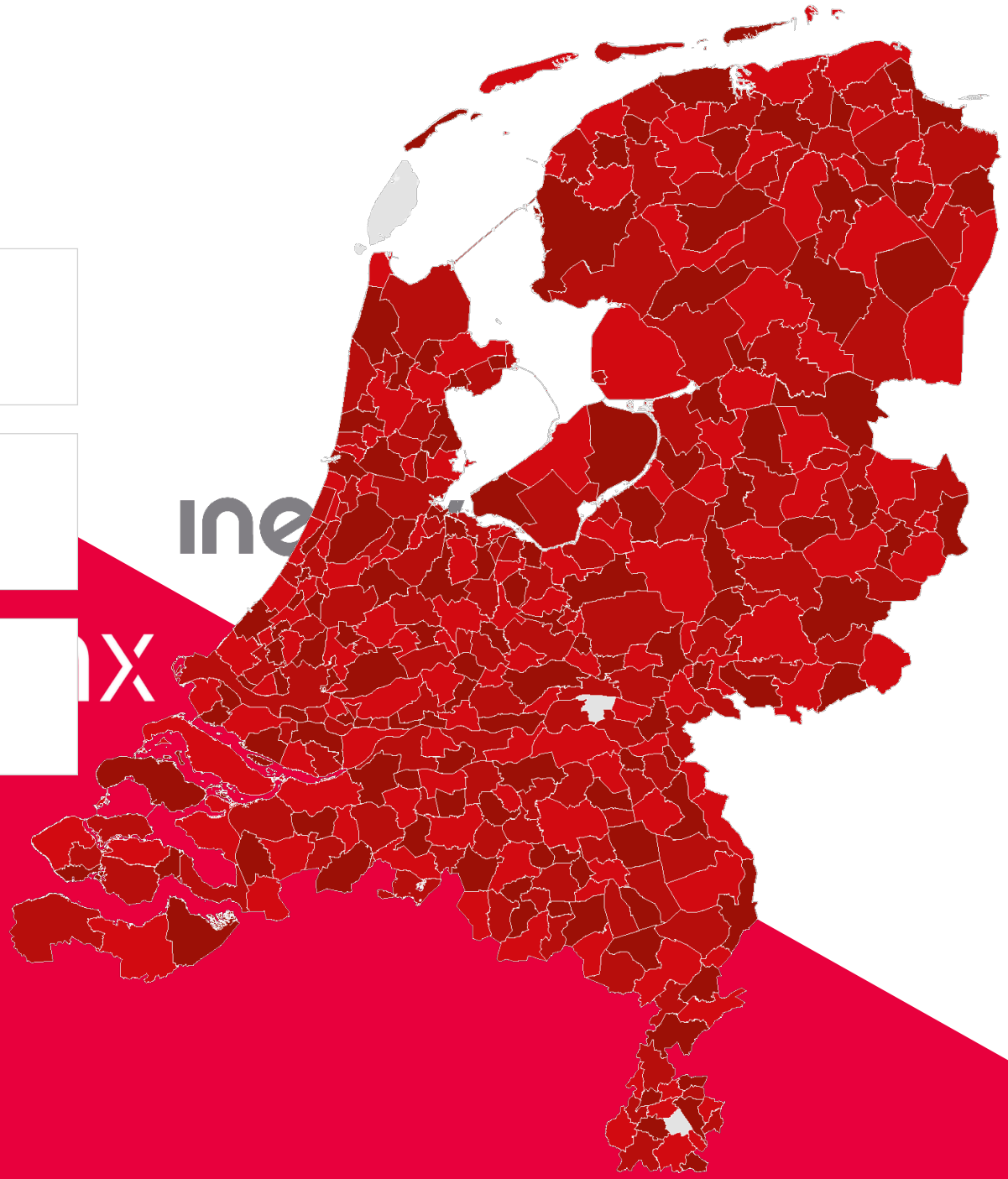
PRESENTATIE

CYBERSECURITY DECENTRALE OVERHEID

- Inergy: versterkt de ilionx-familie
- krachtige samenwerking
- verbonden in expertise



ruim 1.500 medewerkers

onze mensen maken wie wij zijn: experts in eenvoud.

