Controlware Security Day 2022

Controlware
Security Day
22. - 23. September 2022
Congress Park Hanau

Transformieren Sie Ihr SOC und nutzen Sie XDR um Cyber-Angriffe zu stoppen

Profitieren Sie von der Zusammenarbeit von Vectra mit führenden Unternehmen der IT-Sicherheitsbranche

VECTRA
SECURITY THAT THINKS®

VECTRA®
SECURITY THAT THINKS.®

controlware

Wann / Warum man N**D**R/C**D**R/X**D**R dem SIEM vorziehen sollte.

David Lin | Regional Sales Manager | dlin@vectra.ai

Controlware Security Days 22/23 September 2022 - Hanau

Wer von Ihnen setzt ein SIEM ein?

Wer setzt es für Detection im SOC ein?

Wer hat es mit einer Angriffssimulation (Redteam) getestet?

Wer ist mit der Erkennung zufrieden?

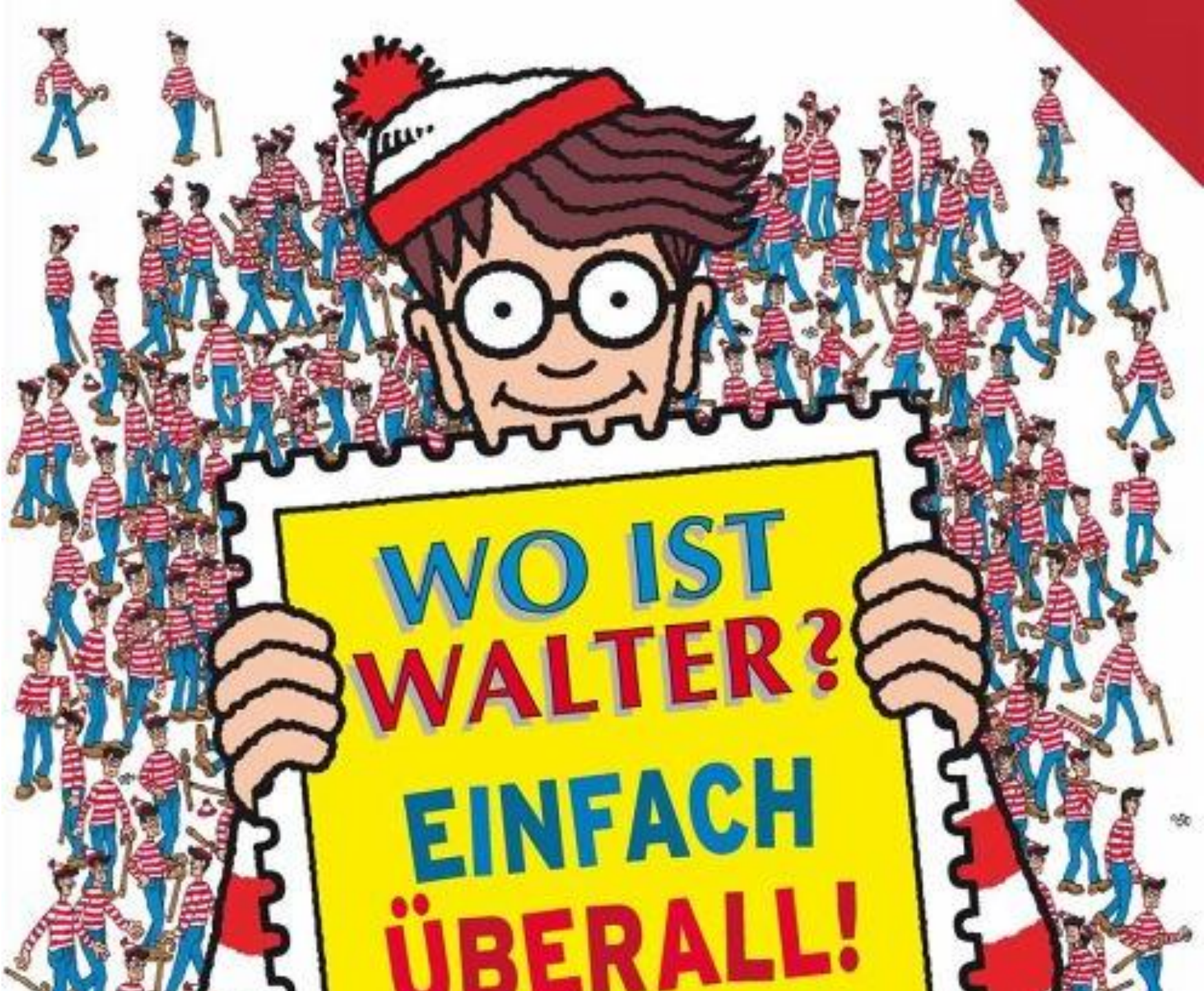
Typische Einsatzgebiete des SIEMs

#	Szenarien	Zweck
1	Logs zentral sammeln	Forensik & Compliance
2	Unstrukturierte Daten (Logs) auswerten	Reporting & Analysen
3	IT Services	Performance/Ressourcen monitoren
4	Konfigurationen und Changes	Dokumentation
5	Sicherheitslücken	Patchmanagement, Vulnerability Mgt.
6	Management von Sicherheitsvorfällen	Security Operations
7	Erkennung von Sicherheitsvorfällen	Detection
8	Unterstützung von Geschäftsprozessen	

Quelle: Dr. Michael Gorski, https://www.youtube.com/watch?v=s31AtCGlyq4&t=626s

Big Data.

