



Rethinking your Microsoft Sentinel implementation

A use case-driven approach

Jemal Mohamed
Sr. Adviseur Informatiebeveiliging @ EQ Consulting B.V.
Partner @ Confidentity B.V.

Datum: 16 mei 2024
Classificatie: public edit



CONFIDENTIETY
IDENTITY SECURITY EXPERTS



gemeente
Haarlemmermeer

Introductie



ID CARD **CONFIDENTI**T**Y**



The ID card template features a blue header bar with 'ID CARD' on the left and 'CONFIDENTI**T**Y' on the right. Below the header is a white rectangular area containing a portrait photo of Jemal Mohamed, his name, IT experience, Cyber Security Pro status, education, and a blue footer bar.

NAME
Jemal Mohamed

IT EXPERIENCE **CYBER SECURITY PRO**

15 years Since 2013

EDUCATION

CISM, ISO27001, HBO



Strategie en Beleid

- Advisering op het gebied van informatiebeveiliging (CISO/ISO)
- Security GRC (Governance, Risk & Compliance)
- Security Maturity & Compliance Assessments
 - BIO, ISO27001, NEN7510, Norea CSA, NIST CSF, NIS-2
- Begeleiden van aanbestedingen op het gebied van SIEM/SOC en Managed Detection & Response (MDR) dienstverlening.

Security Architectuur

- Security Monitoring (SIEM/SOC)
- Privileged Access Management (PAM)
- M365 Security / Microsoft Sentinel
- Security Hardening en Security Assessments (o.a. Azure Cloud)
- Doorontwikkeling Security Architectuur in complexe omgevingen

Ervaring

- Strategisch Adviseur Informatiebeveiliging (overheid)
- Senior Information Security Officer, CISO office (ziekenhuis)
- Adviseur Informatiebeveiliging (overheid/gemeente)
- Security Architect (overheid/gemeente)
- Cybersecurity Officer (luchthaven)
- Senior Consultant Cybersecurity (industrie en financiële sector)



CONFIDENTIT**Y**

Over gemeente Haarlemmermeer

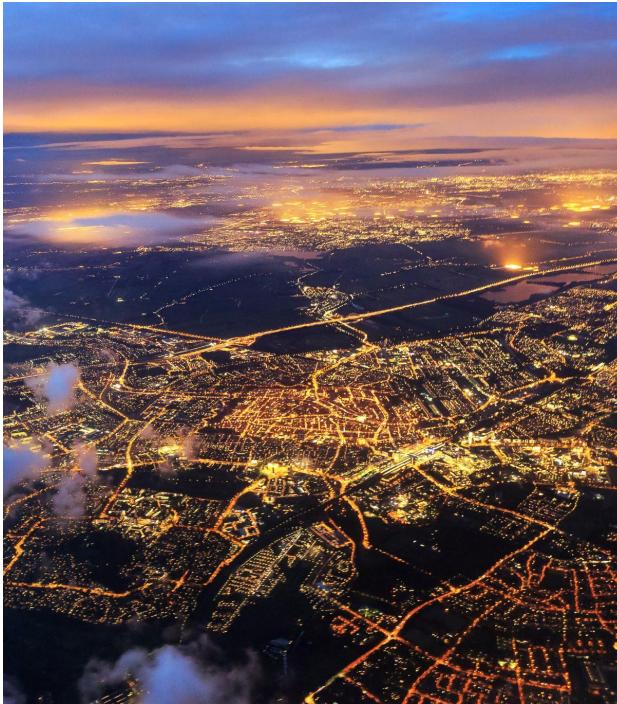


gemeente
Haarlemmermeer

- Heeft **163.196 inwoners**, Hoofddorp is de grootste plaats met ruim 78.000 inwoners.
- Gemeente Haarlemmermeer bestaat uit **31 officiële kernen** (dorpen en buurtschappen).
- De luchthaven **Schiphol** is gevestigd binnen gemeente Haarlemmermeer.
- Het dorp **Spaarndam** ligt in 2 gemeenten. Spaarndam-Oost valt onder gemeente Haarlemmermeer, het historische westelijke deel, Spaarndam-West behoort bij de gemeente Haarlem.
- Gemeente Haarlemmermeer is voor 18e keer **economisch sterkste gemeente** van Nederland volgens het Elsevier Weekblad.
- **Stoomgemaal Halfweg** is het oudste en grootste nog werkende schepradstoomgemaal ter wereld. De 500pk stoommachine (en ook de stoomketel) bestaat al 100 jaar en functioneert nog steeds.



Nº	Naam	Provincie	Inwoners
1	Amsterdam	Noord-Holland	934.927
2	Rotterdam	Zuid-Holland	671.125
3	Den Haag	Zuid-Holland	565.701
4	Utrecht	Utrecht	374.411
5	Eindhoven	Noord-Brabant	246.443
6	Groningen	Groningen	243.833
7	Tilburg	Noord-Brabant	229.797
8	Almere	Flevoland	226.630
9	Breda	Noord-Brabant	188.217
10	Nijmegen	Gelderland	187.011
11	Apeldoorn	Gelderland	168.212
12	Haarlem	Noord-Holland	167.763
13	Arnhem	Gelderland	167.651
14	Haarlemmermeer	Noord-Holland	163.196



gemeente
Haarlemmermeer

Cybersecurity in-control



Security Governance & Beleid



Risk Management



Compliance reporting



Vulnerability Management



Security Monitoring & Incident Response (SIEM/SOC)



Privileged Access Management (PAM)



Mobile Device Management (MDM)



Cloud Security



gemeente
Haarlemmermeer



Agenda

- Aanleiding voor de Sentinel-implementatie
- SIEM/SOC landschap
- Rol van use cases bij de Sentinel-implementatie
- Aanpak
- Resultaat
- Lessons learned



gemeente
Haarlemmermeer

[Home](#) / [Gemeentelijk uitvoering](#) / [GGI-Veilig](#)

GGI-Veilig

GGI-Veilig helpt gemeenten hun digitale weerbaarheid te verhogen en hun ICT-infrastructuur veiliger te maken. GGI-Veilig bestaat uit een portfolio van producten en diensten voor operationele informatiebeveiliging. Via GGI-Veilig nemen gemeenten onder andere een actieve monitoring en response dienst af voor het

Gerelateerde thema's

› [Informatiesamenleving](#)



gemeente
Haarlemmermeer

Lessons learned GGI-veilig

Detectiecapaciteit en flexibiliteit

De KPN SIEM/SOC omgeving was qua architectuur en opbouw niet flexibel, waaronder nieuwe use cases niet (snel en efficiënt) doorgevoerd konden worden.

Cloud toepassingen monitoren

Het was niet mogelijk om security data uit cloud logbronnen zoals Microsoft365 te ontsluiten in de KPN SIEM-omgeving.

Proactieve monitoring door SOC-analisten

Een SIEM/SOC oplossing zonder 24/7 proactieve bewaking door een SOC heeft weinig toegevoegde waarde bij het realiseren van vroegtijdige detectie van dreigingen (inbraakpogingen) en security incidenten van de IT-infrastructuur.

