PwC Poland

SIEM Implementation

Key challenges in incident detection and response

Lack of talent and analyst burn-out

There is huge lack of skilled cybersecurity personnel across all regions of the world.
On top of it the current workload in typical Security Operations Center contains a lot of mundane, boring tasks, such as manual checking IoCs, running SIEM searches, creating service desk tickets, preparing reports etc. This holds back the ability of organizations to focus on adapting to new threats and building knowledge, drives up the costs of SOC and finally makes organizations vulnerable.

Our approach

- Automate and streamline processes in SOC with SOAR
- Bring in additional security analyst and engineering resources when needed
- Move to outsourcing or co-sourcing model tailored to specific needs

Enormous complexity of IT environments and sophistication of threats

Nowadays whole IT is heavily virtualized and abstracted - topics like SaaS, serverless computing, service mesh, software defined networks are the new normal. Long gone are also days where the virus or malware file can be identified and tracked - most attacks are now using common tooling available in OS (like PowerShell scripting) and blend into the background noise of regular IT and user operations. This results in low effectiveness in finding and responding to threats.

Our approach

- Deploy machine learning technologies
- Bring in additional expertise for new technologies
- Provide threat intelligence and threat hunting for sophisticated threats

Lack of tangible results from technology investments

Billions of dollars are spent each year on cybersecurity technologies, yet the outcomes from investments are not tangible or are not proportionate to the investment made. With the multiple new technologies and vendor solutions it is hard to determine which value added the specific solutions bring and with the lack of time for anything else than every day operations, it is challenging to to show the benefits of technology investment to the board.

Our approach

- Optimize costs of existing solutions by clever engineering and smart design of system architecture
- Build outreach program to show value of SOC to business and board

Threat detection and response

To keep the pace with the attackers organizations needs to act quickly and effectively. This means that threats need to be detected as soon as possible, using multiple data sources and techniques, combined together. Once possible security incident is identified it needs to be analyzed and responded to.

Our approach is based on three fundamental technologies to achieve this:

EDR

(Endpoint Detection and Response) tools

Security analytics

SIEM combined with UEBA and other advanced analytical methods (ML, AI)

SOAR tool

to streamline and automate incident analysis and response

There are many other solutions and technologies which are vital for prevention and detection which important, but each building needs to have strong foundation first.

Challenges

The quality of data in CMDB is often a challenge to understand what needs to be protected, and pace at which IT can deliver integrations to get the security relevant data is often a problem.

Ideal Solution

There is no ideal solution - each organization is different, and the IT environment is not ideal either. We believe that the best solution is one tailored to organization’s needs.

Desired Outcomes

Technology must bring tangible value by driving down detection and response time, and help to limit amount of boring tasks done by SOC team.

Our implementation and operations services

Design

- Requirements analysis/preparation
- HLD & LLD preparation
- Target architecture design

Implement

- Install software (and hardware if required)
- Deliver licenses (for selected vendors)
- Configure software and integrate with client's infrastructure
- Deliver acceptance testing
- Deliver post-implementation documentation