compleet IT-dienstverlener

wij richten ons op het complete IT-landschap van onze klanten.

expertises

digitale strategie, cloud applicaties, data & AI, hyperautomation en managed services.

ilionx

locaties

Hoorn

healthcare

Watergang

Amsterdam

Amersfoort

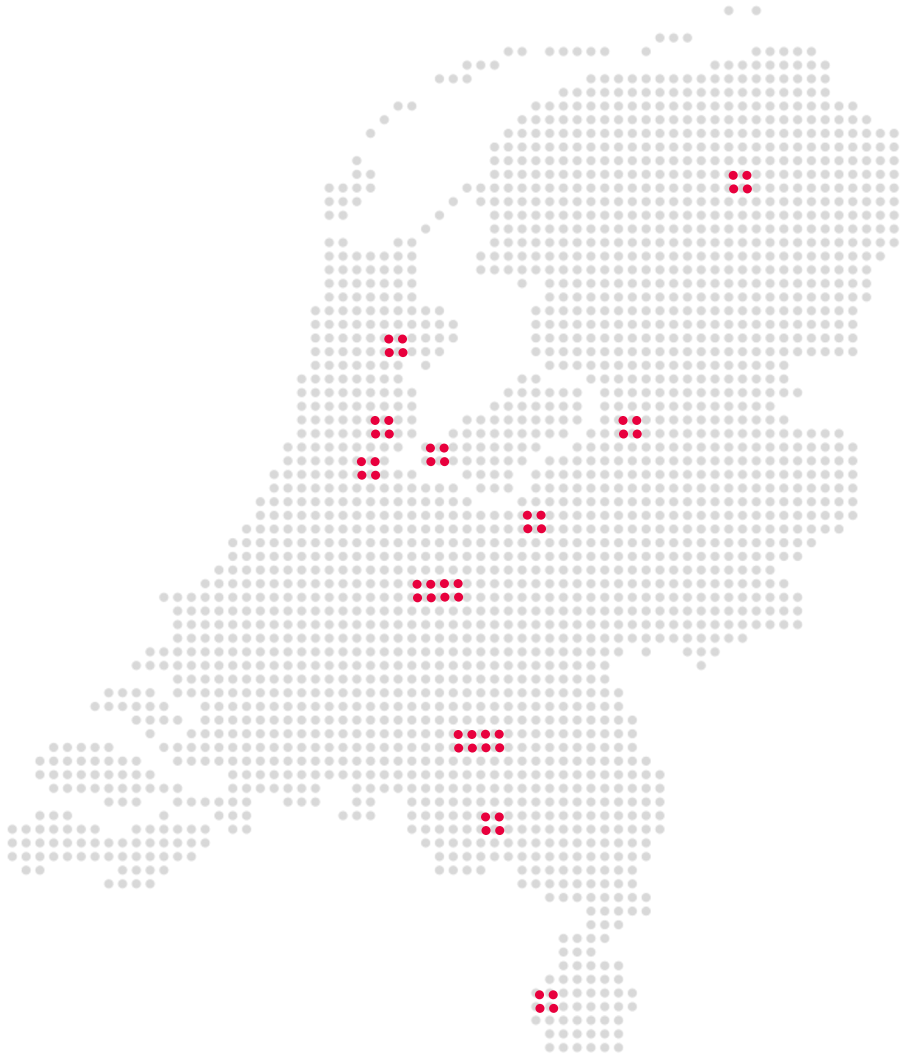
Woerden

Inergy

Utrecht

Den Bosch

overheid



Groningen

Zwolle

Almere

Salesforce Design Lab

Utrecht

Le Blanc Advies

Den Bosch

Eindhoven

Maastricht

landelijk bereik vanuit 14 locaties

ilionx is altijd dichtbij met veertien locaties door het hele land.

ilionx

klanten en partners

Rijksoverheid

gasunie
crossing borders in energy

OCI

ebn

ASML

sitech
services

vodafone Ziggo

alliade

kpn

Microsoft

postnl

NXP

veiligheidsregio
limburg-noord

VNG

apg

ABN·AMRO

Selection of partners:

Betty Blocks

salesforce

IBM

tableau

MicroStrategy

aws

DELL

SentinelOne

exabeam

CITRIX

ChipSoft

LMS365

CompLion

FORTINET

Microsoft

TIMEXTENDER

Awingu.com

imprivata

thycotic

ORACLE

nexus | nederland

fluxicon

Hewlett Packard Enterprise

Doel

- cybersecurity en -risico’s
- security oplossingen
- ervaring gemeentelijke markt
- groeipaden

ilionx verkozen tot 1 van de 6 security leveranciers
Vereniging van Nederlandse Gemeenten

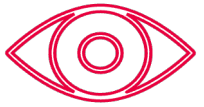
BEOORDELING

VNG aanbesteding

kwaliteit

De aanbesteding toont een complete dienstverlening van hoge kwaliteit aan.

transparantie



De VNG benadrukt de transparantie van ilionx in hun dienstverlening en advies. ilionx streeft naar het bieden van de beste waarde voor de gemeente, wat helpt bij het besparen op onnodige kosten.

betrouwbaar

ilionx wordt gepresenteerd als een betrouwbare partner dankzij hun realistische en waardevolle advies over groeimogelijkheden in de casus.

kennis

De beoordelaars waarderen dat ilionx zich goed kan aanpassen in de gemeentelijke omgevingen.