Complexity



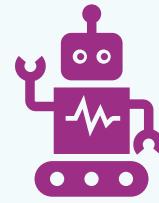
Speed of change

Innovation



Vulnerabilities

Software



New technology

AI, machine learning,
IoT, quantum computing

Attribution



Speed of change

International laws and regulations



Traceability on the internet

Hackers and cybercriminals

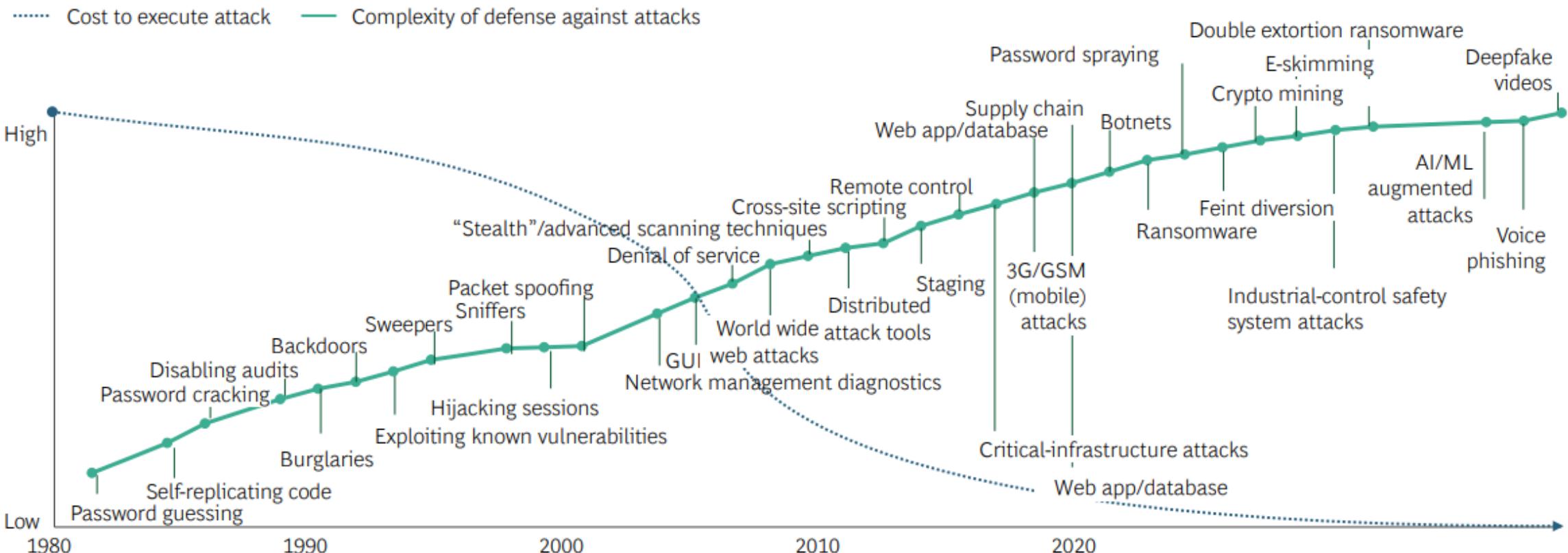


Cyberspace is unregulated

International cooperation
to combat cybercrime

Cyber attacks are increasingly cheaper to execute as technology advances; this leads to a need for increased complexity of defense

Illustrative





Cyberdreigingslandschap

- Artifical Intelligence | AI-based cyberaanvallen met geavanceerde malware
- Supply-chain aanvallen | aanvallen op ketenpartners en leveranciers | Third-party risk
- Complexe vormen van phishing met behulp van AI zoals deep-fake video, deep fake afbeeldingen en audio naast de reguliere BEC attacks
- Toename van complexiteit en kwantiteit m.b.t. gerichte ransomware aanvallen | beschikbaarheid van ransomware-as-a-service tools- en diensten.



Nieuws



Phishingaanval kost gemeente Haarlemmermeer 298.000 euro

dinsdag 27 december 2022, 15:02 door [Redactie](#), 10 reacties

Een phishingaanval kost de gemeente Haarlemmermeer 298.000 euro, zo is vorige week bekendgemaakt. De aanval deed zich vorige maand voor. Twee medewerkers van de gemeente traptten in een phishingmail waardoor aanvallers toegang tot de mailaccounts van de ambtenaren kregen. De phishingmails waren afkomstig van de e-mailaccounts van relaties van de gemeente, die zelf ook het slachtoffer van een phishingaanval waren geworden.

De aanvallers dienden vanuit één van de relaties een vervalste factuur in waarin het rekeningnummer was aangepast, zo meldt het [Noordhollands Dagblad](#). Naar dat rekeningnummer maakte de gemeente 118.000 euro over. Het herstel van de phishingaanval kost de gemeente nog eens **180.000 euro**. "Dit is iets dat je niet wil", zegt wethouder Charif El Idrissi. "We krijgen wekelijks tachtig meldingen van mogelijke phishing. We proberen die te voorkomen, maar het systeem is niet waterdicht." De gemeente heeft aangifte bij de politie gedaan.

- [Huis van Afgevaardigden VS verbiedt TikTok op werktelefoons](#)
- [Frankrijk gaat ziekenhuizen tegen ransomware-aanvallen beschermen](#)

[Reacties \(10\)](#)



