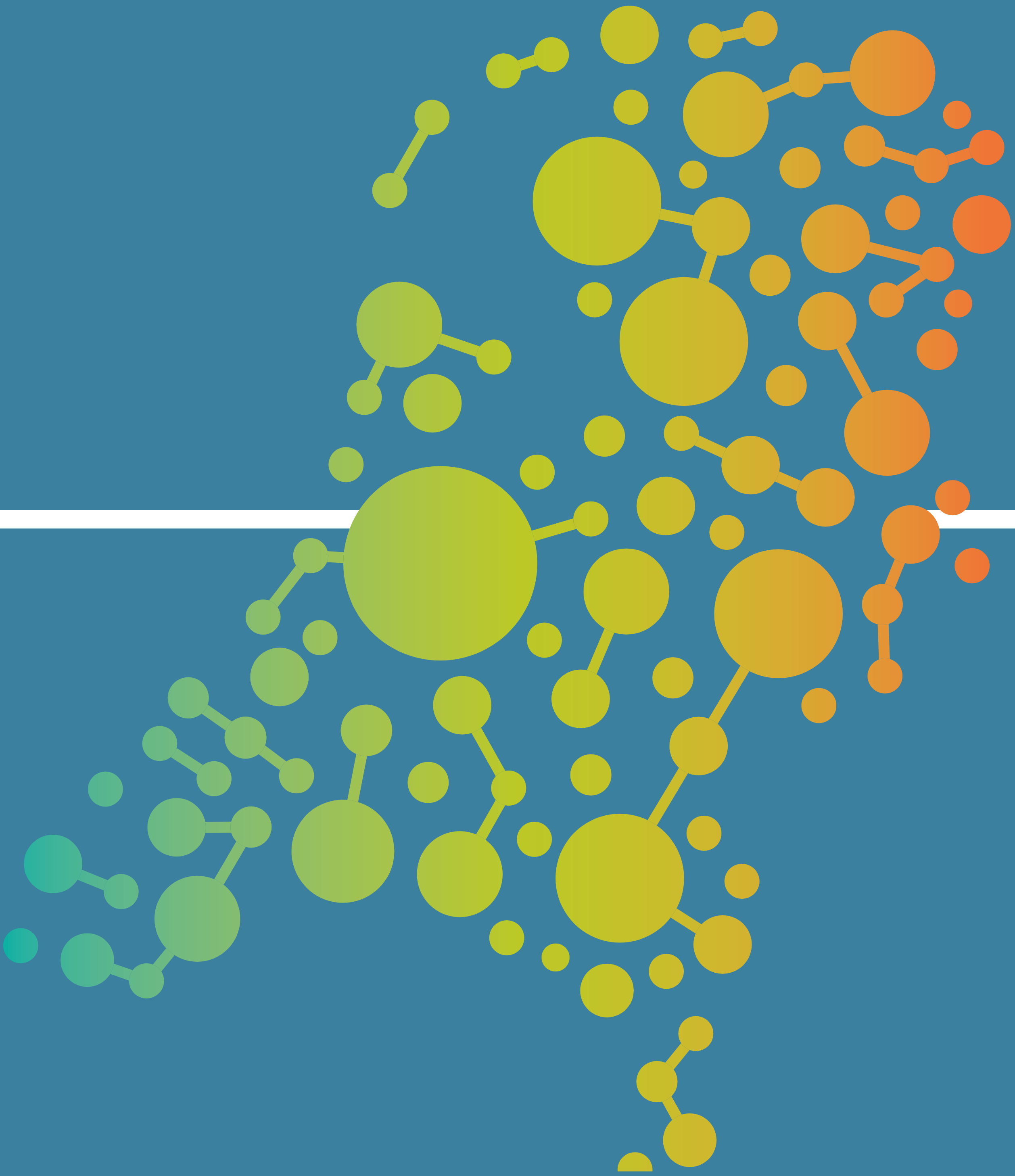


TABLE OF CONTENTS

MANAGEMENT SUMMARY

MANAGEMENT SUMMARY

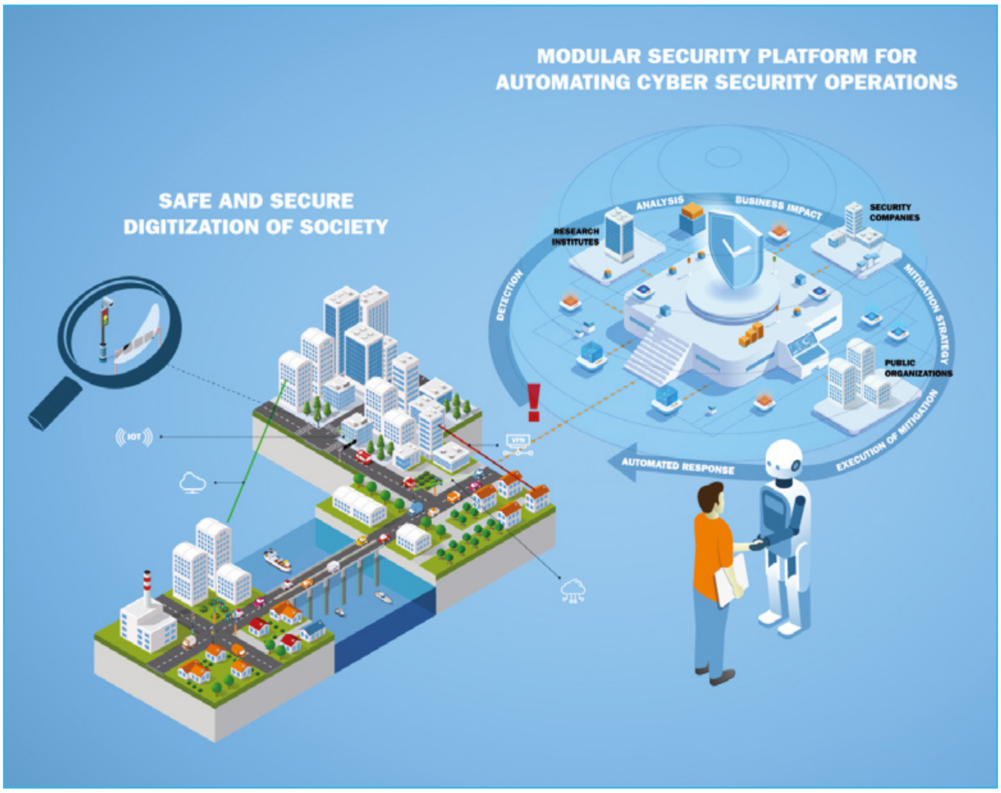
Cyberattacks are becoming more sophisticated, and their disruptive effects on business and society are increasing. Advanced attacks are often so highly automated that they can (largely) be carried out at machine speed. As ICT infrastructures are becoming larger and more complex, the workload for security analysts is likely to increase even further. Meanwhile, the cybersecurity market is starting to face a shortage of qualified security personnel. A manual approach to countering advanced cyberattacks is no longer sufficient.

Dutch security companies are currently experiencing particular difficulties in the lack of interoperability between cybersecurity products, and in finding capable personnel to analyse and respond to increasing amounts of alerts and incidents in a timely manner (interoperability & workforce). Due to the enormous increase in data volume and data diversity (sources and protocols/push-pull), manual filtering is becoming insufficient.

The most - if not only - feasible way to make a meaningful change is to integrally automate security operations. Targeted and effective cybersecurity operations require an integrated approach, as well as cross-sector knowledge and experience. Additional research in the field of AI, and the translation of this into practical solutions, are of great importance when it comes to being able to act quickly, effectively and adequately in response to a cybersecurity incident.

The ASOP consortium therefore aims to develop a game-changing integral platform for security operations based on a modular design that is easily extensible. The platform must be scalable and guarantee a high degree of interoperability between cybersecurity products. This will enable a high level of automation for security operations, making it easier for the entire chain of end users, system integrators and developers to proactively and reactively repel (complex) cyberattacks. By developing the new modular security platform and working towards the integration of services automation in Security Operation Centres (SOCs), the goal of this partnership is to:

– guarantee a secure and robust digital economy in the Netherlands (end user security products);
– compete on a global level as a cybersecurity sector (providers of cybersecurity products/ services).



Recent attacks on the municipality of Lochem and on Maastricht University show how large the consequences of a cybersecurity incident can be for citizens, organisations and their employees. Cybersecurity is a basic prerequisite for a prosperous and secure society in the twenty-first century. SOCs are considered crucial when it comes to detecting attacks and are at the heart of most cybersecurity strategies.

With the new modular platform for security operations, ASOP will improve the interoperability of security products independently of vendors, lower the workload of security specialists and reduce the required workforce. In addition, vendor lock-in will be prevented by ‘standardising the architecture’. By following a holistic approach to the integral automation of security operations and collaborating with both public and private organisations, the chances are increased that we, as the Netherlands, will have confidence in the digital world, can continue to take advantage of economic and social opportunities and can compete at a global level.

AMBITION

AMBITION

Through a multi-year public-private partnership between cybersecurity companies, public organisations and TNO, we aspire to take the next step in the automation of security operations. In order to guarantee a secure and robust digital economy in the Netherlands and to compete at a global level as a cybersecurity sector, we are working on the development of a modular and flexibly extensible security platform, and on the development and integration of SOC services automation.