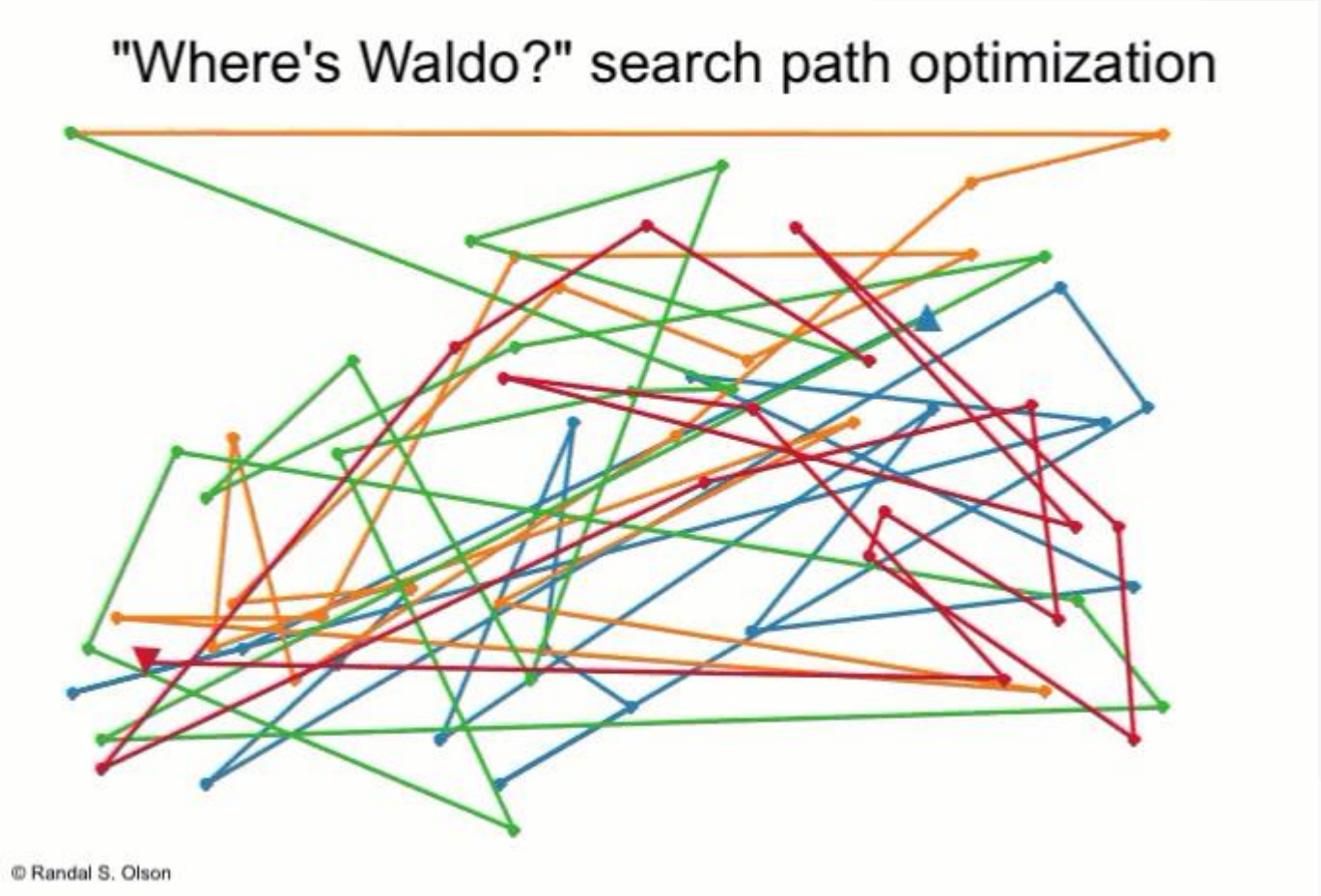
Was suche ich?



Welche Daten brauche ich?

Dann kommt die Methode.

- Auf der unteren linken Seite mit der Suche zu beginnen.
- Als nächstes im oberen Viertel der rechten Seite suchen. Hier scheint tatsächlich Walters bevorzugter Aufenthaltsort zu sein.
- Dann in der unteren rechten Hälfte der rechten Seite nachschauen.
- Walter scheint eine Aversion gegenüber der linken unteren Hälfte der rechten Seite zu haben. Hier solltet ihr wirklich erst schauen, wenn ihr alles andere abgesucht habt.



https://www.vice.com/de/article/gv573b/so-findet-ihr-walter-am-schnellsten-293

Welche Daten brauche ich?

Vectra AI, optimiert zur Erkennung von Angreifermethoden

1

Analysieren von **Angreifermethoden**

MITRE | ATT&CK®

Pro-Domain-Analyse ermöglicht tiefe Abdeckung

2

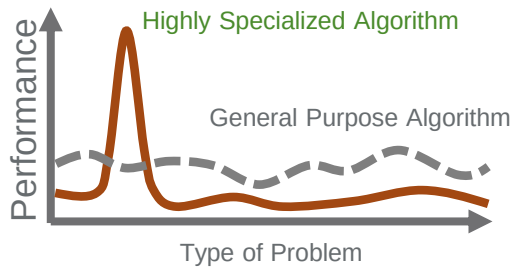
Gegenmaßnahmen definieren

MITRE | DEFEND™

Definieren von Techniken zur Erkennung von Angriffsmethoden

3

Verwenden Sie den **optimalen ML-Ansatz**



Sicherheitsorientierter KI-Ansatz

Angetrieben von modernster ML

Ergebnis: höhere Abdeckung, geringeres Rauschen gegenüber einfache anomaliebasierte Erkennung

VECTRA® SECURITY THAT THINKS.®

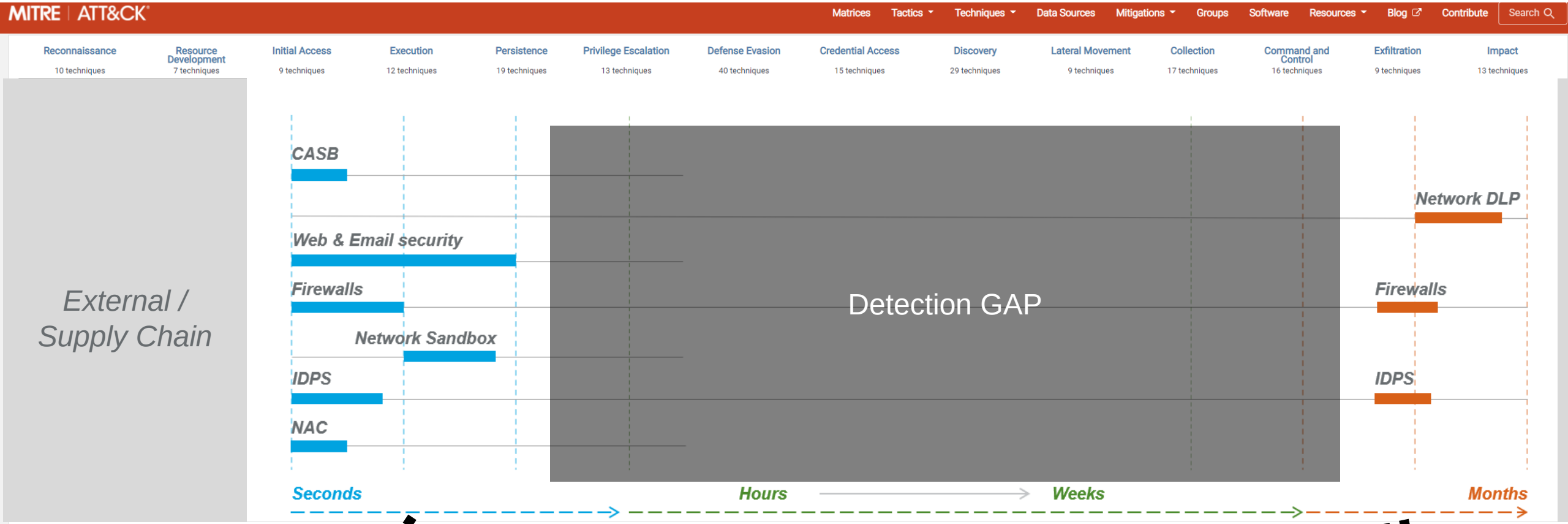
Wir unterstützen bei der SOC Transformation

