We gaan bijna beginnen...
10:00

Jan Willem Molenaar — Presales Consultant

Thijs Bisseling — Presales Consultant

Lessons learned van een ransomware aanval

28 februari 2024

Jan Willem Molenaar — Presales Consultant

Thijs Bisseling — Presales Consultant

Agenda

- Intro
- Welke fases zijn er bij een cyberaanval
- Je bent alsnog gehackt.... Wat nu? Praktijkvoorbeeld
- Samenvattend

Lessons learned van een ransomware aanval

Even voorstellen

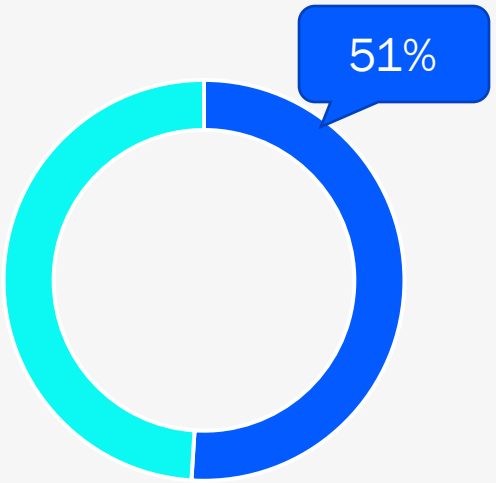
Thijs Bisseling
Pre-Sales Consultant
LinkedIn

Jan Willem Molenaar
IT Architect
LinkedIn

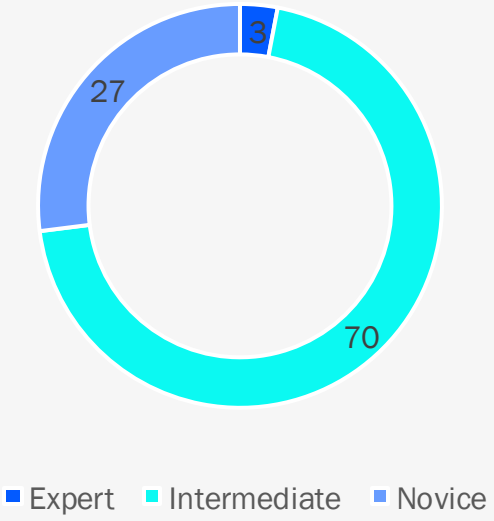
Cybersecurity

Waar staan we vandaag de dag?

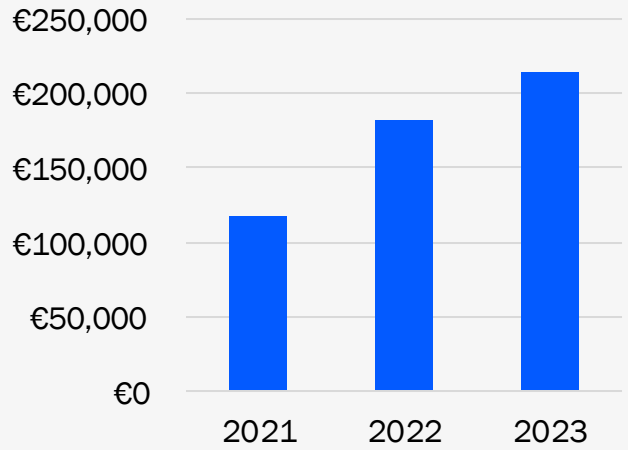
Meer dan de helft van de bedrijven heeft te maken gehad met een cyberaaanval



Cyber volwassenheid in Nederland



Mediaan schadekosten is gestegen met 55%



Bron: Hiscox-Cyber-Readiness-Report-2023.pdf (hiscoxgroup.com)

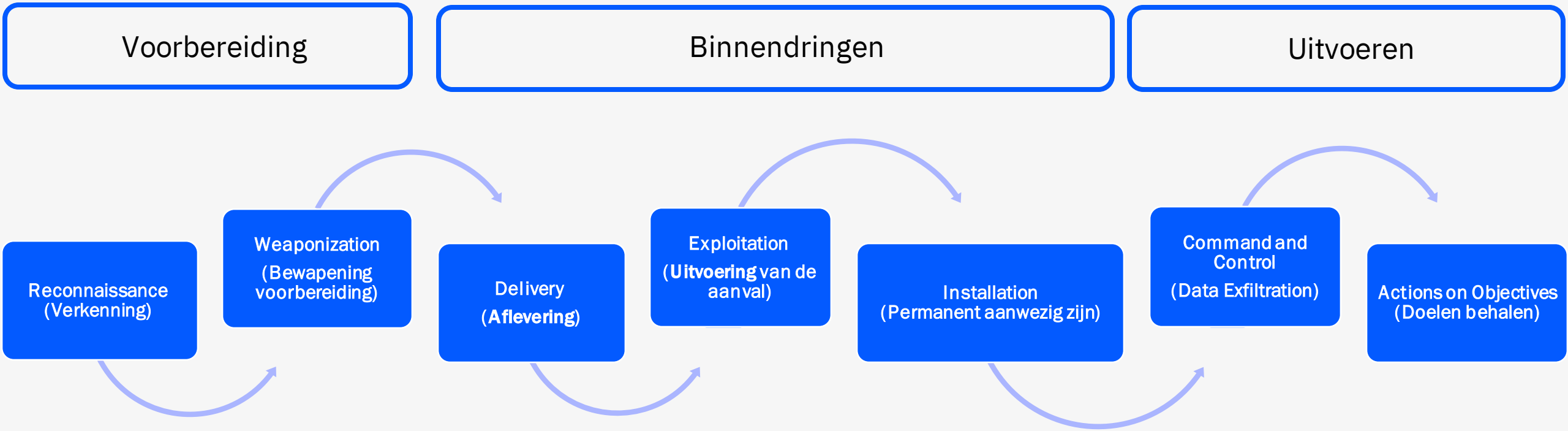
- Iedereen heeft een brandverzekering. De kans op een brand is 1 op 8000 en de schade gemiddeld € 13.790,-