THE CHALLENGES FOR DUTCH SECURITY COMPANIES

For a digitally resilient Netherlands and for combating increasingly sophisticated threats, it is essential to automate security operations in the near future. However, the automation of single sub-areas of the SOC, such as monitoring, detection and flagging, turns out much less valuable than an integrated holistic approach. Bringing together automatic detection, analysis, response options and infrastructure interventions offers the strongest advantage to end users with regard to the digital security of their own infrastructure(s). Due to the complexity of an integral approach, however, only large international players or partnerships are able to automate security operations in this way. By working together with different organisations (both public and private), the partners can participate in automation efforts and compete at a global level. An additional advantage of a solution developed in a partnership between different parties is that end users will be less dependent on one provider (avoidance of vendor lock-in).

Several security companies have already recognised the need to automate security operations. This has led to the development of Security Orchestration, Automation and Response (SOAR) products. These kinds of products can relieve specialists in a Security Operation Centre (SOC) of routine tasks and thus contribute to improving the average time needed to detect an attack (MTTD) and to recover from it (MTTR).

Nevertheless, SOCs still have a strong emphasis on necessary human actions; although SOAR products are a step in the right direction, security operations need to be further automated to keep reducing the dependence on human intervention. It is important to note that the automation of security operations depends on and must be consistent with the further development of the underlying infrastructure of computer networks. This is also mentioned in the Section Innovation 4: [PROGRAMMABLE INFRASTRUCTURE & INTERVENTIONS] ‘Programmable, composable and accelerated’ infrastructure for cybersecurity.

The next generation of security tools will need to automate the analysis of complex threats and attacks in the context of an organisation’s business and infrastructure. This can be achieved by developing tools that model ICT networks, detect attacks with extremely low false positive rates, calculate attack paths, assess the potential business impact and automatically execute infrastructure interventions. This will be an enormous improvement compared to the current working method, in which SOCs and the client take an average of three months to half a year to filter out events and logging in order to reduce false positives.

By working towards the next generation of security tools (and thus the further automation of SOC services), we as a Public Private Partnership (PPP) also address the biggest challenges faced by Dutch security companies. These are currently:

- Interoperability: a lack of interoperability between cybersecurity products, particularly in relation to the provision of information and telemetry for ensuring the digital protection of organisations. This lack of interoperability means that alerts from different security products are difficult to correlate, resulting in the inability to detect complex multi-stage attacks. Moreover, the correlation of information can greatly contribute to the lowering of false positive rates in the detection of attacks.
- Workforce: Finding sufficient capable personnel to analyse and respond to increased alerts and incidents in a timely manner.

- Data: Due to increased data volume[1] and data diversity (a huge increase in data sources & protocols/push-pull), manual filtering is insufficient.

SCALABLE, EXTENSIBLE AND MODULAR SECURITY PLATFORM

The integral automation of security operations is beneficial for consumers but also for security companies. By making use of the large range of cybersecurity products, we see opportunities within the PPP to further automate security operations in order to:

- improve the interoperability of security products through the development of an open API-based **scalable, extensible and modular security platform**, independent of vendors. In short, we aim to improve the interoperability of security products by developing a vendor-independent platform.
- **decrease the workload of security specialists** and reduce the size of the required workforce by developing the adapted competencies of future SOC employees in line with technical innovations.
- prevent **vendor lock-in** by 'standardising the architecture and modules for security operations' and stimulate cybersecurity product innovations.

APPROACH

Following a holistic approach to the integral automation of security operations and working with different organisations (both public and private) increases the chances that we, the Netherlands, have confidence in the digital world, can continue to take advantage of the economic and social opportunities and can compete on a global level. The connected security companies will be engaged in:

- Improving the quality of services: innovations which will make it possible to include not only security considerations but also operational considerations when mitigating incidents.
- Being part of an integral, automated solution for end users by anticipating the demand-driven functionalities of the cyber sub-product.
- The modular integration and demarcation of existing and future security products. This requires the smart combination of open standards and the far-reaching automation of data processing.

The adequate modular integration and demarcation of existing and future security products is necessary in order to realise the above gains for Dutch security companies. This requires a smart combination of open standards and the far-reaching automation of data processing. Applied research is necessary in order to translate this into practical solutions and to build up the required knowledge and experience.

Only by working together in an innovation ecosystem with cybersecurity companies, public organisations and knowledge institutions can we take steps towards realising the aforementioned ambitions. None of the parties mentioned are in a position to integrally automate solitary SOC services (including detection, analysis, response and infrastructure interventions) and thereby satisfy the greatest need of end users.

The exact content of the PPP activities will always be determined for the following phase in the form of use cases, and on the basis of the expertise and ambitions of participating partners.

As a participating partner, you can propose adjustments to the activities already defined and suggest new directions, so that the work within the PPP responds as well as possible to your (and the other partners') most relevant challenges and needs. You can also make a substantive contribution to the technical innovations to be developed. Of course, all activities within the partnership are carried out in consultation with the other partners.