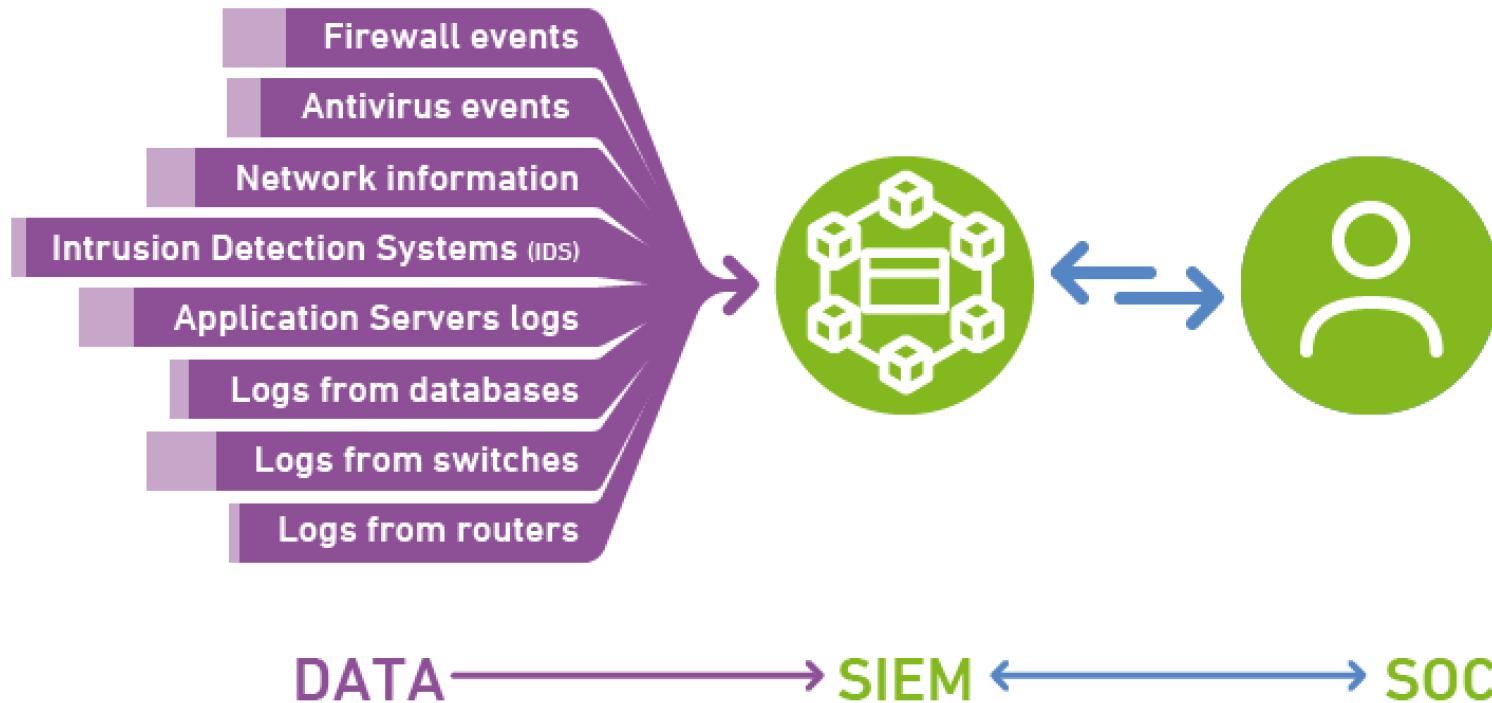
gemeente
Haarlemmermeer



A photograph of two surveillance cameras mounted on a black pole against a clear blue sky. The camera on the left is a dome-style camera with a white housing and a dark lens. The camera on the right is a bullet-style camera with a light-colored, elongated housing and a dark lens. Both cameras are mounted on articulated arms.

Wat is Security Monitoring?





gemeente
Haarlemmermeer

Mean Time
to
Detect (MTTD)

Mean Time to
Respond (MTTR)