- Inmiddels heeft 56% (in 2020 was het nog maar 20%) van het MKB een cybersecurity verzekering. De kans op een cyberaanval is 1 op 8 en de schade is gemiddeld € 270.000,-

Welke fases zijn er bij een Cyberaanval

Cyber Kill Chain

7 fases bij cybercrime



Fase 1: Reconnaissance

Verkenning (Informatie verzamelen)

- De aanvaller verzamelt informatie over het doelwit, zoals netwerkinfrastructuur, systeemconfiguraties, en mogelijke zwakke punten. Dit kan gebeuren via openbare bronnen, social media, of zelfs directe interacties met het doelwit.

Reconnaissance
(Verkenning)

Fase 2: Weaponization

Bewapening (Voorbereiding)

• De aanvaller verzamelt informatie over het doelwit, zoals netwerkinfrastructuur, systeemconfiguraties, en mogelijke zwakke punten. Dit kan gebeuren via openbare bronnen, social media, of zelfs directe inte
doe

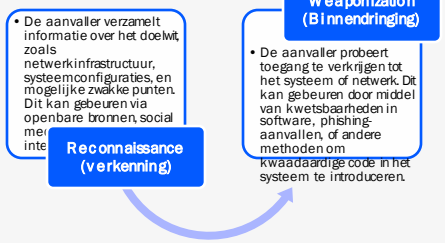
Reconnaissance (verkenning)

Weaponization (Bewapening voorbereiding)

- De aanvaller bepaalt wat hij nodig heeft **om** binnen te komen. Dit kan gebeuren **doormiddel** van kwetsbaarheden in software, phishing-aanvallen, of andere methoden om kwaadaardige code in het systeem te introduceren.

Fase 3: Delivery

Aflevering

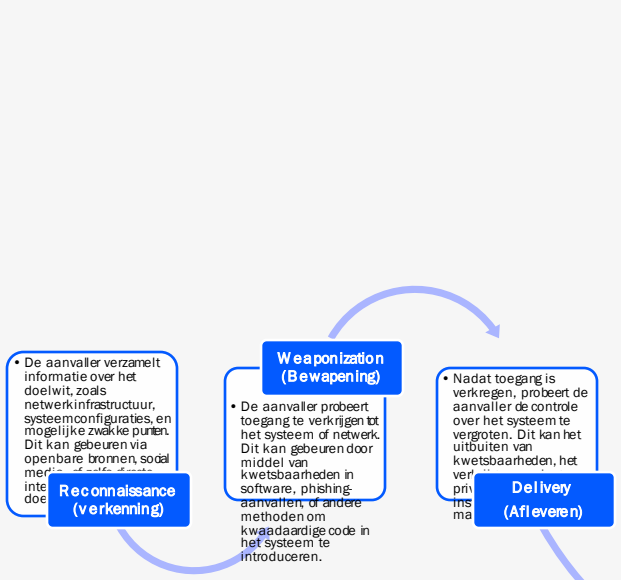


- De aanval wordt uitgevoerd door bijvoorbeeld via email of USB software te verstoppen. Via een vulnerability is veelal geen medewerker nodig om de malware te installeren.

Delivery (Aflevering)

Fase 4: Exploitation

Uitvoering van de aanval



Exploitation (uitvoering van de aanval)

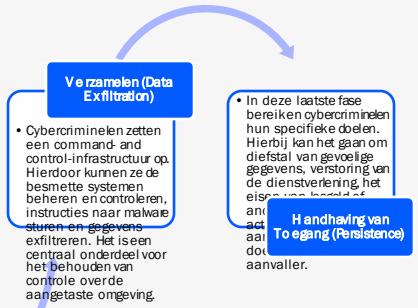
- In deze fase maken aanvallers gebruik van de kwetsbaarheden die ze hebben ontdekt in eerdere stadia om verder in het netwerk van een doelwit te infiltreren en hun doelstellingen te bereiken.

Fase 5: Installation (Persistence)

Permanent aanwezig zijn

- Zodra toegang is verkregen, installeert de cybercrimineel de schadelijke software of vestigt hij zich permanent in het aangetaste systeem. Hierbij kan het gaan om het creëren van “backdoors” of andere middelen om de toegang te behouden, zelfs nadat de eerste toegangspunten zijn gesloten.