A thematic approach will be used in the innovation ecosystem. This ensures that various activities carried out in parallel fit together in a connecting, overarching theme. The aim is also to work in a "chain-oriented" manner, which means that the various partners have a complementary role to play in relation to one another. Within the PPP, all parties will be given the opportunity to contribute to the social and economic challenges, while focusing on their own supply and demand. The thematic approach and chain-oriented working method will be shaped by cooperation at the technical and organisational levels, and by bringing the innovations to the market.

[1] *Data growth https://en.wikipedia.org/wiki/Amsterdam_Internet_Exchange.*

ORGANISATIONAL COOPERATION

The identification of shared interests and ambitions contributes to the achievement of a constructive group dynamics with partners. In order to safeguard the common denominator for all innovations within the domain of security operations, we strive for effective shared working methods that lead to decisions and support for future developments within the PPP.

BUSINESS COOPERATION

Within the partnership, we will use the specific expertise of partners and common facilities to work towards a collection of coherent value propositions, which will lead to an integrated platform for security operations. These value propositions need to be acceptable to all parties involved and must take into account the (business) context, which will change as a result of the introduction of these innovations and the associated roles of the partners. The expertise of the partners and the innovation issues that the partners intend to work on will be determined in consultation with the partners.

TECHNICAL COOPERATION

The substantive technical objectives that the PPP aspires to achieve (see the following chapter: Technical objectives) are technically challenging in a way that cooperation between several kinds of sub-expertise is required. Interoperability within the platform must be arranged in such a way that flexibility, extensibility and market adoption remain unhindered. In the ASOP innovation ecosystem, the most renowned and progressive Dutch security companies (and international companies with a Dutch branch) will work together in order to meet this technical challenge.

SUMMARY

Within the Automated Security Operations PPP, we will tackle one of the biggest challenges in the field of cybersecurity (**automation through innovation**) in a collaboration with security companies and public stakeholders. We will do this by developing a modular and flexibly extensible security platform, enabling the automation of security operations. At the same time, we will map and develop the necessary competences of future SOC employees, so that security companies can provide scalable products and services. We enable the participating security companies to bring future-proof products and services to the market. Only by working together can we achieve these ambitious objectives. Together, we make the Netherlands more digitally resilient.

BUSINESS OBJECTIVES

BUSINESS OBJECTIVES

The multi-year programme aims to support the partners with technological developments in order to achieve the following business objectives:

1. **Thought leadership:** by being part of an exclusive ecosystem (a non-competitive, complementary partnership), companies take a distinctive, leading position on cybersecurity.
2. **Market edge:** the exclusive opportunity to make money through cost savings by marketing automated security operations and making this visible both nationally and internationally.
3. **Determination of the (market) standard:** pre-competitive collaboration contributes to the determination of the standard for an automated framework and the early adaptation of services to the standard.

TECHNICAL OBJECTIVES

TECHNICAL OBJECTIVES

The multi-year programme aims to achieve the following **substantive technical** objectives within the public-private partnership ASOP:

1. **Architecture development and platform implementation**: the development of an open, modular and flexibly extensible architecture and the implementation of this architecture in the form of a cloud-based platform for automated security operations. This enables the integration of existing and emerging technologies into a whole. The platform offers tools to increase the efficiency and effectiveness of SOC and CSIRT operations. The modular and flexible structure of the platform will allow users to adapt to changing threats in the future. This objective contributes to the realisation of an integral solution and a high degree of interoperability between security products.
2. **The (further) development of automated security operations**: the further development of existing technologies and the development of new technologies to enable various aspects of automated security operations for the entire chain of end users, system integrators and developers. More specifically, this means:
    a. The design and development of monitoring and detection algorithms and modules with ultra-low false positive rates as a basis for automatic responses. New AI algorithms are being developed alongside advanced methods for sensor and data combination in order to minimise false positive rates.
    b. The design and development of technologies for the automatic analysis of the effects of security events (both detected attacks and information on new threats) on the digital security of the ICT infrastructure. This includes the associated impact on an organisation and the identification, analysis, planning and activation of mitigation or response actions.
    c. The design of an architecture component for translating the alerts/actions from the monitoring and detection algorithms and the automatic response actions into suitable infrastructure interventions which function regardless of the design of the (re)programmable infrastructure.
3. **Competence development**: competence development in order to equip future ICT/SOC specialists for their tasks within automated security operation centres.

ANALYSIS
BUSINESS IMPACT
MITIGATION STRATEGY
EXECUTION OF MITIGATION
AUTOMATED RESPONSE
DETECTION

THEMATIC APPROACH OF THE PPP

The PPP's thematic approach is building a strong cyber-ecosystem to support the partnership on usage research by focusing on a strong (supply and demand) relationship between the government, the cybersecurity sector and (academic) research. In making the ongoing challenges in cybersecurity concrete and ensuring that the solutions are properly aligned with the market, the PPP will work with a thematic approach by formulating specific use cases and scenarios. The government will act as a 'launching customer' to drive innovation in the Dutch cyber-domain by providing a test environment for our innovations. This reinforces the economic and social opportunities of digitisation and protects national security in the digital domain.