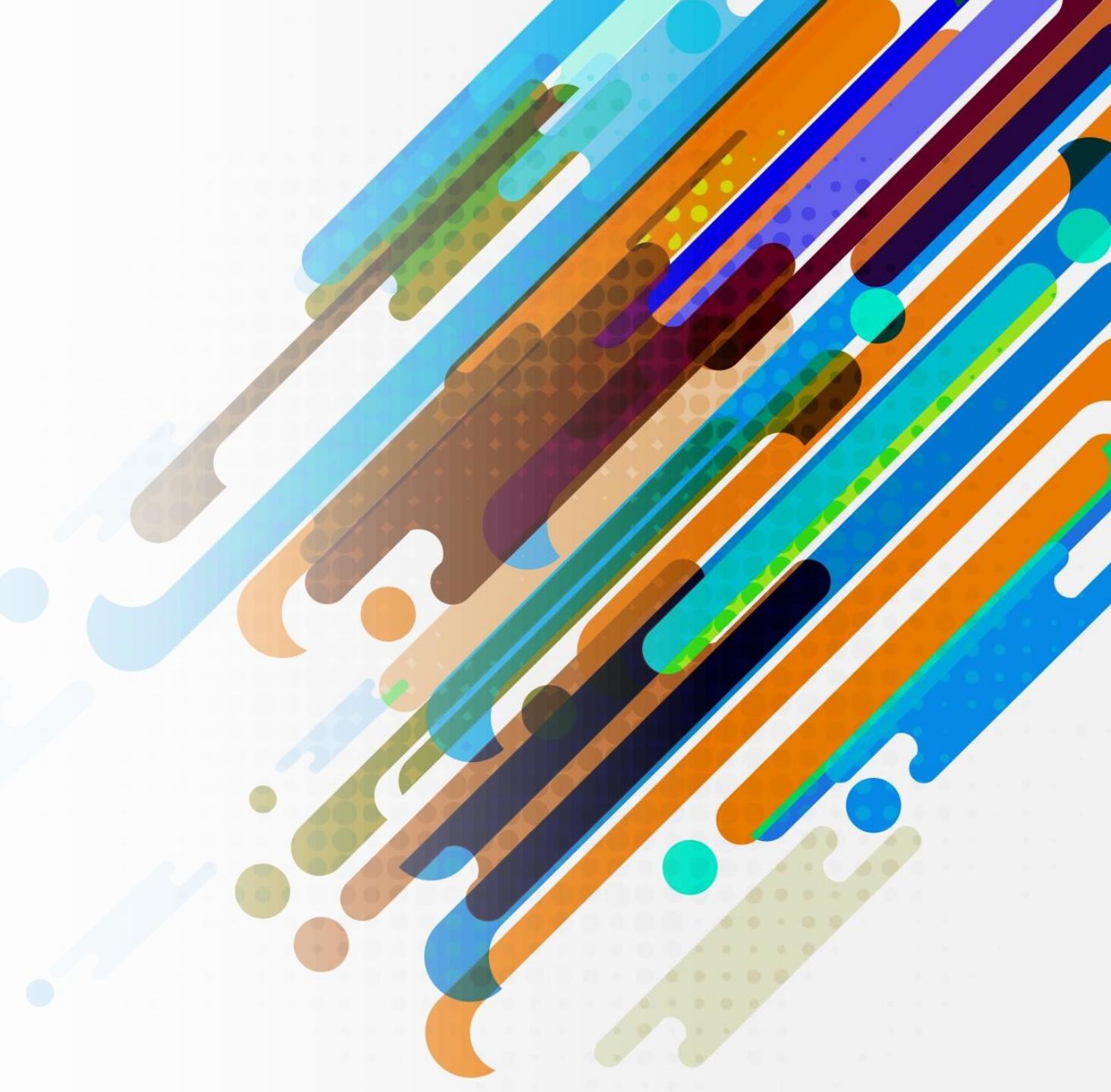
Detection

Finding a needle in a haystack

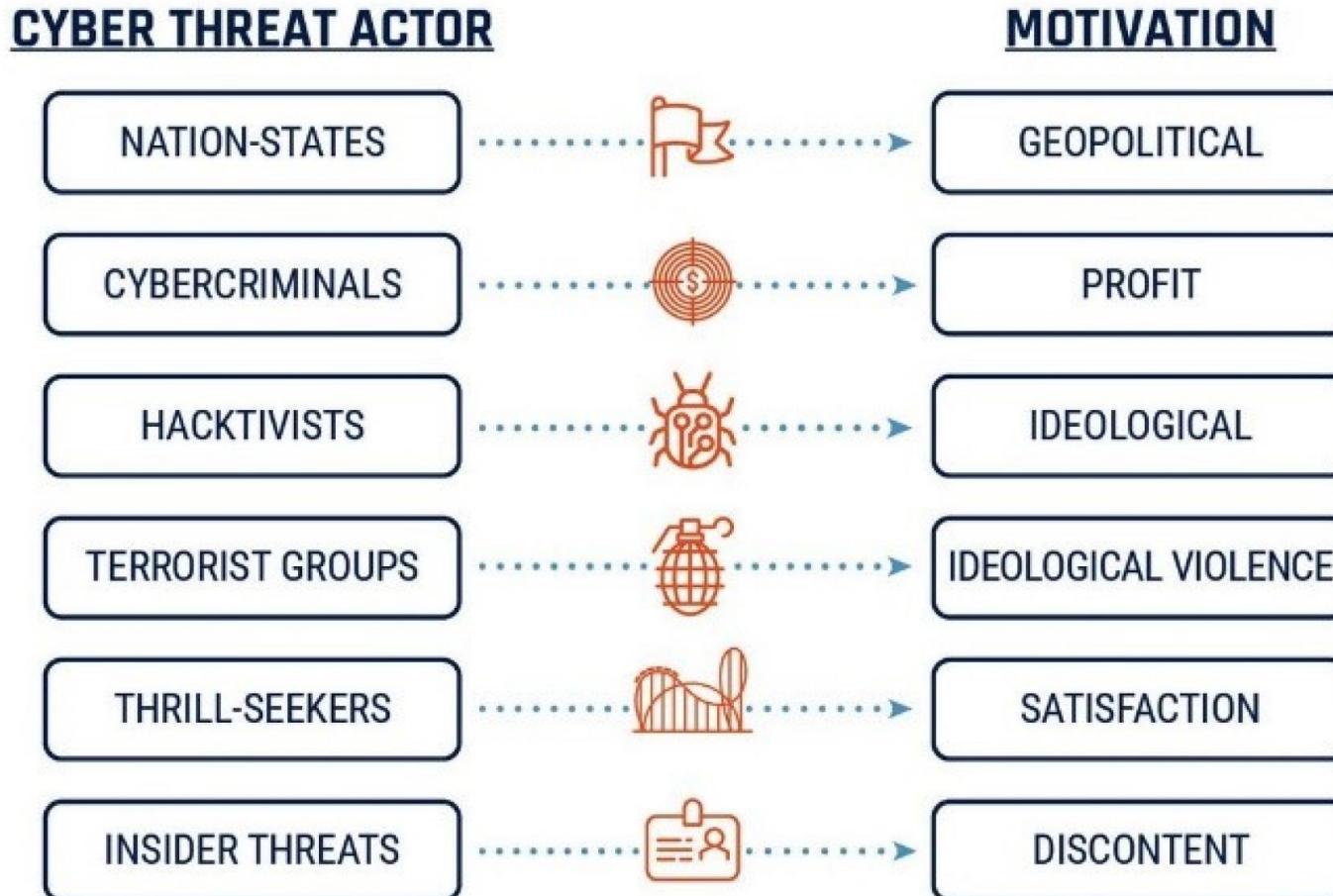


“There are known knowns. These are things we know that we know. **There are known unknowns.** That is to say, there are things that we know we don't know. **But there are also unknown unknowns.** There are things we don't know we don't know.”

Risk Appetite



CYBER THREAT ACTORS



SIEM capabilities

- Logmanagement
- Real-time security monitoring
- Threat Intelligence
- User Behaviour profiling
- Data- en end-user monitoring
- Application Monitoring
- Predictive Analytics
- Deployment & support simplicity



Proces

01

Identificatie
van risico's

02

Vertalen van
risico's naar
SIEM use cases

03

Implementatie
SIEM-tooling
en use cases

04

Analyse en
proces
optimalisatie

05

Follow-up op
alerts en
incidenten

Proces

01

Identificatie
van risico's

02

Vertalen van
risico's naar
SIEM use cases

03

Implementatie
SIEM-tooling
en use cases

04

Analyse en
proces
optimalisatie

05

Follow-up op
alerts en
incidenten

A wide-angle, low-light photograph taken from an airport control tower at night. In the foreground, the dark interior of the control room is visible, featuring several large computer monitors displaying flight information and maps. Through the glass windows of the tower, a brightly lit city skyline is visible in the distance. In the middle ground, the airport tarmac is filled with several aircraft, including a prominent white airplane with blue accents. The sky above is dark, with some light trails from planes or traffic visible.

Sourcing Strategie

Scenario's

- Scenario 1 – In-house SIEM/SOC
- Scenario 2 – Uitbesteden van SIEM/SOC
- Scenario 3 – Hybride SIEM/SOC oplossing