Installation (Permanent aanwezig zijn)



Fase 6: Command and Control (C2)

In controle zijn van de besmette systemen

Command and Control (Data Exfiltration)

- Cybercriminelen zetten een command- and control-infrastructuur op. Hierdoor kunnen ze de besmette systemen beheren en controleren, instructies naar malware sturen en gegevens exfiltreren. Het is een centraal onderdeel voor het behouden van controle over de aangetaste omgeving.

• In deze laatste fase bereiken cybercriminelen hun specifieke doelen. Hierbij kan het gaan om diefstal van gevoelige gegevens, verstoring van de
eis
act
doelstellingen van de aanvaller.

Handhaving van Toegang (Persistence)

Fase 7: Actions on Objectives

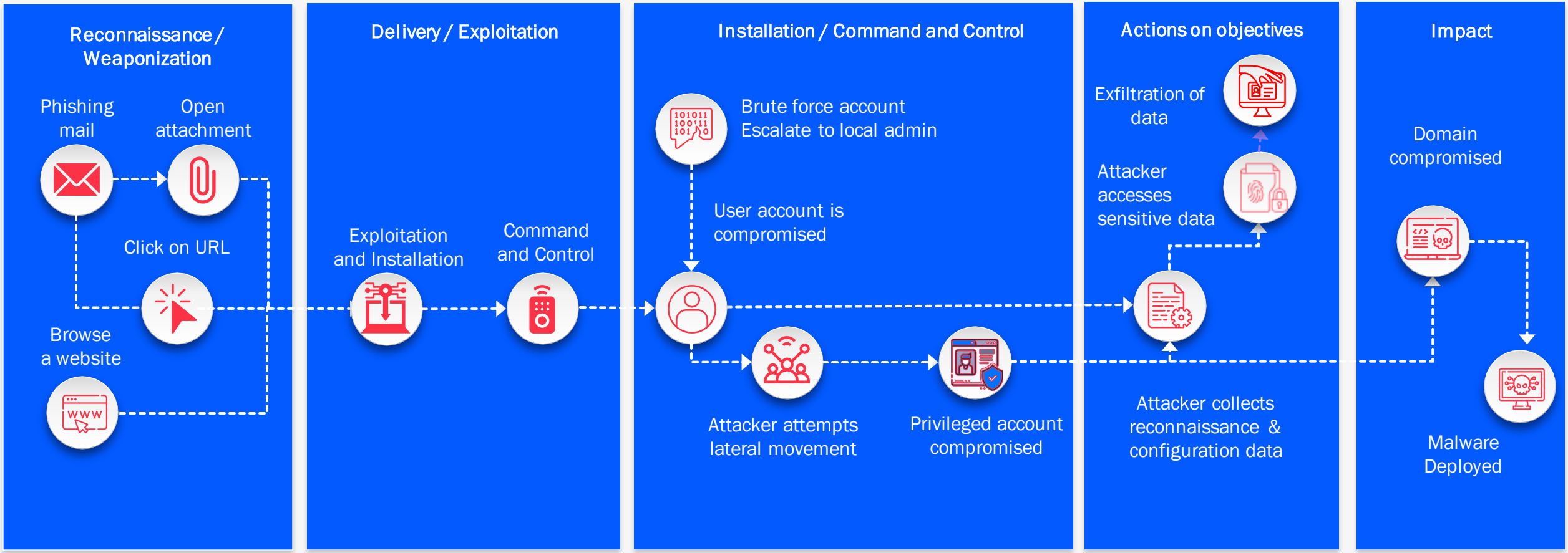
Doelen behalen

- In deze laatste fase bereiken cybercriminelen hun specifieke doelen. Hierbij kan het gaan om diefstal van gevoelige gegevens, verstoring van de dienstverlening, het eisen van losgeld of andere kwaadaardige activiteiten die aansluiten bij de doelstellingen van de aanvaller.

Actions on Objectives (Doelen behalen)

Voorbeeld: Ransomware Attack

Hoe een hacker binnenkomt op een systeem

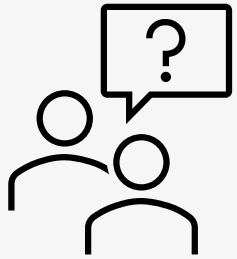


Je bent alsnog gehackt.... Wat nu?

Praktijkvoorbeeld

Wat gebeurde er?

Februari 2022



De IT-afdeling krijgt de eerste meldingen binnen van medewerkers **die melden** dat bepaalde applicaties niet functioneren.

Wat gebeurde er?