security oplossingen

trends in de markt

NIS 2

WETGEVING

DATALEK

IN HET NIEUWS

TEKORT AAN

SECURITY PERSONEEL

PHISHING

VIA AI

SUPPLY CHAIN

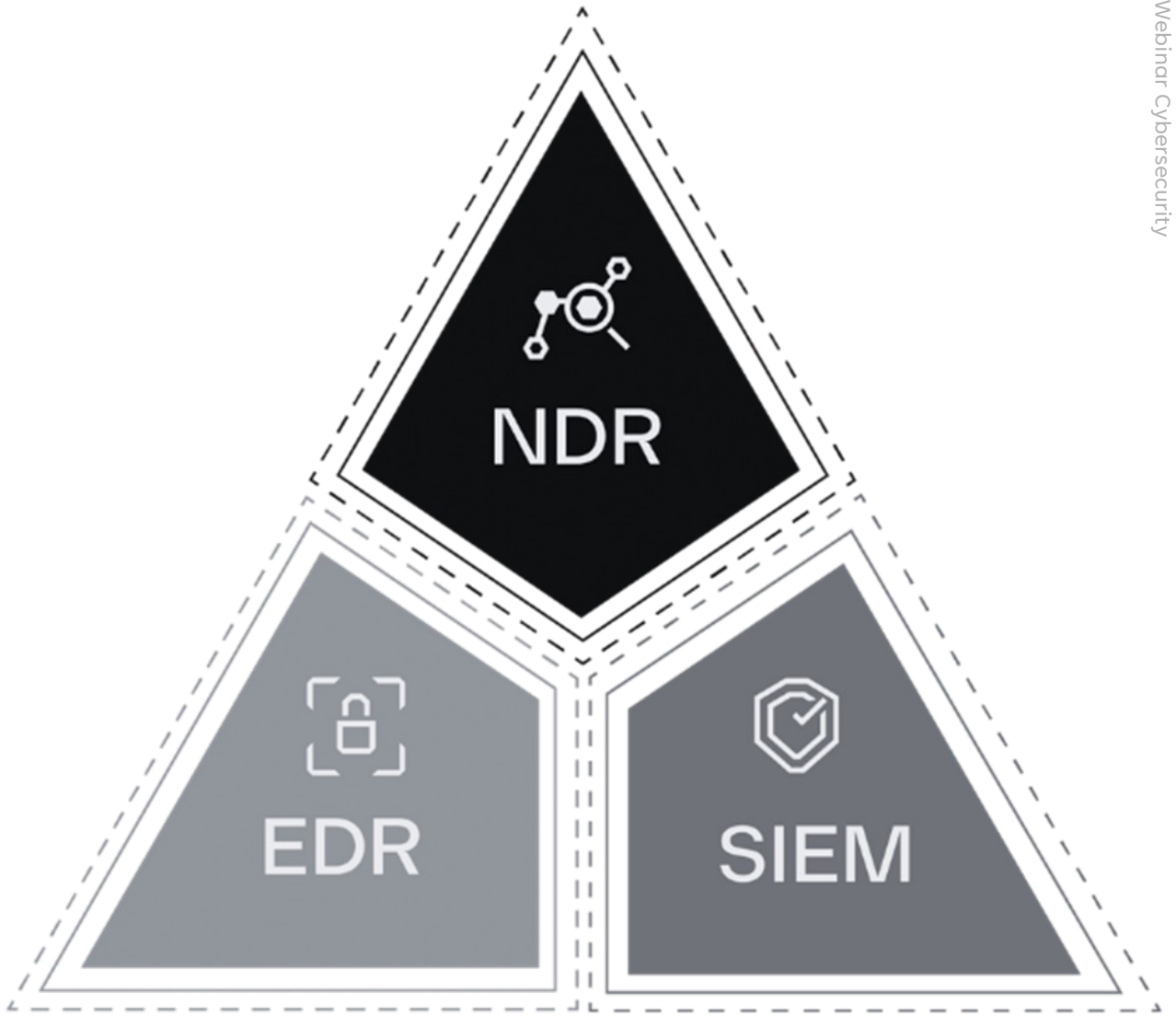
HACKS

MFA

HIJACKING

GARTNER

SOC Visibility Triad



GROEIPAD

security advies

NGAV

Solving the AV Problem

Prevent

Autonomous AI Prevention

Reduce Device Impact

EDR

Detect & Respond

Behavioral AI Automation

Recover Faster

SIEM

Augment & Resolve

Behavioral Cross Domain Detection

Business Resilience

SOAR – optional service

Mandating Tasks

Incident Responder

Process Automation

NDR

Inspect & Trace

Evidence First Approach

Threat Enrichment

Device Focused

Incident Focused

Outcome Focused

Evidence Focused

endpoint detection and response [EDR]

SentinelOne

algemeen

- Cyberbeveiligingstechnologie die voortdurend activiteiten monitort en analyseert om dreigingen te detecteren, onderzoeken en erop te reageren.
- Preventieve en reactieve werking.
- Reageert automatisch op gedetecteerde dreigingen, variërend naar gelang de ernst en aard ervan.
- EDR ondersteunt incidentenonderzoek met gedetailleerde forensische gegevens.