Criteria

Security Strategie

Kwaliteit dienstverlening / functionaliteit systeem

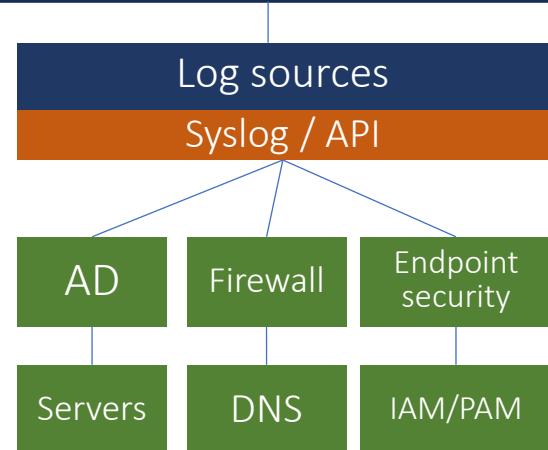
Kosten

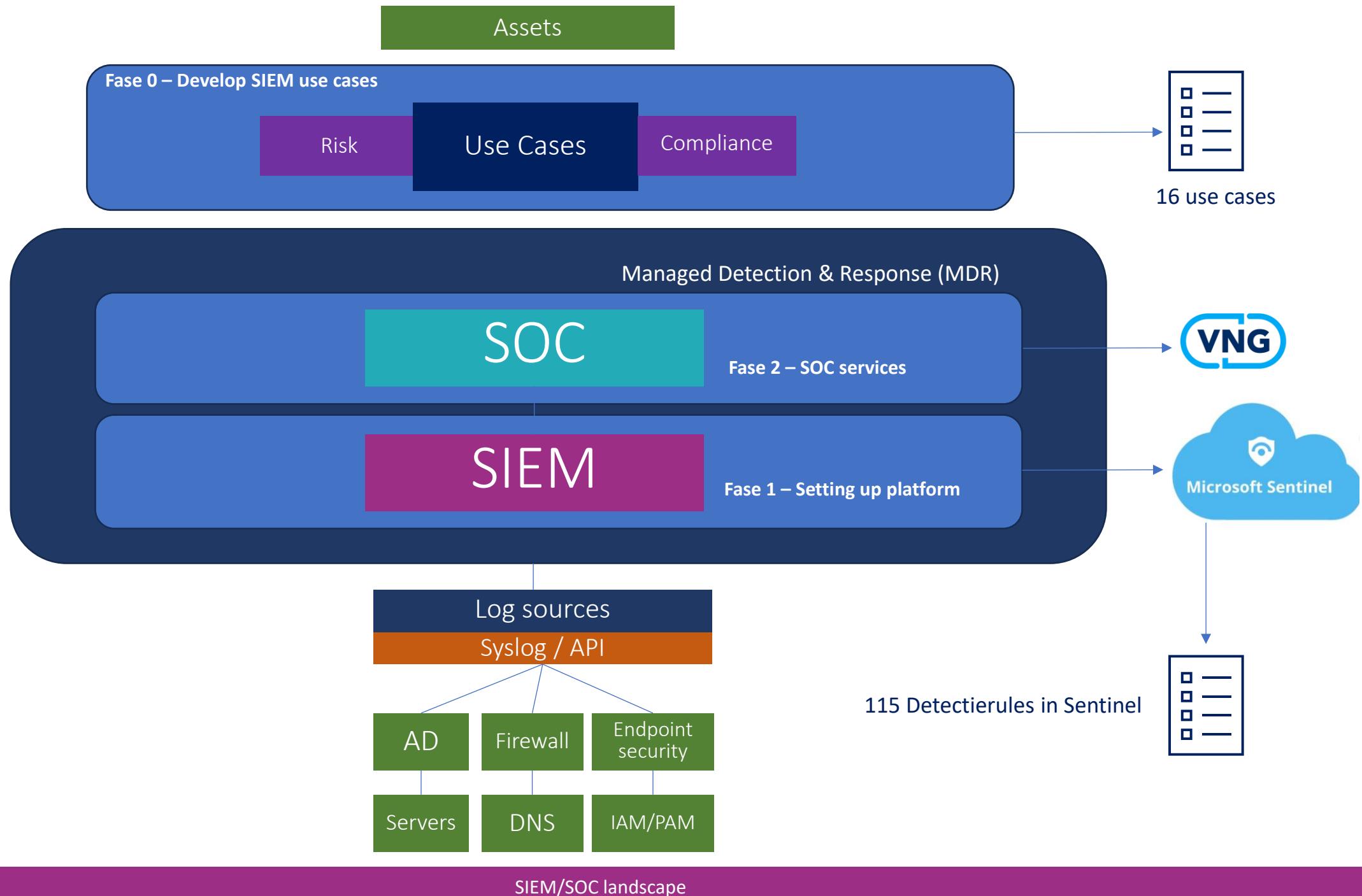
Beheer

Expertise

A wide-angle aerial photograph of a large international airport. The foreground shows a runway with several commercial airplanes, including one with red and white livery. In the background, there are more runways, a terminal building, and surrounding urban areas under a clear sky.

SIEM/SOC landscape



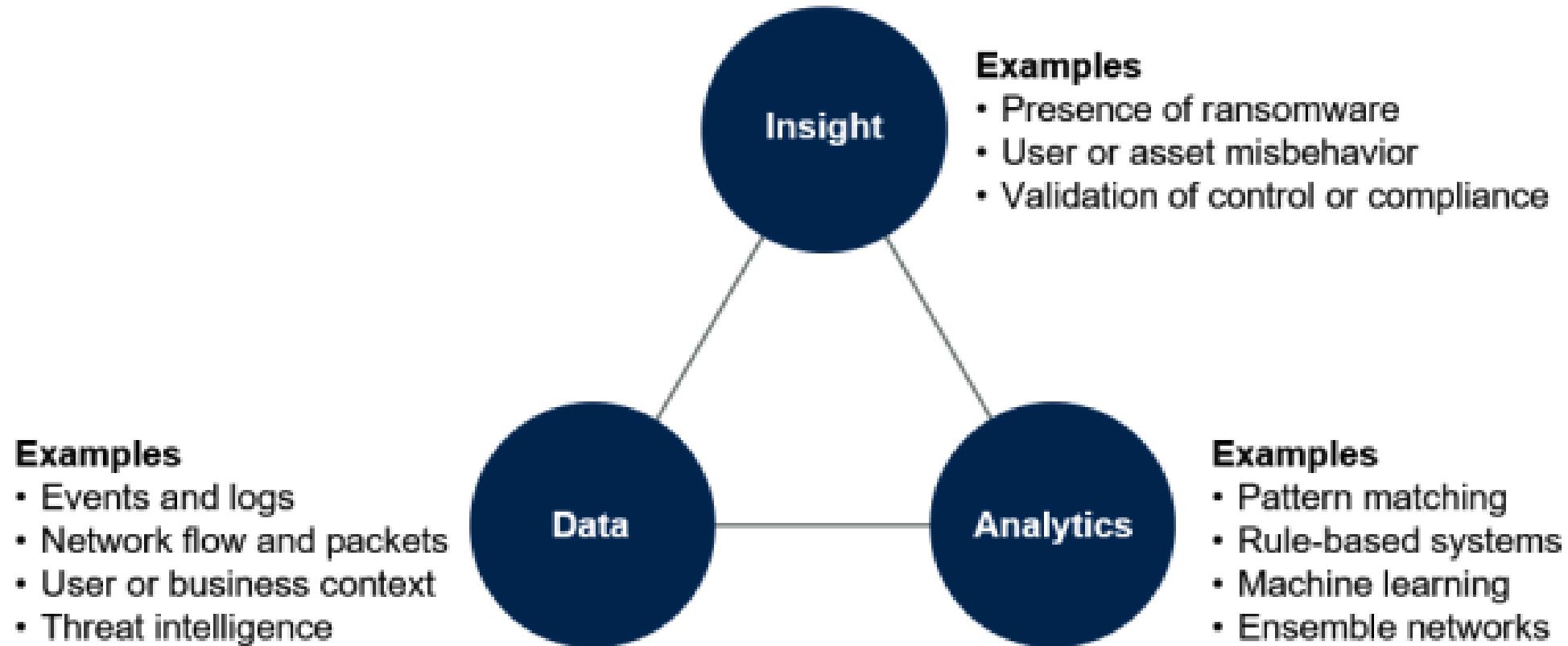




SIEM Use Case Development

- **Workshops**
 - Getting insights and input of the system administrators, information security team/CISO and application managers.
- **Frameworks**
 - Lockheed Martin's Cyber Kill Chain
 - MITRE ATT&CK framework
- **Knowledge base van cybersecurity vendoren**
- **Cybersecurity Threat Reports**
 - **VNG IBD** Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2023/2024
 - **NCSC** Cybersecuritybeeld Nederland 2023