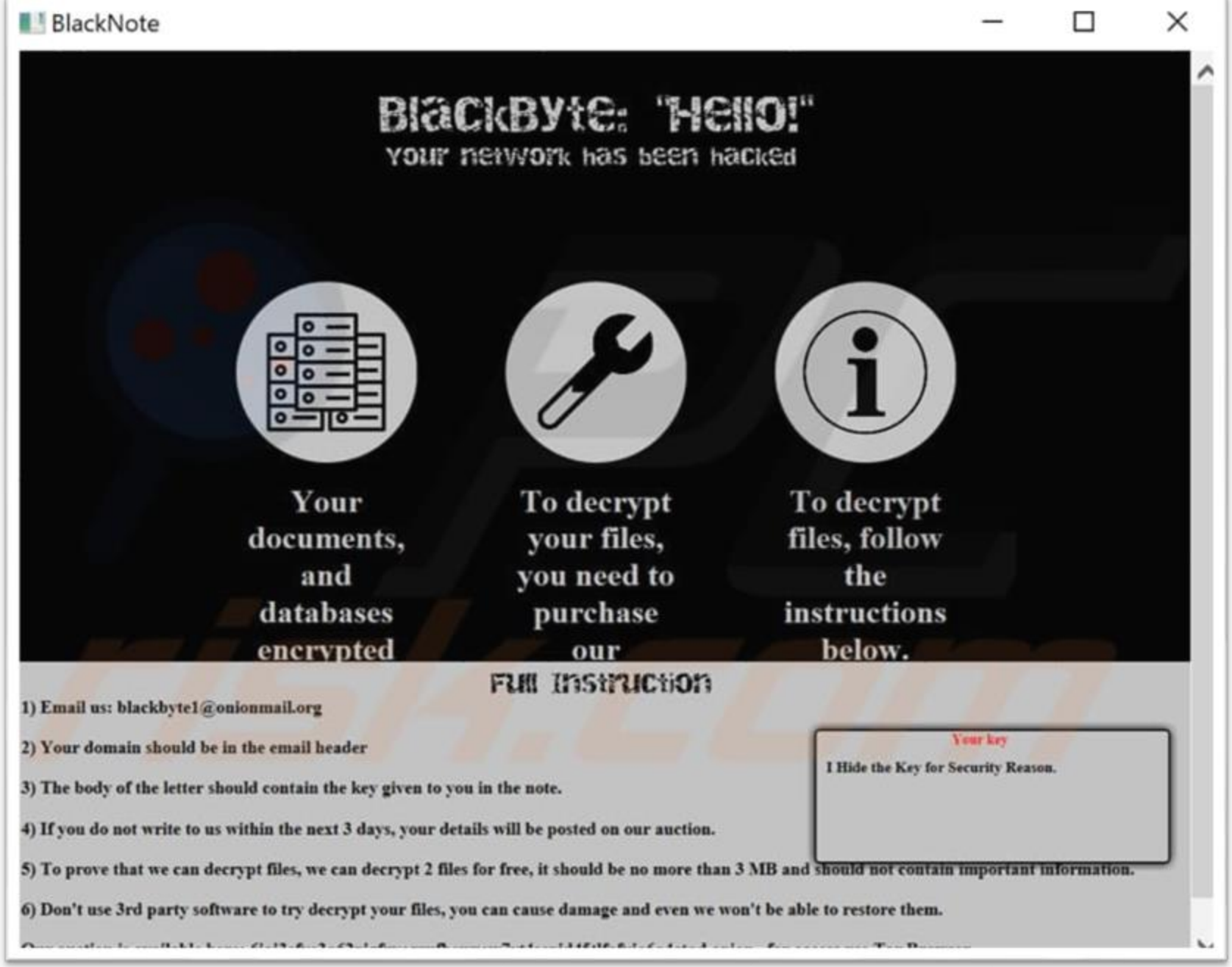
Februari 2022

Al snel constateert de IT-afdeling dat ze getroffen zijn door een ransomware aanval.

Wat gebeurde er?

Februari 2022

Ook verschijnen deze meldingen op werkplekken.


BlackNote
BlackByte: "Hello!"
Your network has been hacked
Your documents, and databases encrypted
To decrypt your files, you need to purchase our
To decrypt files, follow the instructions below.
Full Instruction
1) Email us: blackbyte1@onionmail.org
2) Your domain should be in the email header
3) The body of the letter should contain the key given to you in the note.
4) If you do not write to us within the next 3 days, your details will be posted on our auction.
5) To prove that we can decrypt files, we can decrypt 2 files for free, it should be no more than 3 MB and should not contain important information.
6) Don't use 3rd party software to try decrypt your files, you can cause damage and even we won't be able to restore them.
Your key
I Hide the Key for Security Reason.

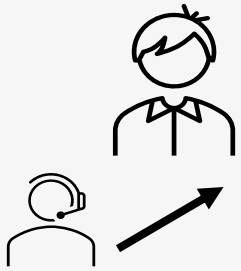
Wat gebeurde er?

Februari 2022

IT-afdeling neemt contact op met Ekco (stand-by).

Wat gebeurde er?

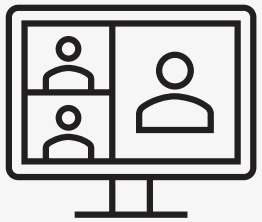
Februari 2022



Escalatie naar Incident Manager.

Wat gebeurde er?

Februari 2022



Conference call met IT afdeling en Ekco.

Vraag klant: “Ik denk dat we backups moeten terugzetten???”…

Wat gebeurde er?