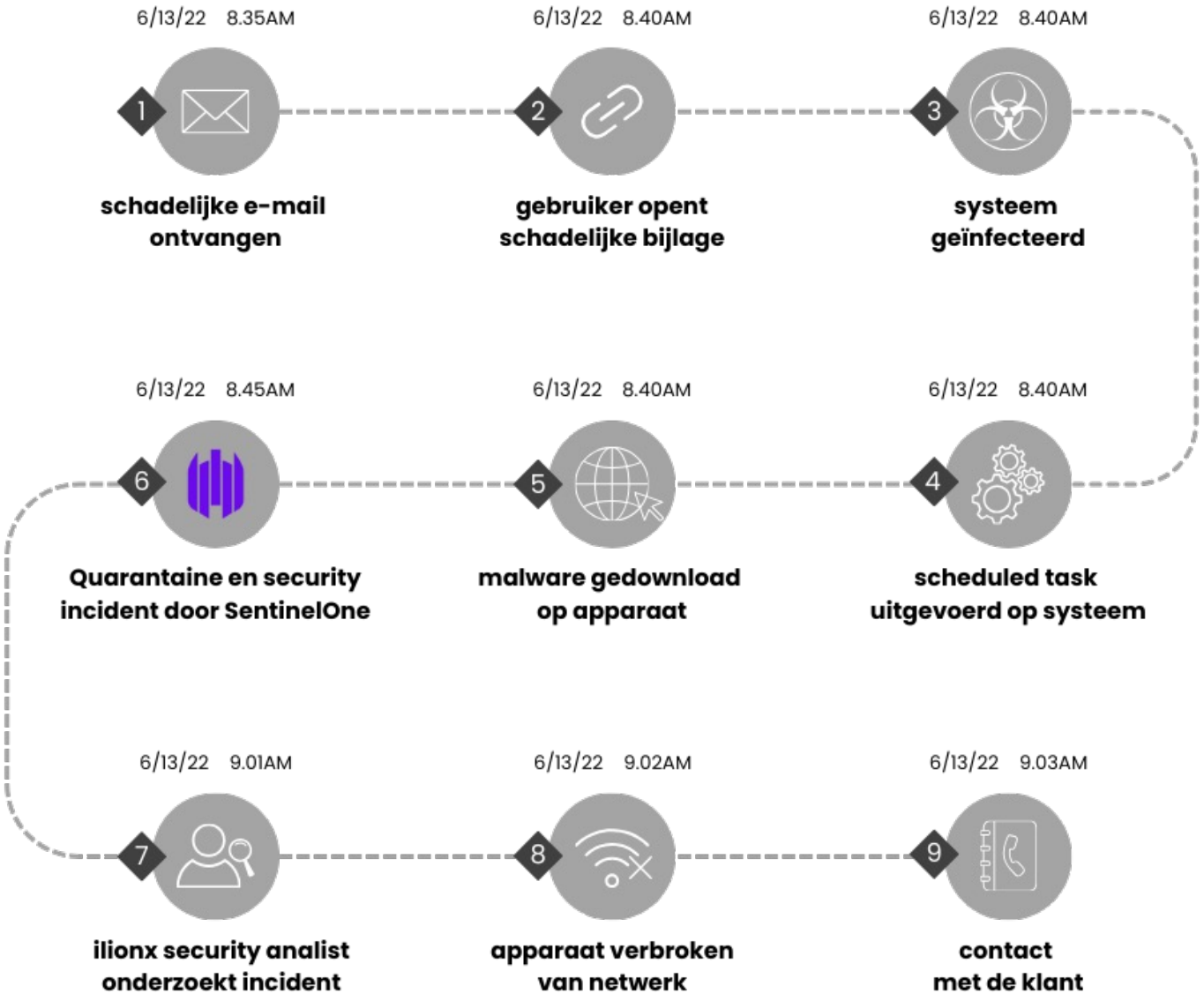
implementatie

- Inventarisatie: in samenwerking met securitypartner scope bepalen.
- Installatie agents: op werkplekken, servers en/of mobiele apparaten.
- Configuratie: EDR-agent afstemmen op de beveiligingsbehoeften van organisatie.
- Verificatie: controle of de EDR-agent bedreigingen effectief detecteert en reageert.

visie

- AI en ML detecteren afwijkingen door gedragspatronen te analyseren.
- Detectie van virussen in bestanden én ‘in memory’ virussen.
- Security specialisten analyseren meldingen en nemen actie, 24/7.
- Lightweight: Nauwelijks belastend voor systeemperformance.
- Hoge dekking in MITRE ATT&CK Evaluations.

tijdlijn | malware SentinelOne



1. email bevat schadelijke bijlage: "31350101616_112241979.html"
2. endpoint: ********
3. infectieuze payload creëert Scheduled Task op systeem
4. het systeem markeert kwaadaardig gedrag, wat resulteert in het aanmaken van een incident
5. "31420.dat" download
6. connectie met 91.199.147.26 is gemaakt
7. ilionx SOC analist detecteert extreem verdacht gedrag
8. ilionx SOC analist koppelt de endpoint los van het netwerk
9. ilionx SOC analist contacteert de klant om informatie over het incident te delen en maatregelen te treffen

security information event management [SIEM]

Exabeam

algemeen

- SIEM software beheert en analyseert loggegevens, en identificeert verdachte activiteiten.
- Verzamelde gegevens worden gestandaardiseerd voor vergelijking en correlatie.
- Identificatie van abnormale activiteiten of bedreigingspatronen.
- Risicoscores per gebruiker genereren een incident.
- Security analisten onderzoeken het incident en mitigeren de dreiging.

implementatie

- Implementatie SIEM software en onboarding.
- Inventarisatie: onboarden van logbronnen, welke waarde heeft een bepaalde logbron (o.b.v use cases).
- Configuratie en parsing van logs.
- Tuning en optimalisatie: configuraties aanpassen en verfijnen om false positives te verminderen en daadwerkelijke dreigingen sneller te detecteren.

visie

- Veel meer en sneller dreigingen detecteren door data science.
- Effectieve detectie interne en phished credentials dreigingen.
- 3x snellere detectie dankzij data science.
- 10x snellere (incident) response door geïntegreerde tijdslijnen.
- Voor de legacy én de nieuwe SaaS wereld.