WORKING WITH USE CASES AND SCENARIOS

A use case is a concrete delimitation of a challenge within practical security operations.
The scenarios which are part of these use cases are specific situations that occur in practice, and that will be used to steer the direction for new innovations. The innovations to be developed within this PPP are the necessary techniques in order to solve the current limitation(s) of state-of-the-art technology within the field of security operations automation.

In other words, the use cases and scenarios define the problem to be solved and thus the innovations to be developed, but also make it easier to determine whether innovations will meet market needs. In consultation with the partners, the current use cases can be adjusted and extended. An initial outline of the use cases is shown in Figure 1.

For each phase of the partnership, the use cases will be supplemented on the basis of input from market parties. In consultation with the partners, they can be adjusted and extended, and new use cases can be suggested and introduced. On the basis of the established governance, partners can join a use case as a whole or a separate scenario and/or contribute to one or more innovations. The idea is also that the market parties will continuously steer the use cases and scenarios into the right direction based on their wishes and needs.

The (further) development of techniques for automated security operations will be sub-divided into three types of research activities or work packages (WPs): 1) monitoring and detection techniques (WP3); 2) automatic analysis and response techniques (WP4); and 3) programmable infrastructure and intervention techniques (WP5). For each scenario, the various research activities work towards predefined deliverables so that it remains possible to integrate these activities while all of them can be worked on simultaneously, despite the underlying dependencies.

USE CASES IN IT INFRASTRUCTURES

Within the consortium, the following use cases serve as a basis for the innovations to be developed in order to meet the needs of security operations regarding the protection of IT infrastructures.

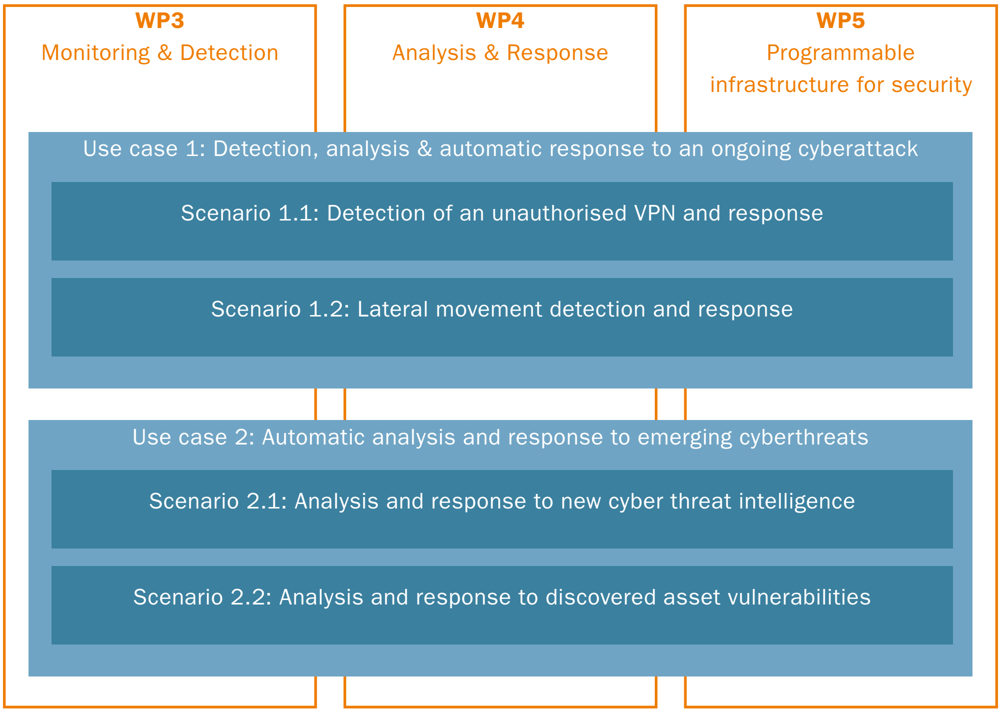

WP3
Monitoring & Detection
WP4
Analysis & Response
WP5
Programmable infrastructure for security
Use case 1: Detection, analysis & automatic response to an ongoing cyberattack
Scenario 1.1: Detection of an unauthorised VPN and response
Scenario 1.2: Lateral movement detection and response
Use case 2: Automatic analysis and response to emerging cyberthreats
Scenario 2.1: Analysis and response to new cyber threat intelligence
Scenario 2.2: Analysis and response to discovered asset vulnerabilities

Figure 1 Use cases and scenarios which transcend the work packages

Use case 1: Automatic incident response to detected cyberattack
A challenge that many (security) companies and organisations face is the difficulty in accurately detecting cyberattacks such that little or no human action is required to proceed from detection to a response. A solution for this is detection with ultra-low false positives, followed by an automatic analysis and response. With such a solution, however, one must get a view of the expected impact of the security incident and the corresponding response on the organisation, and only then apply the correct intervention. This use case is therefore focused on the automatic execution of the following incident response phases: (a) detecting advanced cyberattacks with a high degree of certainty; (b) determining the full scope and impact of the incident; (c) identifying response options (particularly for the containment of the incident); and (d) executing the selected response actions.