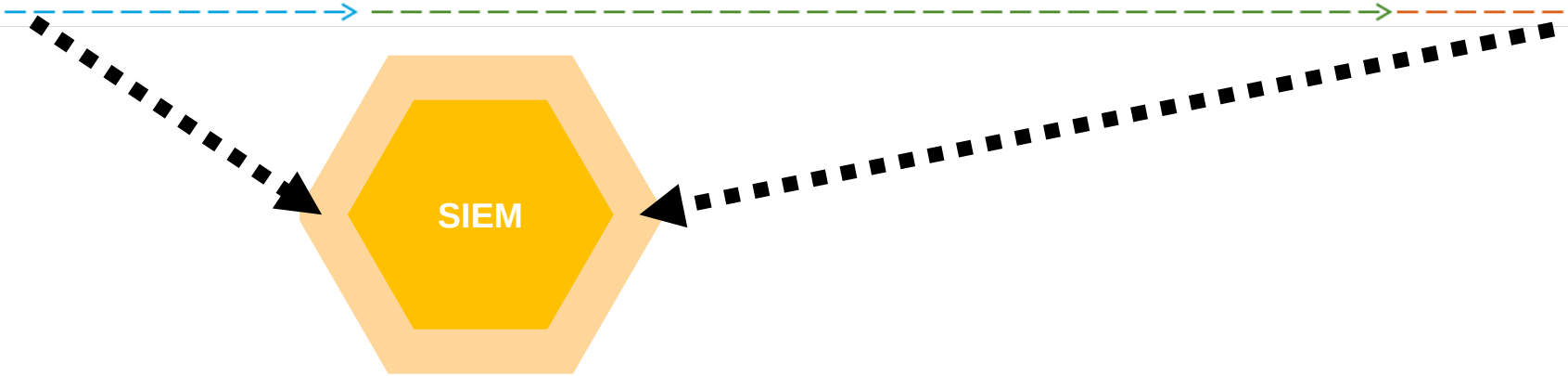
Log based SOC (SIEM only)
Datenquelle = Protokolle Die Abdeckung hängt von der Protokollabdeckung ab
Erkennen Sie die "bekannten schlechten" (Bedrohungsinformationen)
Erkennung basierend auf Regeln und Schwellenwerten
Fokussiert auf die smarten SOC-Analysten
Langsame Bereitstellung – benutzerdefinierte Anwendungsfälle, Protokollerfassung, Ermüdung von Warnungen, Fehlalarme
SLA konzentriert sich auf die Verarbeitung von Ereignissen

SOC Triade
Datenquelle = Protokolle + Endpunkte + Netzwerk Abdeckung aller Angriffsflächen (On-Prem, Cloud & SaaS)
Erkennen Sie unbekannte und laterale Bewegungsangriffe
ML automatisiert die Erkennung des Angreiferverhaltens
KI automatisiert Tier-1-Analysten-Workflow
Funktioniert out-of-the-box, selbstlernend
SLA konzentriert sich darauf, Verstöße zu stoppen