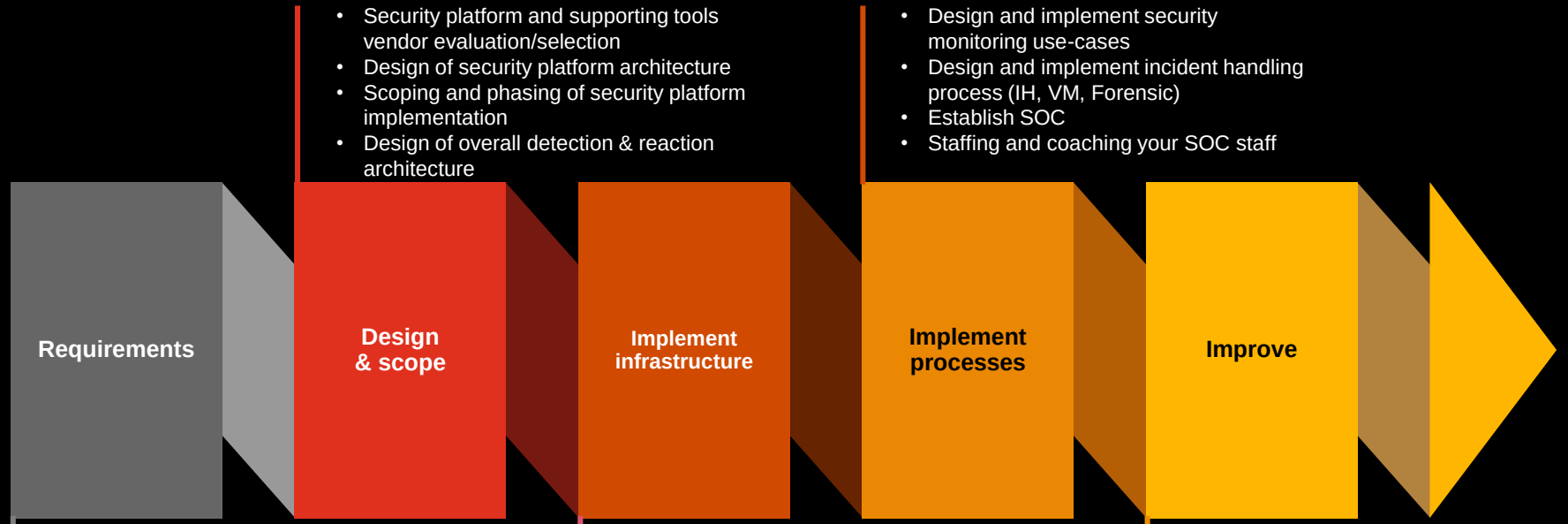
Support & operate

- Provide first line of support for clients
- Proactive maintenance (healthchecks)
- DevOps - daily maintenance and small development of platforms (upgrades, new integrations, keeping system healthy, plan capacity and performance etc.)

Technology	Solutions we support
SIEM	Microsoft Sentinel, MicroFocus ArcSight, Splunk, IBM QRadar, ELK Stack
EDR	Microsoft Defender ATP, Tanium, Palo Alto Networks XDR, FireEye HX
VS	Qualys, Rapid7, Nessus
SOAR	Microsoft Sentinel, Demisto
OT/SCADA	Claroty

Security platform and SOC services

Security platforms like SIEM / EDR / SOAR provides organization with a centralized, real-time view on its critical assets, enabling monitoring, detection and automated response to IT incidents.



Security platform Migration or Implementation in Microsoft Azure

Either it is Microsoft Sentinel, other SIEM solution ro EDR deployment in Microsoft Azure cloud offers unmatched availability and scalability, ease of on-boarding and configuration.

Deployment in Microsoft Azure Cloud

We provide end-to-end implementation and configuration of security platform solutions in Microsoft Azure cloud independently of technology Vendor. Usage of Microsoft cloud-native SIEM / EDR / SOAR solutions eliminate security infrastructure setup and maintenance, and elastically scales to meet organization's security needs.

Cloud and hybrid models

Depending on the organization's IT infrastructure, SIEM / EDR / SOAR solution can be implemented fully in Azure cloud or in hybrid model. Both models offer flexibility that is unparalleled in traditional on-premises.

Managed Security Services and Platform Engineering

We provide flexible support in security monitoring and engineering for critical assets security, vulnerability management, monitoring, analysis, Incident Handling and Threat Hunting.

Customer success: SIEM migration to Azure

We helped a global professional services company to migrate their on-premises Splunk SIEM solution to Microsoft Azure cloud in the hybrid model.

The project included:

- migration of core components of the system
- implementation and configuration of new components within the collection layer
- Security solutions maintenance
- Ongoing development and support (SIEM, EDR, VM)

Customer details

- Global Fortune 500 company
- 50,000 endpoints
- 3,000+ servers
- SIEM size ~1TB/day

Azure – ease of on-boarding

We were able to complete the project in fraction of time usually needed in similar on-premises projects.

We ensured a full transparency of migration in terms of SIEM operations throughout a project.

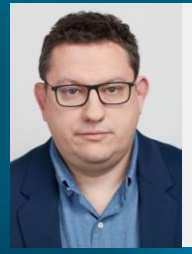
Azure – flexibility and scalability

Together with our customer we were able to allocate just the right amount of IT resources to meet system loads.

Azure cloud-based Splunk can be easily scaled in order to address customer's evolving IT infrastructure.

Contact us

and learn more



Szymon Sobczyk

PwC Senior Technology Leader
+48 519 504 525
szymon.sobczyk@pwc.com

Łukasz Kowalski

PwC Manager
+48 519 504 217
lukasz.kowalski@pwc.com

pwc

Microsoft Partner

2017 Partner of the Year Finalist
Public Sector: Microsoft CityNext Award