The Use-Case Triangle



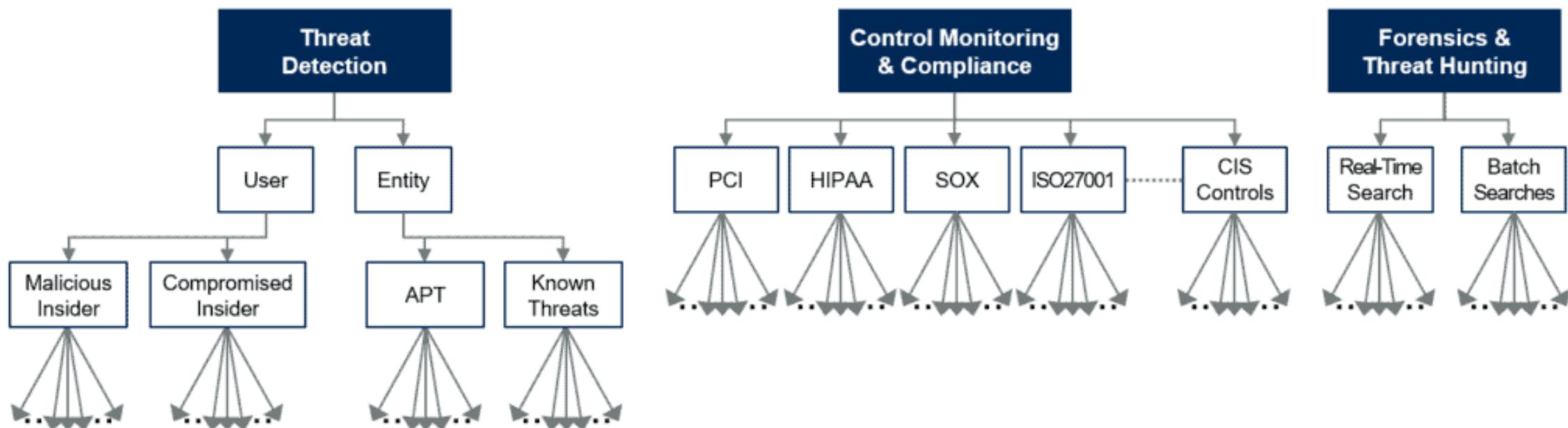
Source: Gartner
ID: 382579

Security Monitoring Use Cases

- Compliance based
- Threat-based
- Assets based



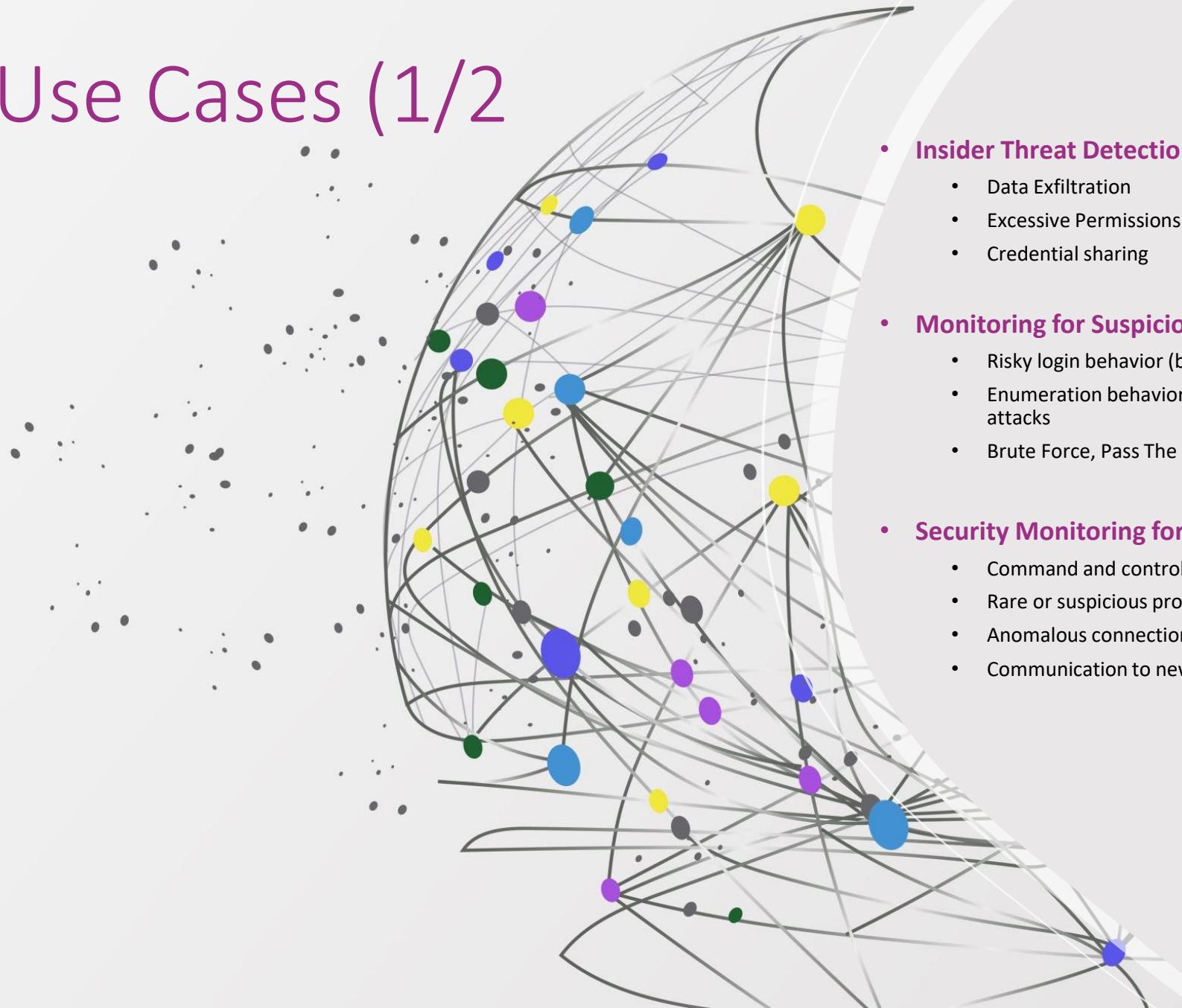
Organization Structure for Use Cases



Source: Gartner
ID: 382579

SIEM Use Cases (1/2)