VECTRA
SECURITY THAT THINKS.®

Viele Daten vs. die richtigen Daten



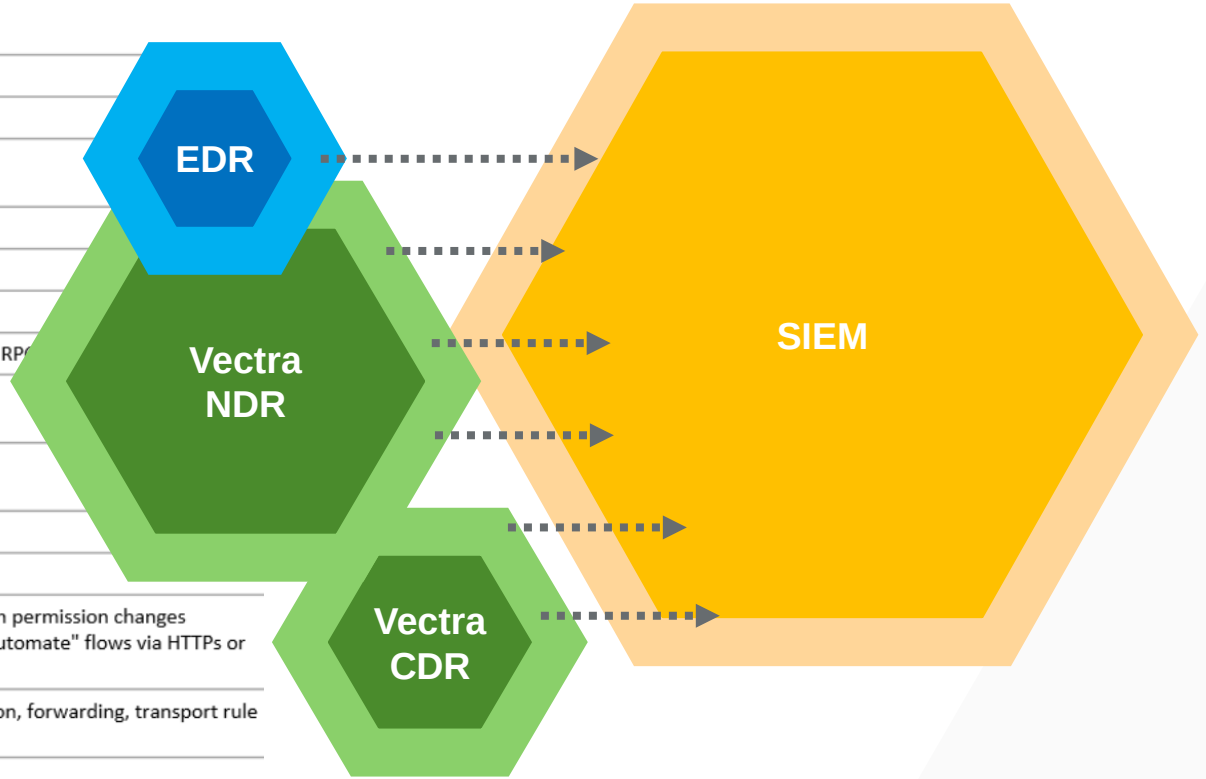


Die richtige Sensorik reduziert Zeit / Geld.

8 Controls to Thwart Sunburst and Other Supply Chain Attacks

By Thomas Lintemuth, Gartner | February 19, 2021

Step	Purpose	Activity to Detect
1	Download software update	
2	12-14 days after download SUNBURST activates	New programs running
3	DNS lookups to avsvmcloud.com	DNS lookup to new domain
4	C2 outbound HTTPS tunnel	HTTPS tunnel to new domain
5	Fully functional HTTPS tunnel	HTTPS non-standard activity
6	Domain reconnaissance	Suspicious traffic LDAP Query / RP
7	Access other systems on network	Suspicious remote execution Privilege access anomalies
8	Move to ADFS server to obtain SAML signing certificate	Suspicious remote execution Privilege access anomalies
9	Login to Azure AD	Suspicious login
10	Attackers add trusted domains to Azure AD	Suspicious Azure AD activity
11	Update credentials with access to O365	Suspicious O365 activity - Oauth permission changes eDiscovery searches, "Power Automate" flows via HTTPs or external storage
12	Access Email	Suspicious O365 activity - sign-on, forwarding, transport rule eDiscovery



https://blogs.gartner.com/thomas-lintemuth/2021/02/19/8-controls-to-thwart-sunburst-and-other-supply-chain-attacks/

VECTRA
SECURITY THAT THINKS®

Machen Sie ein Assume Breach Assessment.

Command and Control
External Remote Access
Hidden DNS Tunnel
Hidden HTTP/S Tunnel
Multi-home Fronted Tunnel
Suspicious Relay
Suspect Domain Activity
Malware Update
Peer-to-Peer
Suspicious HTTP
Stealth HTTP Post
TOR Activity
Threat Intel Match

Recon
Internal Darknet Scan
Port Scan
Port Sweep
SMB Account Scan
Kerberos Account Scan
File Share Enumeration
Suspicious LDAP Query
RDP Recon
RPC Recon
RPC Targeted Recon

Security Insights
New Host
Novel Device Vendor
New Host Role
Novel Admin Protocol Usage

Lateral
PA*: Unusual Account on Host
PA: Unusual Host
PA: Unusual Service
PA: Unusual Service – Insider
PA: Unusual Service from Host
PA: Unusual Trio
Suspicious Remote Exec
Suspicious Remote Desktop
Suspicious Admin
Stage Loader
Shell Knocker
Automated Replication
Brute-Force Attack
SMB Brute-Force
Kerberos Brute Force
Ransomware File Activity
SQL Injection Activity

Exfiltration
Data Smuggler
Smash and Grab
Hidden DNS Tunnel
Hidden HTTP/S Tunnel

Botnet Monetization
Cryptocurrency Mining
Brute-Force Attack
Outbound DoS
Outbound Port Sweep

= Purple Team detection

= Easier - $10-15K use case*

= Challenging - $25K+ use case*

= Not possible with data and tools in SIEM

* Likely not same efficacy as even “simple” models have complexity, e.g., dealing with slow scans well is hard

VECTRA® SECURITY THAT THINKS.®

12 Vectra-Patente, auf die in MITRE D3FEND verwiesen wird.

	Identity *Privileged Access Analytics*	**Network** *Hidden Tunnel / RAT C2*	**SaaS** *Microsoft365 Power Automate*	**Cloud** *AWS Admin API Abuse*
Die Vectra Methode	Identifiziert die Verwendung gestohlener privilegierter Anmeldeinformationen ohne UBA-Rauschen	Durchschaut Verschlüsselungs- und Umgehungstechniken, um C2 zu finden	Befasst sich eingehend mit der nativen Funktionalität, anstatt alle Apps gleich zu behandeln	Findet böswillige Aufrufe in häufig verwendeten Cloud-Admin-APIs
Methode (Security Research)	Die meisten Angriffe nutzen übermäßig gewährte Privilegien aus. Bestimmen Sie die effektive Richtlinie für die geringsten Rechte und erkennen Sie dann relevante Verstöße.	Zwei Hauptsteuerungsmethoden: Beacon und Reverse Shell. Domain ist aufgrund gängiger Umgehungstechniken ein unzuverlässiges Attribut.	PowerAutomate in M365 ist wie Powershell im Netzwerk. Muss die Verwendung gründlich analysieren, mit besonderem Fokus auf Konnektoren, die für Angreifer am wertvollsten sind.	Zugriffs- und Erkennungs-APIs für Anmeldeinformationen sind für viele Angriffe von zentraler Bedeutung, werden aber auch häufig verwendet. Kontext und Nutzungsmuster unterscheiden schlecht von gut.
ML Ansatz (Data Science)	Lernt automatisch die Berechtigungen aller Konten, Dienste und Hosts und ihrer Beziehungen. Erkennt Vorgänge mit hohen Berechtigungen, die zulässig, aber ungewöhnlich sind.	Rekurrente neuronale Netze (Deep Learning) analysieren, wie Verbindungen verwendet werden, um C2 zu finden. Funktioniert mit verschlüsseltem Datenverkehr und wird nicht durch Domain-Fronting oder Domain-Aging besiegt.	Erfahren Sie, wie PowerAutomate-Konnektoren auf Konto- und Mandantenebene verwendet werden. Erkennt neue Flows mit ungewöhnlichen, sicherheitsrelevanten Konnektoren.	Analysiert API-Aufrufe in mehreren Dimensionen, einschließlich Rate und Periodizität für eine bestimmte Quelle, um Missbrauch in einem Ozean legitimer Nutzung genau zu finden.

