VECTRA AI

EBOOK

Achtung, Ihre Security-Gaps

Wie Angreifer durch Ihren Stack kommen

Von Lucie Cardiet · Cyberthreat Research Manager

Warum ich dieses ebook geschrieben habe

Vorwort der Autorin

Ich verbringe meine Arbeitstage damit zu beobachten, was Angreifer tatsächlich tun, in Umgebungen, die Ihrer ähneln.

Was ich immer wieder feststelle: Verteidiger verlieren nicht aus Mangel an Investitionen. Sie verlieren, weil ihre Investitionen in einer Zone partieller Wirksamkeit verharren. Ihr EDR funktioniert genau wie geplant; der Angreifer ist auf der Identitätsebene. Ihr SIEM nimmt jeden Log auf; und der Angriff ist nur in der Korrelation zwischen Logs sichtbar. Ihr IAM genehmigt jeden policy-konformen Login; aber die Person am anderen Ende ist nicht der Mitarbeiter, dessen Credentials sie nutzen.

Dies ist die zweite Auflage dessen, was ich 2025 zuerst geschrieben habe. Neu: zwei zusätzliche Kampagnen (Volt Typhoon und AWS in acht Minuten von KI-Agenten kompromittiert), IDC-Messwerte 2025 zum Einsatz von Vectra AI, ein Abschnitt zum regulatorischen Druck, der kontinuierliche Erkennung zur Compliance-Frage macht, und ein Self-Assessment am Ende.

Lucie Cardiet

Das Netzwerk ist seiner Sicherheitsarchitektur entwachsen.

Heutige Unternehmen leben nicht mehr hinter einem einzigen Perimeter

Unternehmensumgebungen erstrecken sich über On-Prem, mehrere Public Clouds, Dutzende SaaS-Apps, Identity Provider, IoT- und OT-Systeme, KI-Dienste und die autonomen Agenten darüber. Diese Domänen sind nicht unabhängig, sie sind ein einziges verbundenes System.

- ✓ Ihr EDR überwacht die Endpoints.
- ✓ Ihr IAM genehmigt Logins.
- ✓ Ihr CSPM liest Konfigurationen.
- ✓ Ihr SIEM speichert Logs.

Jedes erfüllt seine Aufgabe.

Angreifer, zunehmend mit KI-Unterstützung, haben in den letzten drei Jahren gelernt, sich zwischen ihnen zu bewegen, in den Räumen, die kein Tool beobachten sollte.

Das Netzwerk hat sich weiterentwickelt. Die Angreifer auch.

Ihr Stack ist stark, aber ist er vollständig?

Auf den ersten Blick haben Sie einen starken Security-Stack aufgebaut.

- Sie haben in die besten Security-Technologien investiert, die heute verfügbar sind.
- Sie haben Endpoint-Schutz auf jedem Gerät.
- Sie haben Tools, die Ihr Netzwerk überwachen.
- Ihre Cloud-Posture-Management-Tools scannen Ihre Konfigurationen korrekt.
- Sie haben das Identity Management mit IAM oder PAM gestärkt.

Und trotzdem kommen Angreifer durch, und sie tun es.

Nicht weil Ihre Tools defekt sind. Weil jedes Tool darauf ausgelegt war, seine Domäne zu beherrschen, und Angreifer sich nun zwischen ihnen bewegen.

Angreifer brechen Ihre Tools nicht. Sie umgehen sie.

Die Realität: moderne Angreifer kämpfen nicht gegen Ihren Stack. Sie meiden ihn.

Identitätsmissbrauch
Kompromittierte Credentials sind der initiale Zugriffsvektor in 22 % der Kompromittierungen.[1] 88 % einfacher Web-Angriffe nutzen gestohlene Credentials.[1]

Lateral Bewegung
Sie bewegen sich lateral, ohne Alerts auszulösen. Die durchschnittliche eCrime-Breakout-Time – der Abstand zwischen initialem Zugriff und erstem lateralen Pivot – ist auf 29 Minuten gefallen.[2]

Cloud-Privilegienmissbrauch
Missbrauch gültiger Accounts macht inzwischen 35 % der Cloud-Vorfälle aus.[2]

Operieren zwischen den Tools
Sie verstecken sich in den Lücken zwischen Tools, in Räumen, die kein einzelnes System beobachten sollte.

Ausnutzen des Alert-Rauschens
Sie operieren unter Ihren Schwellen, weil Ihr SOC nicht alles untersuchen kann.