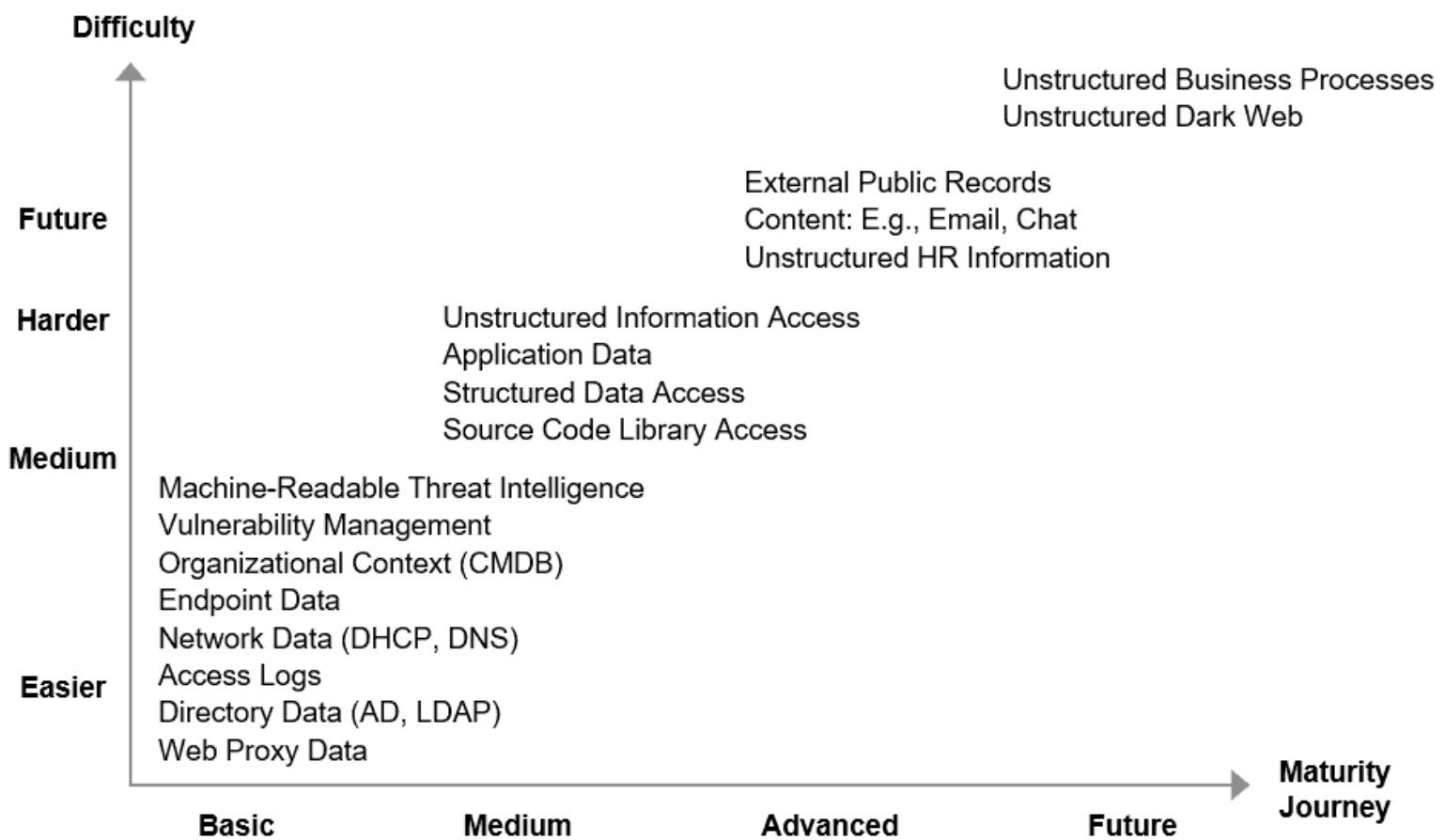
- **Insider Threat Detection**
 - Data Exfiltration
 - Excessive Permissions
 - Credential sharing
- **Monitoring for Suspicious Logins and Account Compromise**
 - Risky login behavior (based on time, geolocation, IP address, etc.)
 - Enumeration behavior patterns to detect sophisticated brute force attacks
 - Brute Force, Pass The Hash, Golden Ticket attacks
- **Security Monitoring for Host Compromise**
 - Command and control (C2) communication/beaconing
 - Rare or suspicious process execution
 - Anomalous connection patterns
 - Communication to newly registered or unregistered domains



SIEM Use Cases (2/2)

- Detection of Anomalous behavior
- Detection of malware
- Security Monitoring of Cloud Applications
- Unusual behavior on privileged accounts
- Traffic to malicious domains
- System changes
- Security Monitoring of VPN and Remote Authentication Devices
- License and Compliance Monitoring (PKI-certificates)

Difficulty Level in Managing Data Sources



Source: Gartner
ID: 382579



De rol van use cases bij de Microsoft Sentinel-
implementatie bij gemeente Haarlemmermeer

The added value of use cases

- The implementation of Microsoft Sentinel was more effective because the use cases **provided direction for the design and configuration** of the detection rules, analytics rules and the building of the fusions.
- The use cases were used in connection with a **formal testing and acceptance plan for the Microsoft Sentinel implementation**. So that the detection capability demonstrably works in rapid detection of possible threats, deviations and security incidents.
- **Cost control** because your **data ingestion** to the Sentinel environment remains under control.



Our Approach

- De output van de workshops hebben we gebruikt voor het opstellen van SIEM use cases.
- Vervolgens is er een marktuitvraag opgesteld en een leverancier gecontracteerd.
- De implementatiepartner heeft op basis van de marktuitvraag een statement-of-work gemaakt die gebruikt is voor de implementatie.
- Het projectteam had **mandaat** en er waren voldoende **resources** vrijgespeeld.
- Het testen van de werking van de use cases en detectieregels in Microsoft Sentinel was **een belangrijk onderdeel om de kwaliteit te waarborgen** van de detectie- en security monitoring oplossing.





The Results

- Er zijn in totaal **16 SIEM use cases** ontwikkeld en geïmplementeerd.
- Dit heeft geleid tot **115 detectieregels** in Microsoft Sentinel.
- Na de implementatie van Microsoft Sentinel heeft er een **formeel test- en acceptatieproces** plaatsvonden.
- De vervolgstap is dat in Q2 2024 een mini-competitie wordt gedaan om een **SOC-dienstverlener** te contracteren via de VNG.

SIEM Use Cases

- Identity and Access (three use cases)
- Identity-based Attacks
- User and Entity Behavior Analytics (UEBA)
- Audit trial
- Microsoft365
- DNS tunneling
- Protecting important servers
- Detection of malware on servers and endpoints
- Unusual behavior on privileged accounts
- Detection of lateral movement
- Network traffic use cases
- Traffic to malicious domains
- Endpoint security
- Detection of (spear) phishing and webbased attacks
- Forensics
- Compliance based security monitoring (DigiD use case)



Microsoft Azure Search resources, services, and docs (G+)

PAM-AZ-SecurityAnalyst GEMEENTE HAARLEMMEER (..)

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | MITRE ATT&CK (Preview) ...

Selected workspace: 'log-analytics-sentinel'

Search by technique... Matrices type view : 13 selected Sentinel detections : All Active ① Active scheduled query rules, ... Simulated ① Analytics rule templates Legend ① 0 1-5 6-10 11+

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques	13 techniques	42 techniques	17 techniques	31 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning	Acquire Access	2 Drive-by Compromise	14 Command and Scripting... +9 Simulated	19 Account Manipulation +5 Simulated	2 Abuse Elevation Control...	Abuse Elevation Control...	1 Man-in-the-Middle	9 Account Discovery +6 Simulated	2 Exploitation of Remote Services +1 Simulated	Man-in-the-Middle	8 Application Layer Protocol +1 Simulated	4 Automated Exfiltration +1 Simulated	6 Account Access Removal
Gather Victim Host...	Acquire Infrastructure	9 Exploit Public-Facing... +2 Simulated	4 Exploitation for Client Execution +3 Simulated	BITS Jobs	Access Token Manipulation	Access Token Manipulation	21 Brute Force +7 Simulated	Application Window...	Internal Spearphishing	Archive Collected Data	Communication Through...	9 Data Transfer Size Limits +3 Simulated	7 Data Destruction +4 Simulated
Gather Victim Identity...	Compromise Accounts	3 External Remote Services	Inter-Process Communication	Boot or Logon Autostart...	Boot or Logon Autostart...	BITS Jobs	Credentials from Password Stores	Browser Bookmark...	1 Lateral Tool Transfer	Audio Capture	1 Data Encoding	1 Exfiltration Over Alternative... +1 Simulated	Data Encrypted for Impact
1 Gather Victim Network... +1 Simulated	Compromise Infrastructure	Hardware Additions	Native API	Boot or Logon Initialization...	Boot or Logon Initialization...	Debugger Evasion	Exploitation for Credential...	Debugger Evasion	Remote Service Session...	Automated Collection	1 Data Obfuscation	3 Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Develop Capabilities	3 Phishing +1 Simulated	Scheduled Task/Job	Browser Extensions	Create or Modify System Process	4 Deobfuscate/Decode Files or...	Forced Authentication	Device Driver Discovery	2 Remote Services	Man in the Browser	11 Dynamic Resolution +4 Simulated	4 Exfiltration Over Other Network...	Defacement
Phishing for Information	Establish Avenues	1 Replication Through...	Shared Modules	2 Compromise Client Software...	1 Domain Policy Manipulation	Direct Volume Access	Forge Web Credentials	Domain Trust Discovery	Replication Through...	Clipboard Data	3 Encrypted Channel	Exfiltration Over Physical...	Disk Wipe