ROI

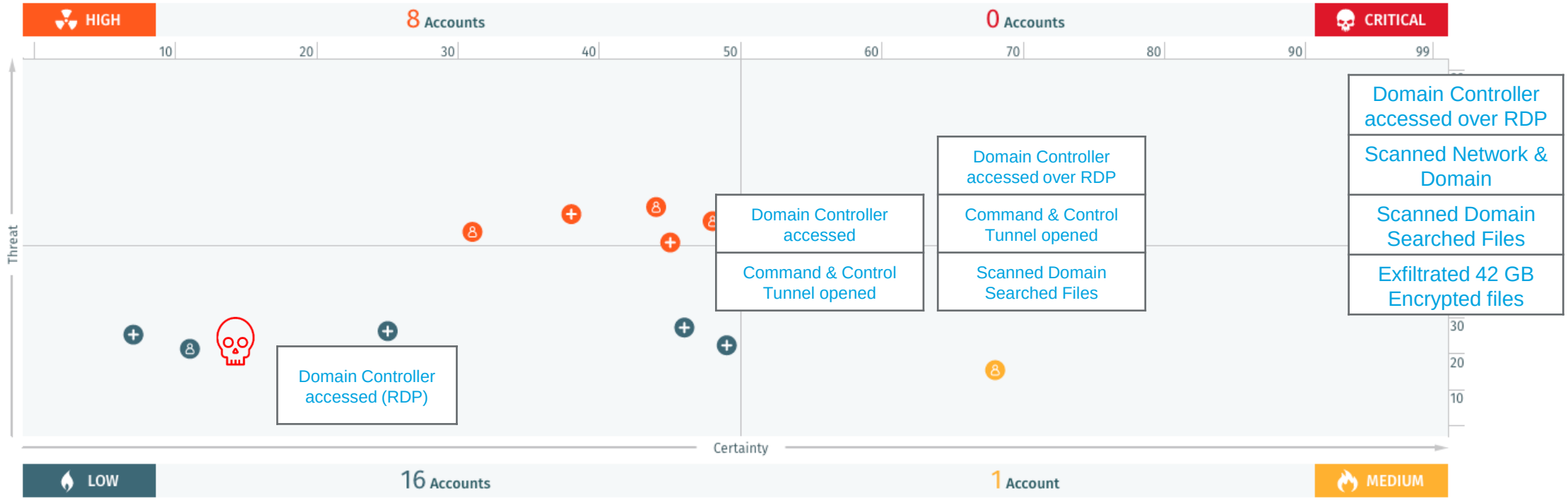
Typical SIEM cost savings[2]

	Before Vectra	After Vectra
SIEM use case development costs	• Splunk $6,000/use case • QRadar $12,500/use case	• 50-68% of SIEM use cases covered by Vectra • Reduction of use case development cost
Yearly use case maintenance cost	• $2,500/use case/year	• Reduced costs with fewer use cases
Log volume		• Up to 50% log volume reduction in SIEM • 37.5% on average
SIEM use case reduction		• 50-63% reduction of # of use cases in SIEM
SOC Level 1 work		• 34x workload reduction in SOC Level-1
IDPS Consolidation		• Reduced need of classic IDPS • Includes cloud apps & environments
IR Response time		• Accelerate IR response • Increase investigation confidence

[2] Based on Vectra AI average customer deployment

Scoring und Priorisierung erhalten Durchblick

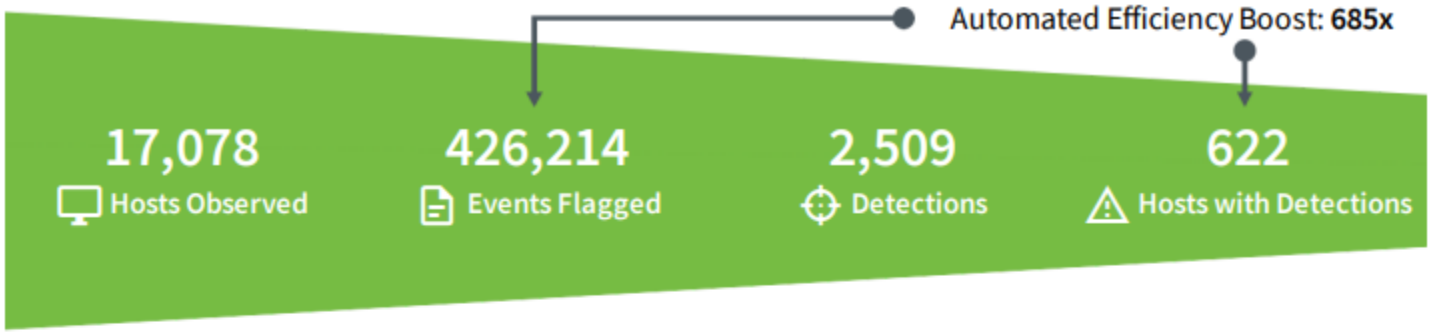
Schweiz: RansomOp bei einem Fertigungsunternehmen



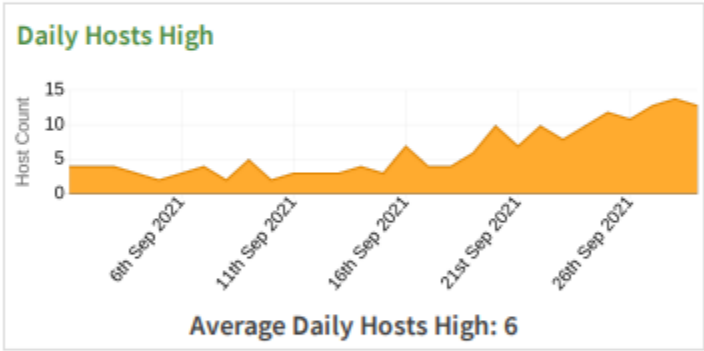
Attack Story

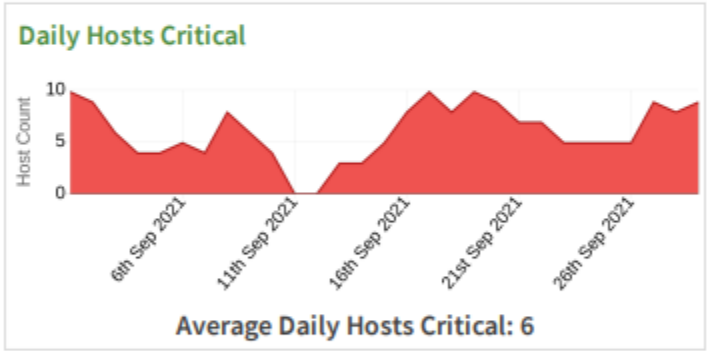
Azure DevOps VM accessed (RDP open) → Accessed Domain Controller → Recon Lateral → Vectra tool owner left company → Company was down for a few days