Februari 2022

Op basis van de feiten die tot dan **bekend** waren… advies Ekco.

“ZET ALLE SYSTEMEN UIT”

“Klant beschikt niet over een Cybersecurity verzekering”

“Toch advies: Schakel een Cybersecurity Forensisch Expert in”

“Wacht op acties en advies van Cybersecurity Forensisch Expert”

Wat gebeurde er?

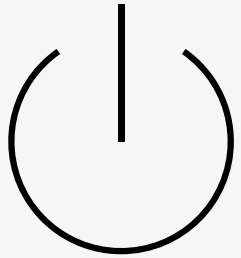
Februari 2022

Ondertussen treft Ekco al voorbereidingen.

“Hardware wordt geregeld voor een eventuele restore”

Hoe nu verder?

De tijd tikt door.....



Alles staat nog steeds uit. Ook geen internet toegang.

“Kritieke meetings werden gedaan via telefoon of mobiele hotspot”

“Ondanks mobiele hotspot werd toch nog tijdens een meeting en laptop gelocked”

Hoe nu verder?

De tijd tikt door.....

Er is inmiddels contact geweest met een Cybersecurity Forensisch Expert.

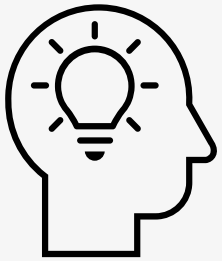
“Zij hebben de casus aangenomen”

“Een offerte / opdrachtbevestiging wordt gemaakt”

“Ondertussen wordt in de planning gekeken wanneer het onderzoek gestart kan worden. (Gelukkig de dag daarna)”

Hoe nu verder?

De tijd tikt door.....

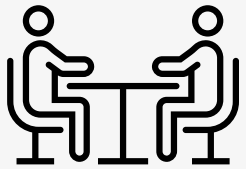


Er dient een analyse gedaan te worden op de besmette omgeving.

“Een kopie van de servers wordt naar de tijdelijke hardware geplaatst”

Ondertussen

Onderhandeling

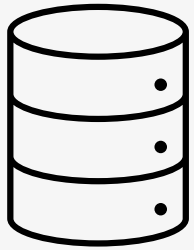


De Cybersecurity Forensisch Expert houdt nauw contact met de hackergroep.

“Om tijd te winnen wordt er onderhandeld over het losgeld”

Analyse

De tijd tikt door....

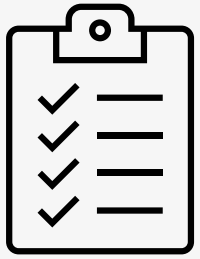


BACKUP! Eindelijk een lichtpuntje. De backup van de backup is niet geraakt.

“Doordat de backup immutable was, is de backup van de backup nog beschikbaar”

Plan maken

Tijd voor een Disaster Recovery Plan



Er was geen Disaster Recovery Plan. Deze werd samen met Ekco gemaakt.

“Welke applicaties zijn het meest belangrijk?”

“Welke servers moeten in welke volgorde opstarten?”

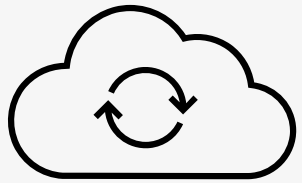
“Welke data meest belangrijk?”

“Wie kan wat testen?”

“Hoe weten we zeker dat we niet meer besmet zijn?”

Het herstel

Ook dit kost veel tijd



Nu kunnen de servers vanuit de backup hersteld worden....

“Het team test de IT omgeving”

“Het team test de applicaties”

De forensische experts blijven meekijken en houden alles nauwlettend in de gaten.

“Wie kan wat testen?”

“Hoe weten we zeker dat we niet meer besmet zijn?”

Het resultaat

Twee weken verder...

Na uitgebreide testen en onderzoek is de IT-omgeving hersteld en “schoon”.

Geen losgeld betaald aan de hackersgroep.

Tussen de €300.000,- en €400.000 schade (out of pocket). Derving en reputatieschade niet meegeteld.

Productie draait weer.

Kantoorautomatisering is hersteld.

Er is nog veel nazorg voor de organisatie. Denk aan facturatieprocessen, handmatige processen en communicatie met klanten en leveranciers.

Immutable BACKUP 🙏

Je bent alsnog gehackt.... Wat nu?

Wat was nu uiteindelijk de oorzaak?

De oorzaak

Een “on-premises” mailserver was niet up-to-date	Fase 1: Verkenning	
De hackers hebben een exploit voor de vulnerability	Fase 2: Weaponization	
De hackers krijgen toegang tot de mailserver en van daaruit tot meerdere systemen in de organisatie	Fase 3: Delivery	
Via Domain Admin rechten toegang tot AD en een GPO geïmplementeerd	Fase 3: Delivery	
Via deze GPO wordt de malware encryptie software over de hele organisatie gedistribueerd	Fase 4: Exploitation	
De aanval is gestart. Bestanden worden versleuteld	Fase 5: Installation	
De hackers hadden ook nog “achterdeurtjes” om de machines via Remote Control over te nemen	Fase 6: Command and Control	
Uit forensisch onderzoek bleek dat de hackers alle servers en werkplekken in controle hadden	Fase 6: Command and Control	
Nadat de aanval uit fase 4 in volle gang is, eisen de hackers “losgeld” via diverse schermen op de werkplekken.	Fase 7: Actions on Objectives	

Je bent alsnog gehackt.... Wat nu?