A use case-driven approach to improve your detection capability against cyber threats



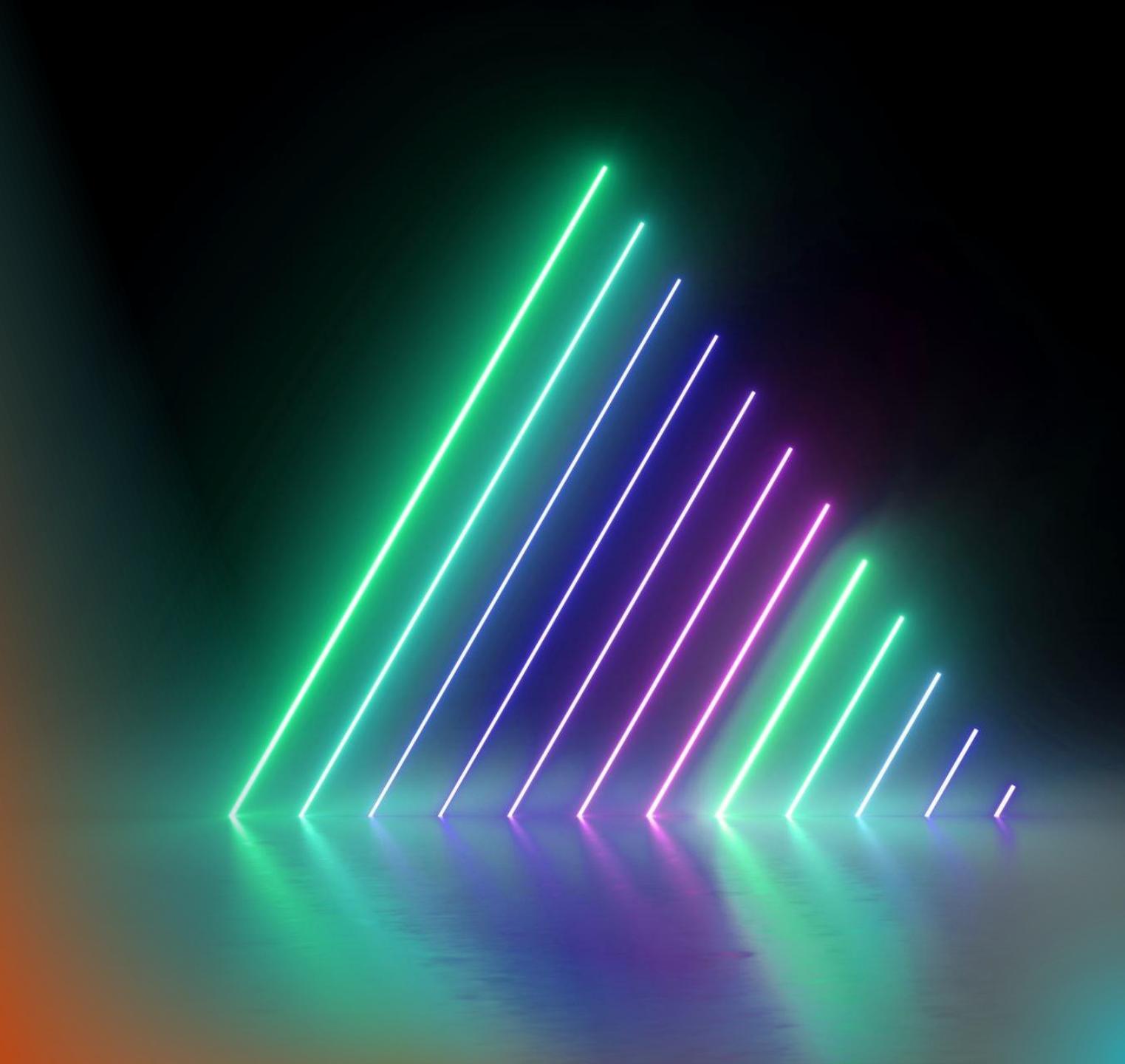
Microsoft Sentinel

- **Integration** with other (Microsoft) security solutions.
- Possibility to connect the SIEM application to suppliers that offer **SOC services based on Microsoft Sentinel**.
- There is a mapping available in Microsoft Sentinel with the **BIO compliance** requirements.
- Cloud Security Alliance (CSA) STAR certificering.
- Sentinel is a **cloud-native SIEM/SOAR** solution, which fits well with the **future situation**. We are working on a transition of our on-prem IT infrastructure to Microsoft's Azure cloud.
- Powerfull **threat intelligence** and **AI/ML**.

Gartner Magic Quadrant SIEM

Figure 1: Magic Quadrant for Security Information and Event Management



The background of the slide features an abstract design of glowing lines. These lines are primarily white and green, set against a dark, textured background that appears to be a floor or wall. The lines converge towards the top left of the frame, creating a sense of depth and perspective. Some lines are longer and more prominent, while others are shorter and fade into the background.

Lessons learned

- De **projectvoorbereiding** is belangrijk en biedt sturing op de daadwerkelijke inrichting en configuratie van een SIEM-oplossing, is onze ervaring.
- Start met een **risico inventarisatie** en het opstellen van SIEM use cases alvorens je start met het project.
- Houd rekening met de **toekomstige ontwikkelingen** in het IT landschap van je organisatie, bijv. een cloud transitie.
- Het bepalen van de **scope** en **fasering** van het SIEM-project is belangrijk.
- Bij de uitvraag en **selectie van implementatiepartner** is het belangrijk om specifiek te zijn wat je van het SIEM-project verwacht qua resultaat en detectiemogelijkheden.
- Bouw een **formeel test- en acceptatieproces** is voor alle use cases, het project wordt pas opgeleverd als de leverancier de use cases c.q. detectieregels **aantoonbaar** heeft ingericht en de klant het akkoord heeft bevonden.



CONFIDENTIETY

IDENTITY SECURITY EXPERTS

Accelerate | Adopt | Interact | Govern

#Vragen?

Met nieuwe inzichten starten aan je IT-security roadmap?

Wij kunnen je helpen met security compliancy,
PAM en SIEM/SOC implementaties.

Behoefte aan een inspiratiesessie?
Meld je dan aan via info@confidentity.nl

www.confidentity.nl