To illustrate the usage of scenarios, the first scenario of Use Case 1 (see Figure 1) is worked out in the text below.

Scenario 1.1: Detecting and mitigating unauthorized VPN connections established from within a corporate network.
In many companies, it is a policy violation to set up a VPN from within a corporate network to an external VPN server, as this poses cybersecurity risks to the company. To avoid circumvention of this policy, there is a need for technology that automatically detects and mitigates such unauthorized VPNs. In Scenario 1.1 we therefore develop a proof-of-principle implementation of a modular security platform, which can automatically detect, analyze and respond to unauthorized VPN connections in a corporate network. The proof-of-principle is implemented in a generic way, such that it can also be used as a basis for the automatic mitigation of other security threats such as lateral movement and command-and-control channels.

- Goal: Development of a modular security platform that supports the SOC with real-time detection and automated response. This is an important milestone towards fully automated incident response.
- Result: A proof-of-principle solution that automatically detects and mitigates unauthorized VPNs.

– Innovations:
  - Monitoring & Detection: Traditionally, VPN detection is rule-based. The innovative goal is to develop an anomaly detection module that reliably detects VPNs without signatures.
    To achieve low false positive rates, the added value of correlating information from multiple data sources (e.g. DNS, NetFlow, public domain/SSL information) is investigated. It is anticipated that computers with active VPNs show different communication behavior than "normal" computers, e.g. lower diversity in external IPs, or unusually long connections. Such features are also investigated.
  - Automatic analysis & response: provides modules for security orchestration, infrastructure modelling, and for the generation of courses of action (CoAs) based on security alerts (such as "VPN detected").
  - Programmable Infrastructure: provides the underlying hardware and cloud infrastructure that provides all the functionality needed to both gather network data and execute automated response actions. To this end, an infrastructure abstraction layer is developed.

The innovative nature of these research activities is explained in more detail in the Innovations chapter.

Use case 2: Automatic analysis & response to emerging cyberthreats
One challenge that many security companies struggle with is combining information from different security tools (due to lack of interoperability) and the smart processing of the increasing amounts of data generated. For this reason, the PPP in this use case focuses on the automated use of threat intelligence information in an effective and efficient way for SOC operations. This is mainly a matter of identifying which information is relevant to the organisation in the face of an extensive stream of incoming data, and then quickly adapting one's own infrastructure and operations to the altered situation.

This use case is aimed at increasing the resilience of the infrastructure (i.e. anticipating future threats) by executing the following steps automatically as much as possible: a) continuously updating a current threat assessment regarding the attack techniques used and the vulnerabilities present in the infrastructure; b) determining the effect of the new threat/vulnerability on the digital security of the ICT infrastructure (will an attack be easier?) and what the potential impact on the business is; c) identifying response strategies to mitigate the increased risk; and d) executing the selected mitigation action.

Conclusion
This is an initial elaboration on the use cases and scenarios within the domain of IT infrastructures in order to concretise the challenges in the field of automated security operations, fit the solutions to the market and safeguard the integration of different types of innovations to be developed (types of innovations: monitoring & detection, analysis & response, programmable infrastructure). This integration is shown in Figure 1. Not all scenarios have been worked out fully, to leave room for partners and adjust to their needs appropriately.

In phase one of this programme (until ca. February 2021), Scenario 1.1 is further elaborated and used for the development of a proof-of-concept as an initial step towards achieving the technical objectives (see the section: Technical objectives). In this proof-of-concept, software will be provided to demonstrate the feasibility of the objectives of Scenario 1.1. Implementation of this software among partners falls outside of the scope of PPP ASOP. During the execution of this project, the use case scenarios will be further elaborated in cooperation with the affiliated partners.

USE CASES IN OT INFRASTRUCTURES

In addition to the use cases and scenarios focused on automated security operations for IT infrastructures, the PPP also aims to develop one or more use cases for OT (operational technology) infrastructures. However, this depends on the wishes of the affiliated partners and investors. The elaboration of these use cases is a project activity and will be carried out at a later phase of the programme.

INNOVATIONS

In order to achieve the technical objectives of the PPP through the above use cases, the technological innovations can be divided into three categories: monitoring & detection, analysis & response and programmable infrastructure & interventions.