Wat kun je er nu al aan doen?

Kill Cyber Kill Chain

Stappen die jouw organisatie kan zetten om de “Kill chain” te verstoren

Reconnaissance (Verkenning)

- ✓ Let op je aanwezigheid op sociale media
- ✓ Wees geen doelwit
- ✓ Gebruik verschillende wachtwoorden
- ✓ Check “haveibeenpwned.com”

Weaponization (Bewapening voorbereiden)

- ✓ Men creëert wapen. Er kan geen actie worden ondernomen.

Delivery (Uitbouw)

- ✓ Antivirus
- ✓ E-mail en webfiltering
- ✓ Educatie
- ✓ Gebruikers awareness
- ✓ Limiteer gebruik van USB
- ✓ Blokkeer autorun

Exploitation (uitvoering van de aanval)

- ✓ Patchen en updates
- ✓ Vulnerability scanning
- ✓ Beveilig websites en webapplicaties

Installation (Permanent aanwezig zijn)

- ✓ Antivirus
- ✓ Goed beheer over admin credentials
- ✓ Multifactor Authenticatie
- ✓ Whitelist tools voor software

Command and Control (Data Exfiltration)

- ✓ Firewalls
- ✓ Intrusion Protection Systemen
- ✓ Proxy filters

Actions on Objectives (Doelen behalen)

- ✓ Beveiligde backups
- ✓ Disaster Recovery Plan
- ✓ Cybersecurity verzekering

Je bent alsnog gehackt.... Wat nu?

Samenvattend

Samenvattend

- Assume Breach and take measures.
- Mocht je wel in het bezit zijn van een Cybersecurity verzekering. Let dan goed op het volgende:
  - Polisvoorwaarden worden jaarlijks aangescherpt
- Herdefinieer de huidige IT infrastructuur voor security maatregelen. (Bijv. Backup)
  - Backup is niet meer alleen voor bestandsherstel, wet- en regelgeving, juridisch
  - Backup is nog belangrijker geworden in het geval van een “Cyberaanval”
- Is er een patchbeleid en systeem (niet alleen van je servers)?
- Is er een incident response plan (weet iedereen wat er moet gebeuren)?
- Zet de risico’s centraal en stel een incident response team samen.
- Is er een Disaster Recovery plan?
- Tijd is van essentieel belang tijdens een cyberincident.
- Specificeer de meeste kritische processen en assets.
- Detect and Respond.
- Betrek specialisten.

Integrated Baseline voor Information security (IBI) als paraplu voor security improvements

Een transparante aanpak die leidt tot continue verbeteringen

Integrated
Baseline for
Information security

IDENTIFY PROTECT

IBI Essentials

- Security best practices voor de Microsoft 365 tenant

IDENTIFY PROTECT

IBI Securepacks

- Configuration best practices
- Vulnerability scanning
- Security recommendations voor servers & werkplekken

IDENTIFY PROTECT

IBI Platform

- Security best practices & security recommendations Voor Azure platform

IDENTIFY PROTECT

IBI Governance

- Beleid, procedures
- Incident response plan
- Business continuity plan
- Warroom simulatie
- Security Awareness

IDENTIFY PROTECT

IBI kwetsbaarheden

- Dagelijkse controle op acute dreigingen
- Maandelijkse bespreking van de gevonden kwetsbaarheden

DETECT RESPOND

Managed Extended Detection and Response (XDR) & Managed Endpoint Detection and Response (EDR)

- 24x7 Analytics, SOAR
- Alert monitoring & triage
- Incident Response
- Custom Analytics rule

Recover

Recovery

- Herstellen van beveiligings-incidenten

Security Awareness

Vergroot bewustzijn van gebruikers

Baseline testen

We bieden baseline-tests om het phish-gevoelige percentage van jouw gebruikers te beoordelen via een gesimuleerde phishing-, vishing- of smishing-aanval.

Train jouw gebruikers

's Werelds grootste bibliotheek met trainingsinhoud over beveiligingsbewustzijn: inclusief interactieve modules, video's, games, posters en nieuwsbrieven. Geautomatiseerde trainingscampagnes met geplande herinneringsmails.

Phish jouw gebruikers

Best-in-class, volledig geautomatiseerde gesimuleerde phishing, vishing- en smishing-aanvallen, honderden sjablonen met onbeperkt gebruik en phishing-sjablonen voor de gemeenschap.

Bekijk de resultaten

Rapportage op bedrijfsniveau. Zowel high-level als granulaire statistieken en grafieken klaar voor managementrapportages. We hebben zelfs een persoonlijke tijdlijn voor elke gebruiker.