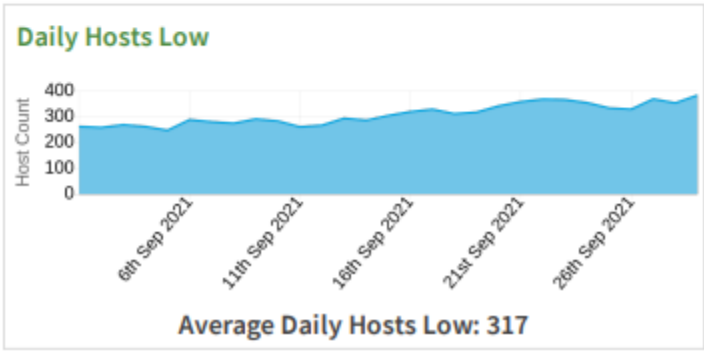
NRW: Arbeitserleichterung durch Priorisierung.

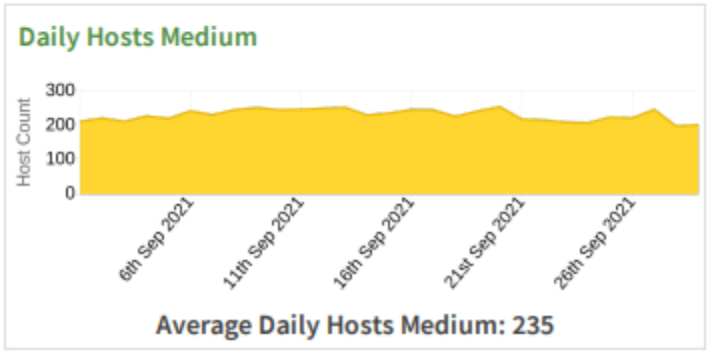


Host Quadrants



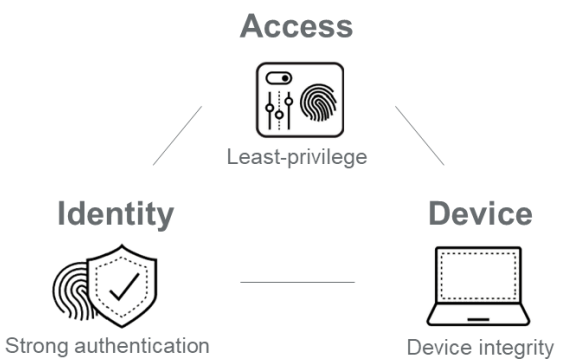






Überwachung privilegierter Accounts

Der Präventionsansatz für Zero Trust ist ein langer, harter Weg

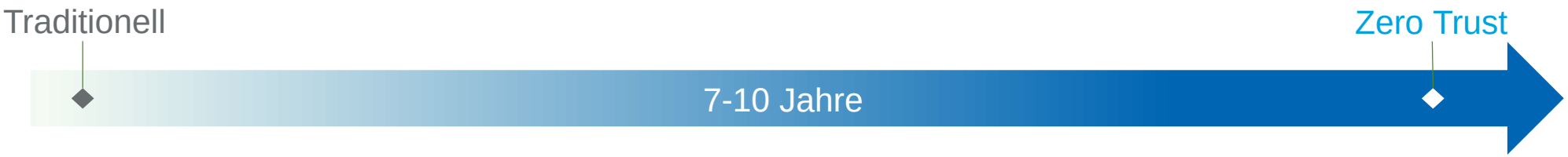


Prevention

Entscheidung, ob der Zugang gewährt oder gesperrt wird.

Hardening | Identity infrastructure | Policy | Enforcement points

Herausforderung: 7-10 Jahre bis zur Zero Trust Reife[1]

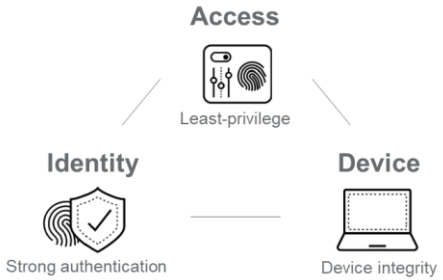


1 Forrester Research, "A Practical Guide to Zero Trust Implementation"

Beschleunigen Sie Zero Trust mit Detection & Response

Detection and Response

Analysieren Sie **jede** Transaktion - autorisiert oder nicht - auf Anzeichen von **Angreiferaktivitäten**

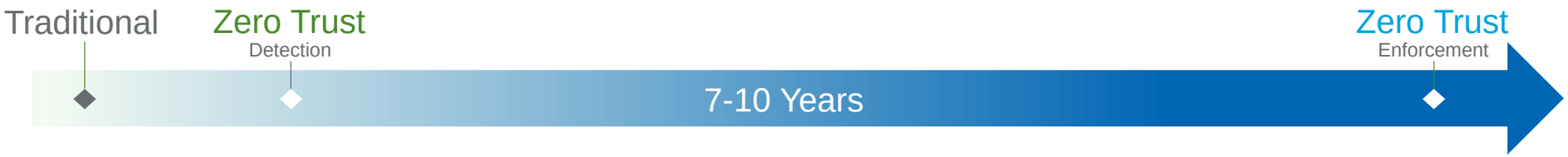


Prevention

Entscheiden Sie, ob der Zugang gewährt oder gesperrt werden soll.