The integration of these three types of innovations is crucial in order to arrive at an easily applicable solution. A simplified version of this integration in an automated security operations architecture is shown below in Figure 2. The underlying dependencies between monitoring & detection (WP3), analysis & response (WP4) and programmable infrastructure & interventions (WP5) in the field of information/data flows are shown with arrows.

The innovations to be developed are explained in the following sections, first by providing an outline of the current state-of-the-art and its limitations, and then by showing which solution the PPP aspires to develop for this.

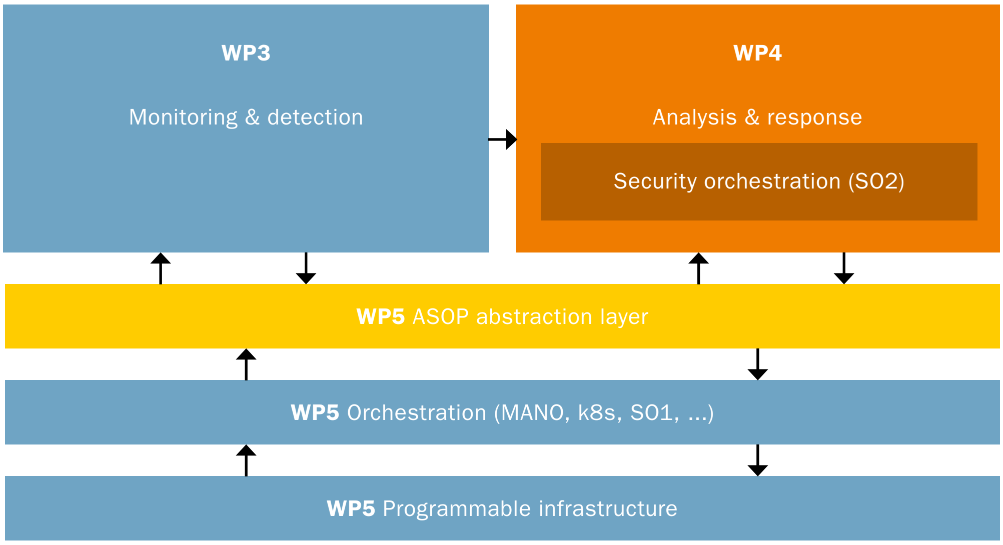

WP3
Monitoring & detection
WP4
Analysis & response
Security orchestration (SO2)
WP5 ASOP abstraction layer
WP5 Orchestration (MANO, k8s, SO1, ...)
WP5 Programmable infrastructure

Figure 2 Overview of programmable infrastructure in relation to the work packages

INNOVATIONS

INNOVATION 1: [MONITORING & DETECTION] DETECTION ALGORITHMS FOR HETEROGENEOUS DATA SOURCES AND METHODS FOR FALSE POSITIVE REDUCTION

State-of-the-art: In current practice, the false positive rates for security alerts (e.g. from the SIEM) are often too high for an automated response.

Limitation: SOC analysts must first manually analyse security alerts/tickets. This is very labour intensive. An automatic response to a false positive has many undesirable effects.

Innovation: Detecting advanced cyberattacks with a high degree of certainty by combining features, detectors and various data sources (such as NetFlow, DNS, proxy, system logs, cloud, etc.), developing (statistical) anomaly detection methods and applying advanced (unsupervised) machine learning/AI-based detection techniques.

INNOVATION 2: [ANALYSIS & RESPONSE] METHODS FOR CREATING AND INCREASING SITUATIONAL AWARENESS

State-of-the-art: Many security products for SOCs offer users a situational view from the information position of the specific product. SIEMs can combine parts of this information position by collecting security events and correlating them for alerts. The dashboard of a SIEM thus offers a situational view of the potential attacks on the ICT infrastructure. With the recent introduction of Threat Intelligence Platforms (TIP), systems are available that offer a situational view of the current threats.

Limitation: For a full picture, the various views of individual security products need to be combined. There is a lack of automatic security analysis in regard to the effects of a threat, vulnerability or cyberattack on the ICT infrastructure and the (potential) business impact. This requires an up-to-date view (or model) of the ICT infrastructure within which the threat and attack can automatically be analysed and visualised.

Innovation: Technology for the automatic creation of a high-quality situational view of the threat and/or detected attack within the context of the ICT infrastructure and the (potential) business impact. The work will include:

- Automatic ICT infrastructure modelling;
- Automatic analyses of possible attack steps within an ICT infrastructure model;
- Automatic analyses of the business impact of an attack or threat;
- An open and modular platform for the orchestration and integration of security analysis tools (and control of the automatic response).