Managed EDR versus Managed XDR

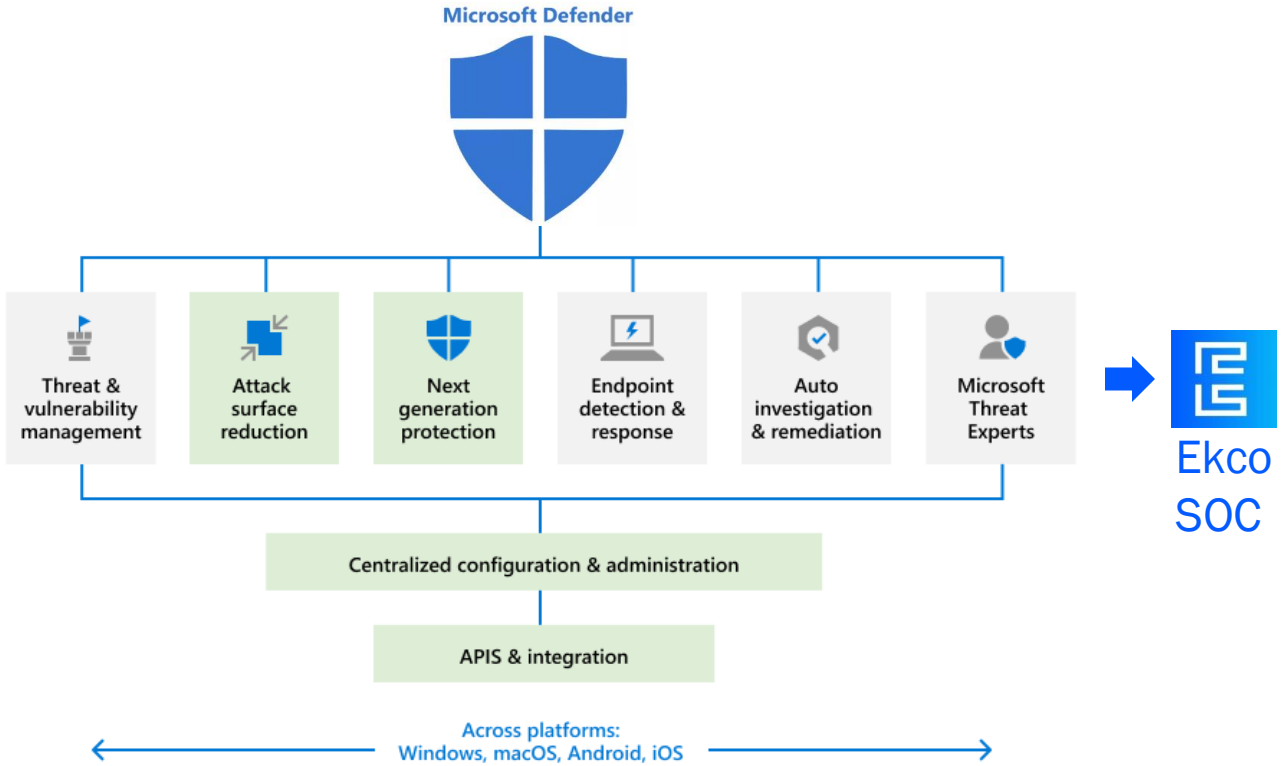
De verschillen tussen twee cyber security diensten

Parameter	Managed XDR	Managed EDR
Wat het doet?	Monitoren van endpoints, servers, netwerk, hypervisors en cloud op threats	Monitoren van endpoints, op cyber threats
Hoe wordt er gemonitord?	Verzamelt data uit meerdere (type) bronnen via data connectors	Microsoft Defender for Endpoint agent, optioneel Defender for O365
Hoe worden threats gedetecteerd?	Machine Learning, Kunstmatige Intelligentie, Custom Rules	Machine Learning, Kunstmatige Intelligentie
Complexiteit?	Specialistisch werk om in te richten en bij te houden	Microsoft security specialisatie
Kosten?	Over het algemeen duurder dan Managed EDR	Over het algemeen goedkoper dan Managed XDR
Response snelheid?	Reageert sneller doordat meerdere bronnen gecorreleerd kunnen worden	Dikwijls pas zichtbaar als er op het endpoint activiteit is.
Wanneer?	Hybride landschap	SaaS landschap

Managed Endpoint Detection and Response (EDR)

Powered by Microsoft Defender for Endpoint

- Biedt detectie, respons en geïntegreerde dreigingsanalyse
- Eenvoudig te implementeren en integreren
- Besteed minder tijd aan routinematige taken en focus op herstel
- Geen initiële kosten, flexibele voorwaarden, voorspelbare kosten
- Als een beheerde dienst kun je de oplossing snel aanpassen naar behoefte
- Optimaliseer je oplossing en blijf beveiligingsrisico's voor
- Toezicht, onderzoek en oplossingen vanuit ons 24x7x365 SOC