Hardening | Identity infrastructure | Policy | Enforcement points

Chance: Schutz vom ersten Tag an durch Detection and Response

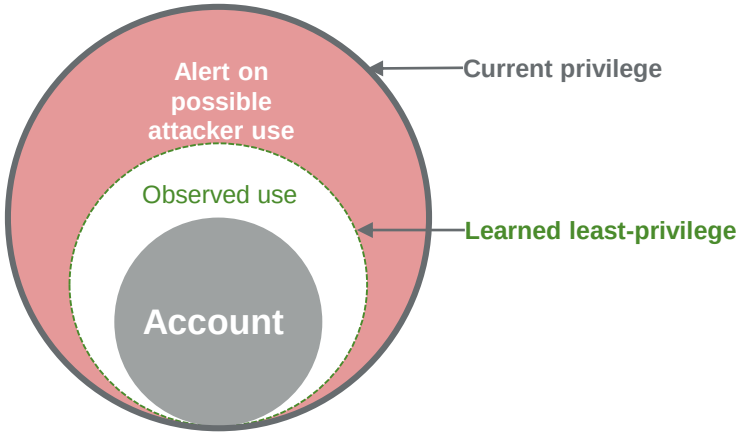


(Bsp.) Beschleunigung von Zero Trust für privilegierte User

85% der Angriffe erfolgen über gestohlene Konten

Detection and Response

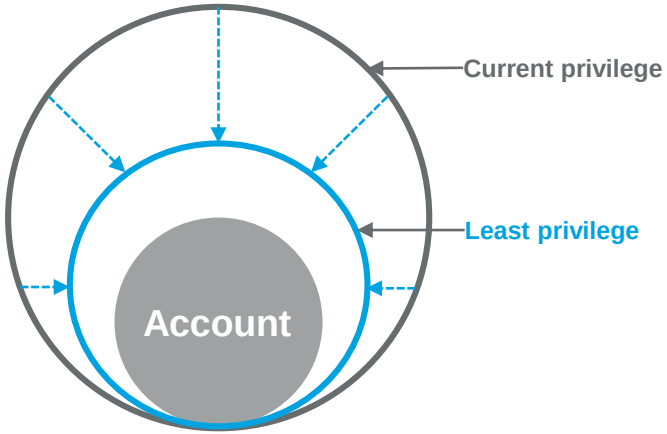
- Automatisches Erlernen aller privilegierten Konten.
- Automatisches Erlernen der Least-Privilege-Richtlinie.
- Warnung bei jeglicher Nutzung außerhalb der Least-Privilege-Richtlinie.
- Keine Richtlinienänderungen erforderlich!



Wochen

Prevention

- Versuchen Sie, alle privilegierten Konten zu identifizieren.
- Neudefinition und Beibehaltung der Richtlinie über die geringsten Berechtigungen für jedes Konto.
- Umgang mit Eskalationen bei gesperrtem Zugang.



Jahre

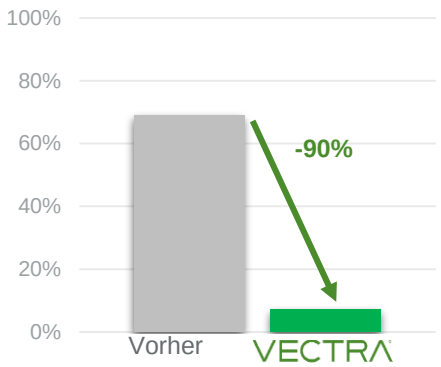
Zusammenfassung

Vectra verändert das Spiel für Sicherheitsteams

Mehr Bedrohungen mit weniger Aufwand finden und gleichzeitig die Gesamtausgaben für Tools reduzieren

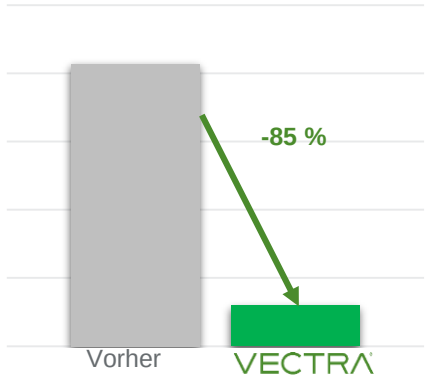
90% weniger unentdeckte Bedrohungen

% of threats bypassing prevention that were not detected before impact



85%weniger Alarm “**Noise**”

Untersuchte Warnungen pro wirkungsvoller Bedrohung



30% Einsparungen durch **Werkzeugkonsolidierung**

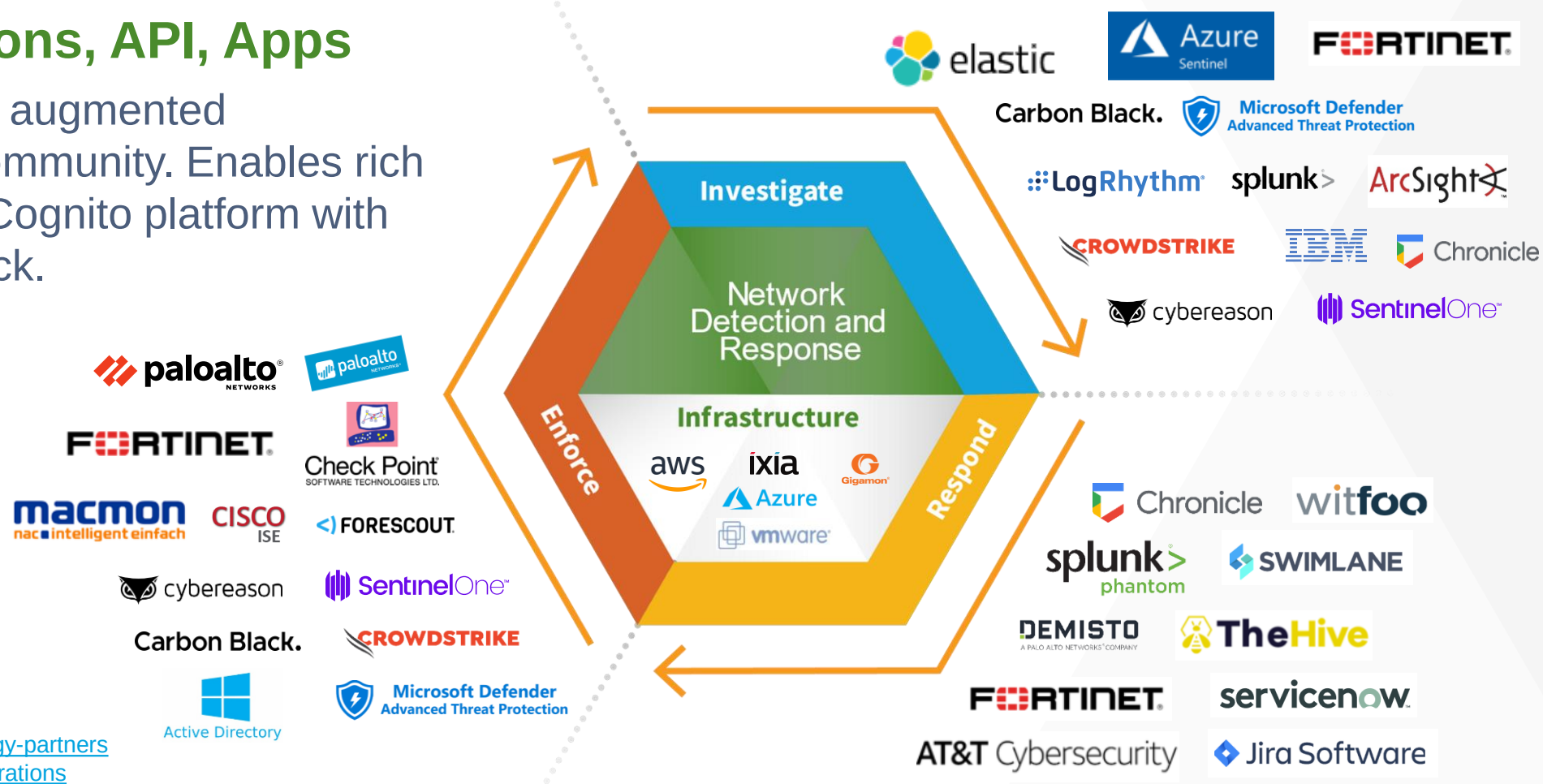
- **SIEM:** Entwicklung von Anwendungsfällen, Wartung und Speicherung
- **IDS, Netflow**-Tools: Ersatz