INNOVATION 3: [ANALYSIS & RESPONSE] METHODS FOR CREATING 'OPTION AWARENESS' AND AN AUTOMATIC RESPONSE

State-of-the-art: The current incident response analysis and identification of response measures to be taken are largely based on human actions. The new SOAR products offer the possibility for the playbook-driven automation of the incident response process. OASIS is working on an interface specification for automatic responses (OpenC2) and a markup language for security playbooks (CACAO).

Limitation: The automation of an incident response process is based on predefined actions. Possible actions are not automatically identified and analysed for their impact on the ICT infrastructure and are not automatically analysed for their business impact (neither the positive nor the negative consequences of applying the response measure).

Innovation: Technology for the automatic creation of ‘option awareness’ (action perspective) for informed decision-making regarding response actions. The response actions, also known as Courses of Action (CoAs), will be automatically analysed on the extent to which the threat or attack can be mitigated and the consequences for business processes.
Technology for automatically planning and initiating the execution of CoAs in a (programmable) ICT infrastructure (Innovation 4).

INNOVATION 4: [PROGRAMMABLE INFRASTRUCTURE & INTERVENTIONS] ‘PROGRAMMABLE, COMPOSABLE AND ACCELERATED’ INFRASTRUCTURE FOR CYBERSECURITY

State-of-the-art: The softwarisation of the infrastructure helps in introducing new services at a faster pace and allows for the automation of their lifecycle management. It also facilitates run-time reconfiguration. Following this trend, many security functions have been softwarised (e.g. virtual firewalls, virtual intruder detection systems) while Security Orchestration, Automation and Response systems to facilitate SOC activities have started to appear on the market.
At the same, the amount of data going through the systems is only increasing (800 Gbps Ethernet is on the way) as more physical and virtual devices are connected.

Limitation: The programmability of the infrastructure comes at the cost of manageability.
For example, a large number of APIs may need be connected (with precisely specified calls) in order to take an action recommended by a response module. That would imply a very detailed knowledge of the internal infrastructure by the analysis and response engine.
Observability could be another issue: cloud-based services can be highly ephemeral and therefore difficult to monitor, malicious flows in SDN switches can be installed for just the timeframe for which the attackers need them and then removed, (serverless) microservices can have very short lifetime (leaving few useful traces) and a constantly changing topology can be difficult to model using the defence/attack graph tooling.
Another problem is that while softwarisation provides flexibility, it does not imply performance – which may be heavily impaired due to the large amount of data to be processed, forcing (for example) monitoring and analysis to be carried out at only a ‘crude scale’ (such as infrequent sampling or fast but inaccurate reasoning). This gives the attackers the opportunity to stay below the radar.

Innovation: ASOP proposes the following innovations in order to address the aforementioned challenges.

An ASOP abstraction layer placed on top of the current orchestration layer, will shield the higher layers (monitoring & detection, analysis & response) from the complexity of the underlying systems. This layer provides a model of the underlying infrastructure to the upper layers, accepts the requests from the higher layers in the form of an ‘intent’ (‘what’, not ‘how’), translates these and analyses them in order to prepare and execute the exact calls towards the appropriate lower-layer control planes. As an illustration, consider the following example:

> The monitoring & detection layer expresses the intent to perform a deep packet inspection of a specific flow and gives a priority of ‘high’ to this request. The ASOP layer concludes that the DPI workload needs to be placed on a node which has an appropriate hardware accelerator which is now fully saturated with medium-priority workloads. ASOP therefore decides to remove these jobs, starting the DPI workload and also contacting the switching fabric controller to make sure that the selected flow reaches the DPI. All of these steps are completely transparent to the higher-layer module which requested the DPI service.

Similarly, monitoring modules can request tracking for a given service, which the ASOP layer translates into the series of specific requests by gathering (for example) the metrics related to the application itself and a compute element running the app components and the network, even if these are ephemeral. A monitoring module therefore does not need to track the exact topology of the infrastructure.

The ASOP abstraction layer will be designed to be modular (e.g. a module to create infrastructure models for the upper layers, a module for translating their requests, a module for functions placement, etc.) and extensible (the ability to add new modules), communicating with other layers via open application programming interfaces (APIs).

To provide these kinds of services, ASOP also innovates in the lower layers. In order to provide, for example, exact measurements and the ability to reconfigure monitoring functions in run-time, the recent developments in data plane programmability (alongside control plane programmability) can be used to provide enhanced telemetry functions. ASOP will also research how the performance and flexibility of the cybersecurity functions can be boosted by exploiting the programmable hardware and by using the concepts of infrastructure composability. The former can offer speed while still allowing for a quick introduction of changes and improvements; the latter can help the ASOP layer to quickly create a high-performance virtual infrastructure for the execution of a given task.

FOR MORE INFORMATION,
PLEASE CONTACT:

Noura El Ouajdi
T +31 (0)6 11 44 79 09
E noura.elouajdi@tno.nl
I www.tno.nl/automated-security

innovation
for life

TNO.NL