Cross-Domain-Tempo
MFA blockiert über 99 % der Identitätsangriffe, doch Angreifer melden sich zunehmend mit gestohlenen Tokens, genehmigten OAuth-Apps, Device-Code-Flows und Adversary-in-the-Middle-Proxies an.[3]

KI-beschleunigte Aufklärung
Angriffe durch KI-gestützte Akteure stiegen um 89 % im Jahresvergleich. 2025 nutzten Angreifer legitime GenAI-Tools in über 90 Organisationen, um Credential-Diebstahl-Befehle zu generieren.[2]

[1] Verizon DBIR 2025. [2] CrowdStrike 2026 Global Threat Report. [3] Microsoft Digital Defense Report 2025.

Best-in-Class-Tools sind keine vollständige Abdeckung.

Jede Investition reduziert Risiko in ihrem Bereich, aber lässt Lücken in Sichtbarkeit und Erkennung zwischen den Tools. Die Zahlen 2026 sprechen für sich:

- 82 % der Intrusion-Erkennungen in 2025 waren malware-frei. Angreifer operierten mit gültigen Credentials, vertrauten Identitätsflüssen und genehmigten SaaS-Integrationen.[1]
- Kompromittierungen über mehrere Umgebungen kosten 5,05 Mio. $ im Schnitt, 25 % mehr als reine On-Prem-Kompromittierungen.[2]
- Die durchschnittliche Breakout-Time ist auf 29 Minuten gefallen. Schnellster Wert: 27 Sekunden.[1]

[1] CrowdStrike 2026 Global Threat Report. [2] IBM Cost of a Data Breach Report 2025.

Das Muster ist nicht neu. Es ist die neue Normalität.

Dieses Ebook hilft Ihnen, diese Gaps zu kartieren, zeigt, wo Vectra AI ansetzt und wie Vectra AI sie schließt.

Inhalt

Überblick zur Abdeckung

Die Security-Gap-Illustration plus drei benannte Kampagnen, die sie ausnutzen.

Die Security-Gap-Illustration

Ihr aktueller Stack: keine Kombination liefert kontinuierliche Erkennung über die gesamte hybride Infrastruktur. Jedes Tool stoppt an Schlüsselphasen.

		Initialer Zugriff	Ausführung	Persistenz	Privilege Escalation	Defense Evasion	Credential Access	Erkundung	Lateral Movement	Sammlung	Command & Control	Exfiltration	Impact
ENDPOINT	EDR	●	●	●	●	●	●	●	●	●	●	●	●
ENDPOINT	EPP	●	●	○	○	○	○	○	○	○	○	○	○
CLOUD	CASB	●	○	○	●	○	●	○	○	●	○	●	○
CLOUD	CNAPP	●	●	●	●	●	●	●	●	●	●	●	●
CLOUD	CSPM	○	○	○	●	○	●	○	○	○	○	○	○
CLOUD	CWPP	●	●	●	●	○	○	●	○	●	●	○	●
CLOUD	SASE	●	○	○	○	○	○	○	●	○	●	●	○
NETZWERK	Email	●	○	○	○	○	○	○	○	○	○	○	○
NETZWERK	Firewalls	●	○	○	○	○	○	●	○	○	●	●	○
NETZWERK	IDPS	●	○	○	○	○	○	●	●	○	●	●	○
NETZWERK	NAC	●	○	○	○	○	○	○	○	○	○	○	○
NETZWERK	SSE	●	○	○	○	○	○	○	●	○	●	●	○
IDENTITÄT	IAM	●	○	○	●	○	○	○	○	○	○	○	○
IDENTITÄT	PAM	○	○	○	●	○	●	○	○	○	○	○	○
IDENTITÄT	UEBA	●	○	●	●	●	●	●	●	○	○	●	○
Vectra AI Platform		●	●	●	●	●	●	●	●	●	●	●	●

● Partielle Sichtbarkeit ● Volle Sichtbarkeit ○ Keine Sichtbarkeit

Drei Gaps, die jeder Stack heute hat.

Keine Abdeckungs-Gaps. Ausführungs-Gaps. Kontrollen, die existieren, aber nicht erkennen.

1. Nichts wirkt verdächtig.

Die Tools des Angreifers sind Ihre Tools. Remote Desktop. PowerShell. Eine signierte Binary. Living-off-the-Land-Binaries, die Ihre Sysadmins um zwei Uhr nachts nutzen. Jede einzelne Aktion sieht nach normalem Betrieb aus.