Microsoft Sentinel

Cloud-native SIEM

Onbeperkte schaal en snelheid

Gratis invoer van
Office 365 data en meer

Eenvoudige integratie met
bestaande tools

Snellere threat protection
door middel van AI

Ekco SOC

Managed XDR

Wat zit er in de dienst

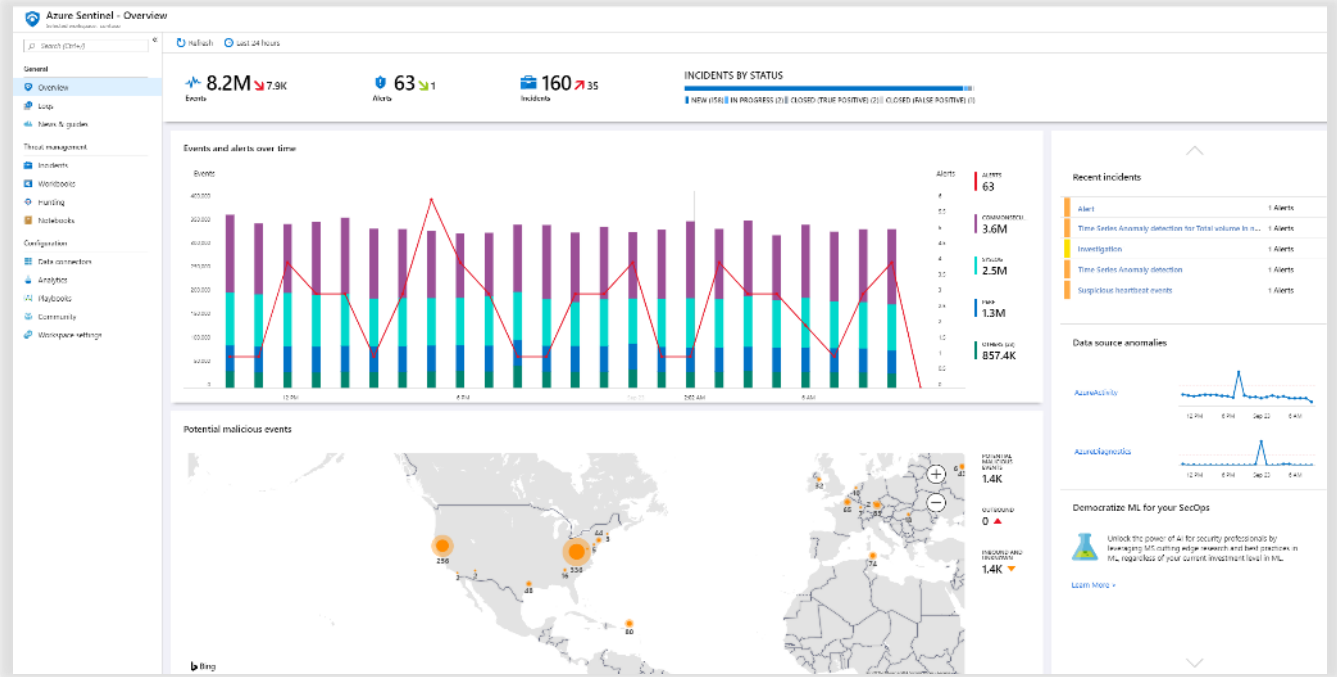
- **Analytics & SOAR implementatie en onderhoud**
  Uitrol en onderhoud van standaard en Ekco specifieke analytics rules waarmee incidenten snel kunnen worden opgespoord.
- **Managed Alert monitoring & triage**
  Onze analisten zitten 24x7 klaar om incidenten te analyseren en te bepalen of er sprake is van een concrete dreiging. Op het moment van dreiging wordt direct geschakeld om de impact te minimaliseren.
- **Incident Response**[1]
  Op het moment dat er sprake is van een incident zijn onze experts onderdeel van het incident response plan en helpen ze jouw organisatie het incident zo snel mogelijk op te lossen.
- **Custom Analytics rule**
  We stellen onze analyses continu bij, aan de hand van de specifieke karakteristieken van jouw organisatie.

1. Het starten van het incident response proces is inbegrepen. De werkzaamheden voor het beperken, wegnemen of herstellen van een dreiging zijn geen onderdeel van de maandprijs, maar worden apart in rekening gebracht. In combinatie met een cyberverzekering is dit meestal kosteloos voor jouw organisatie.

Managed XDR

Helder prijsmodel, eenvoudige opstap

- Gedekt vanuit de dienst:
  - Azure Activity (including Azure AD)
  - Exchange Online (Office activity)
  - Microsoft Teams (Office activity)
  - SharePoint Online (Office activity)
  - Microsoft 365 Defender (Incidents and Alerts)
  - Defender for Cloud (Alerts)
  - Defender for IOT (Alerts)
  - Defender for Identity (Alerts)
  - Defender for Endpoint (Alerts)
  - Defender for Cloud Apps (Alerts)
  - Windows Eventlogs*



- Lage flat fee prijs per medewerker per maand: € 18,00 per actieve AD gebruiker per maand, minimale afname 100 medewerkers
- Exclusief kosten voor Azure Sentinel
- Onbeperkt aantal extra bronnen tegen meerprijs

*Eventlogs die gerelateerd zijn aan het besturingssysteem. Applicatie specifieke logs kunnen extra kosten met zich meebrengen.

EKCO

Vragen?

Bedankt