Source: “The Business Value of Cognito NDR by Vectra”, IDC, December 2020

Vectra integriert mit ihren Security Technologien

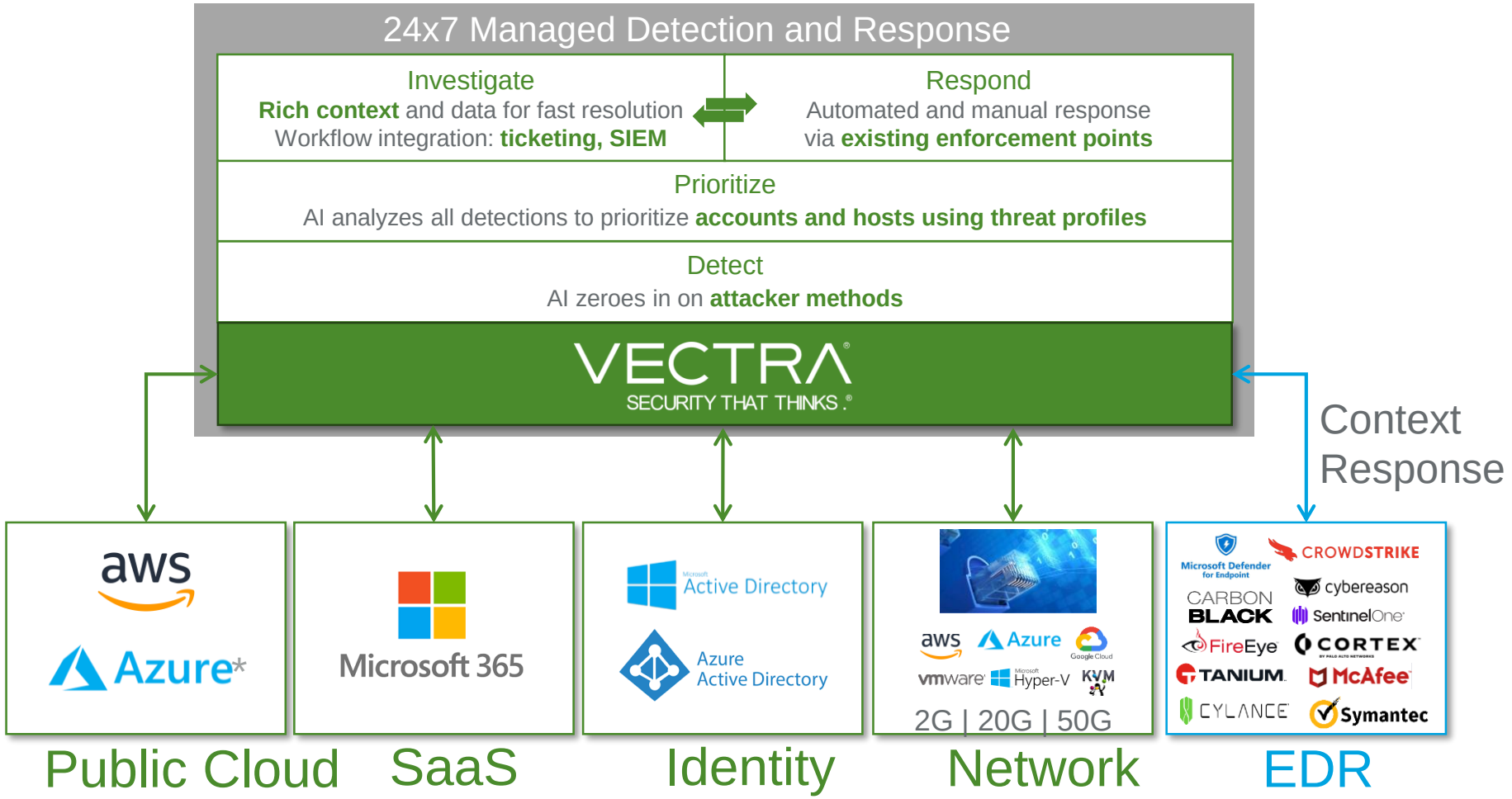
Native Integrations, API, Apps

Comprehensive API augmented by tools and user community. Enables rich integration into the Cognito platform with your technology stack.



https://www.vectra.ai/partners/technology-partners
https://www.vectra.ai/products/api-integrations
https://github.com/vectranetworks

Bedrohungserkennung für Hybrid und Multi-Cloud



controlware