ADVANCED ANALYTICS

Barbara Salazar [cward, lturner, thanson, mleon, rmartin, ...]
human resources coordinator | chicago

TOP PEER GROUP
usa
+6 more groups

MANAGER
Tu Petersen

LAST PASSWORD RESET
–

LAST SCORE
39

Activity on Saturday, 2 Jul Start: 11:52 End: 18:03 (6h 11m)

RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES	SCORE
32	16	1	2	23	1	370

vpn-in

6 COMMENTS

11:52

VPN login from Ukraine

First time activity from country Ukraine	+40
First activity from country Ukraine for organization	+15
First activity from ISP velton.telecom	+15
First VPN connection from device cc559 for Barbara Salazar	+15
Abnormal VPN connection from device cc559 for organization	+10
First VPN connection from device cc559 for organization	+10
Risk transfer from past sessions	+9
First connection from source IP 82.117.234.169	+5
First activity from country Ukraine for group jobvite	+3

LOC

tijdlijn | riskscores externe login

network detection and response [NDR]

Corelight

algemeen

- NDR is een oplossing die continu netwerkverkeer analyseert om verdachte activiteiten en potentiële dreigingen te detecteren.
- NDR biedt een breed overzicht van het netwerkverkeer en de interacties tussen apparaten.
- Detectie en Respons: NDR-oplossing genereert een melding bij afwijkende/verdachte activiteiten.
- Naadloze integratie met SIEMs, SOARs en IDS/IPS systemen.

implementatie

- Inventarisatie: identificeren van de beveiligingsbehoefte en doelstelling.
- Plaatsing van hardware sensoren binnen het netwerk of implementatie van virtuele sensoren in de omgeving.
- Configuratie: omvat instellen van netwerkinterfaces, bepalen van te analyseren verkeer en toevoegen van extra beveiligingsintegraties.
- Testing, verificatie en optimalisatie: wordt het netwerkverkeer goed vastgelegd en geanalyseerd.

visie

- Sessie correlatie met unieke sessie ID’s, verdeeld over 50+ log types.
- Analyse op basis van de gebruikte encryptie ,’shake-the-box principe’.
- Portable door het gebruik van ZEEK open-source software.
- Combinatie van ML, signature en behavior analytics.

cyberdreigingen vs. oplossingen

vergelijkingsmatrix

cyberdreigingen	EDR	SIEM | UEBA	NDR
malware/ransomware	+++	++	+
zero-day aanvallen	+++	+++	+++
phishing	++	+++	+
geavanceerde persistente dreigingen [APT's]	+++	+++	+++
insider threats	+++	++	+
bestandloze aanvallen	+++	++	+
man-in-the-middle aanvallen [MitM]	+	++	+++
command and control verkeer	++	++	+++
brute-force aanvallen	+	+++	++
privilege escalatie	+++	+++	+

SOC-dienstverlening

SOC-dienstverlening

MDR oplossingen

1. endpoint detection and response
   SentinelOne
2. SIEM / UEBA
   Exabeam
3. network detection and response
   Corelight

SOC diensten

1. ilionx dienstverlening 24 x 7
   incident- en dreigingsmeldingen
2. SOC service window
   analyse, advies en opvolging SOC
3. security incident classificatie
   business impact vs. risiconiveau