2. Die Authentifizierung ist erfolgreich.

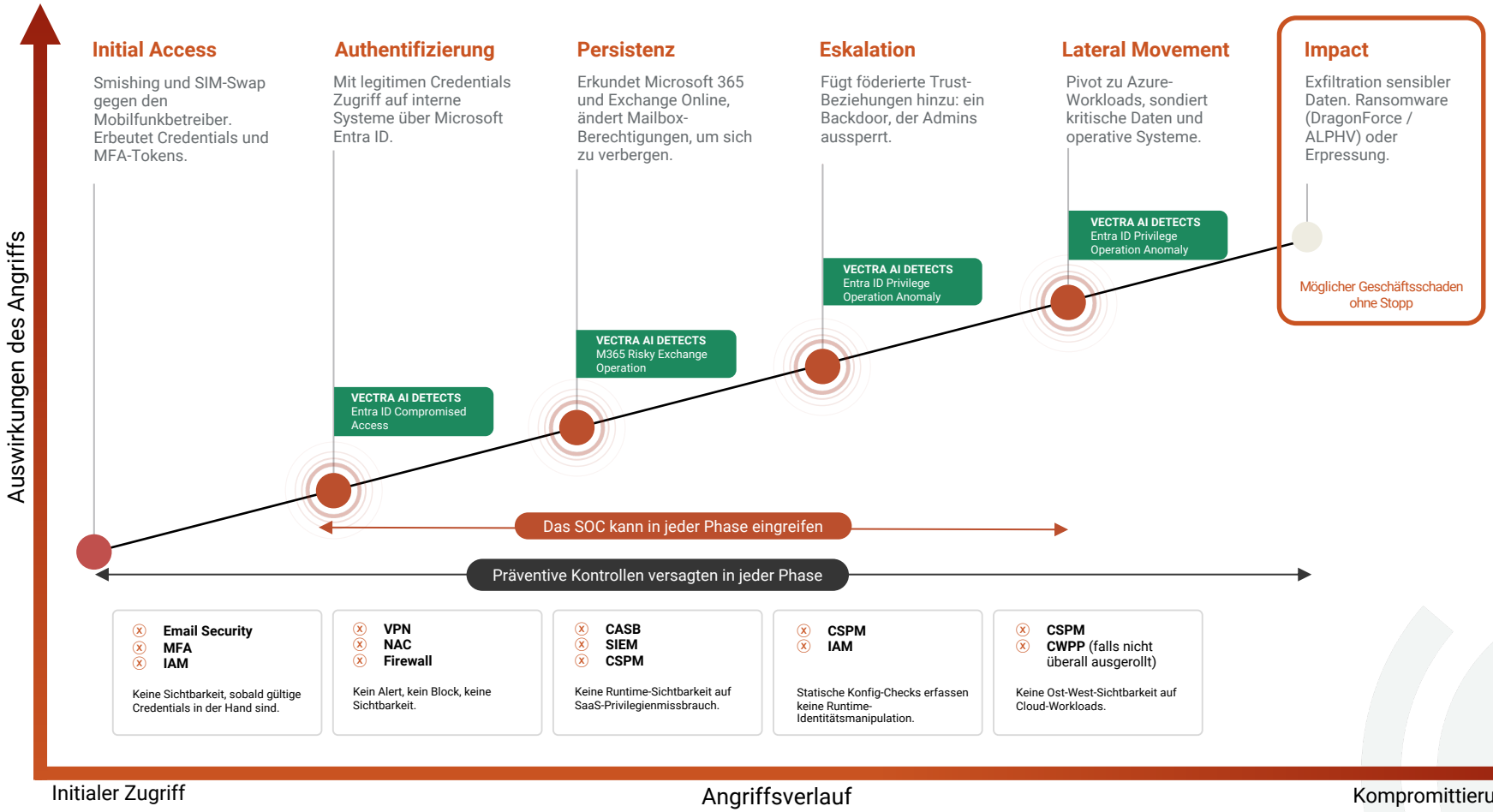
Gültige Credentials, MFA bestätigt, der Login ist echt. Nur ist es nicht die Person, die Sie denken. Jede Authentifizierungsprüfung sagt ja. Die Wahrheit: der gültige Nutzer ist nicht der Nutzer.