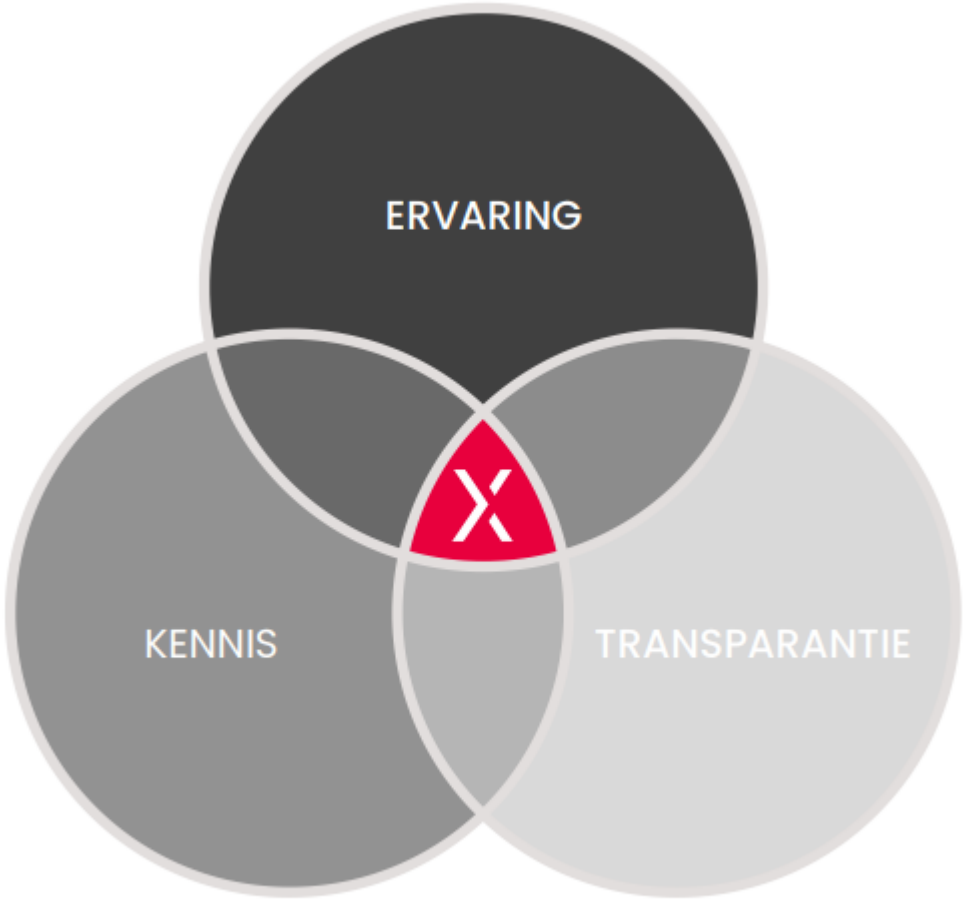
onboarding diensten

1. inventarisatie IT omgeving
2. end-to-end implementatie
3. training security medewerkers
4. workshop (acceptatie)

additionele diensten

1. MDR scope OT omgeving
2. ondersteuning incident response
3. aanvullende consultancy

speerpunten



ERVARING

- ruime set SOC-klanten
- verschillende sectoren en volwassenheidsniveau ’s
- best practices

KENNIS

- training, certificering SOC-analisten
- blue team level 1 - 2, CISSP en CISM
- productkennis

TRANSPARANTIE

- persoonlijke klantomgeving
- real-time dashboard
- één vaste prijs per maand

samenvatting

SOC Visibillity Triad

NDR

EDR

SIEM

behoeften gemeentelijke organisatie

strategie bepaling

cybersecurity en -risico's

security oplossingen

ervaring gemeentelijke markt

groeipaden

wet- en regelgeving (NIS2)

interne en externe risico's

trends

praktijk voorbeelden

MEERWAARDE

SOC-dienstverlening

ONTZORGING

SAMENWERKING

STRATEGIE

KENNISDELING

next steps

Contact

ilionx Group B.V.

Van Deventerlaan 121
3528 AB Utrecht

Contactpersoon

Anne van Gemert, AM
+31 6 5003 88 76

01 CONTACTEER ILIONX

02 INSPIRATIESESSIE

03 PERSOONLIJK ADVIESGESPREK

ilionx