3. Die Bewegung ist nicht sichtbar.

Einmal drin, läuft Lateral Movement über vertraute Integrationen: SaaS-zu-SaaS, föderierte Identität, OAuth-Tokens, Service Accounts. Das EDR sieht es nicht. Das CASB sieht es nicht. Die Bewegung ist unsichtbar per Architektur, nicht per Tarnung.

Scattered Spider: das Helpdesk-Playbook

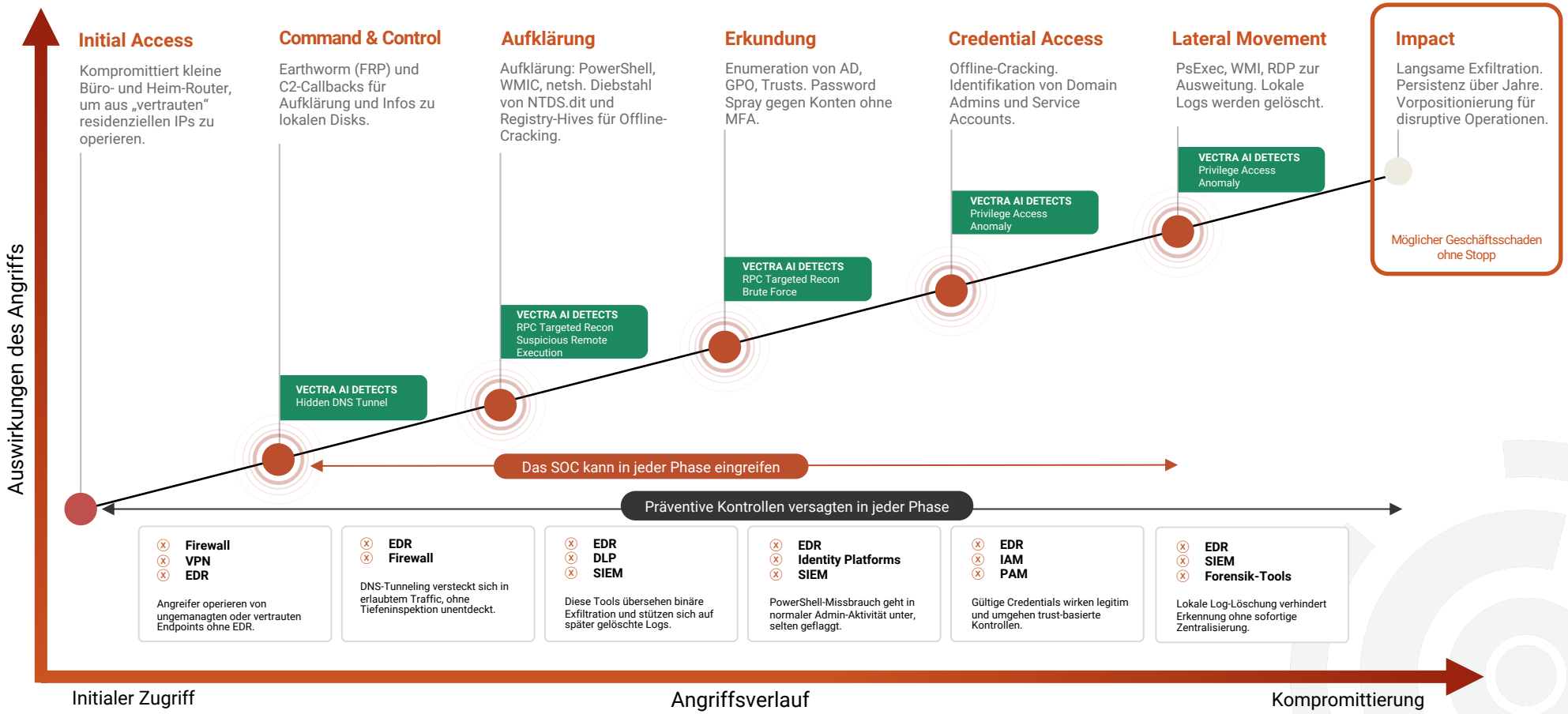
Scattered Spider (UNC3944) veranschaulicht perfekt, warum „gültige Credentials“ zu einem Erkennungsproblem geworden sind. Die Gruppe nutzte keine Schwachstellen. Sie rief den Helpdesk an.



Quellen: Mandiant UNC3944-Reporting (2023–2024); CISA Advisory AA23-320A zu Scattered-Spider-TTPs.

Volt Typhoon: das Living-off-the-Land-Playbook

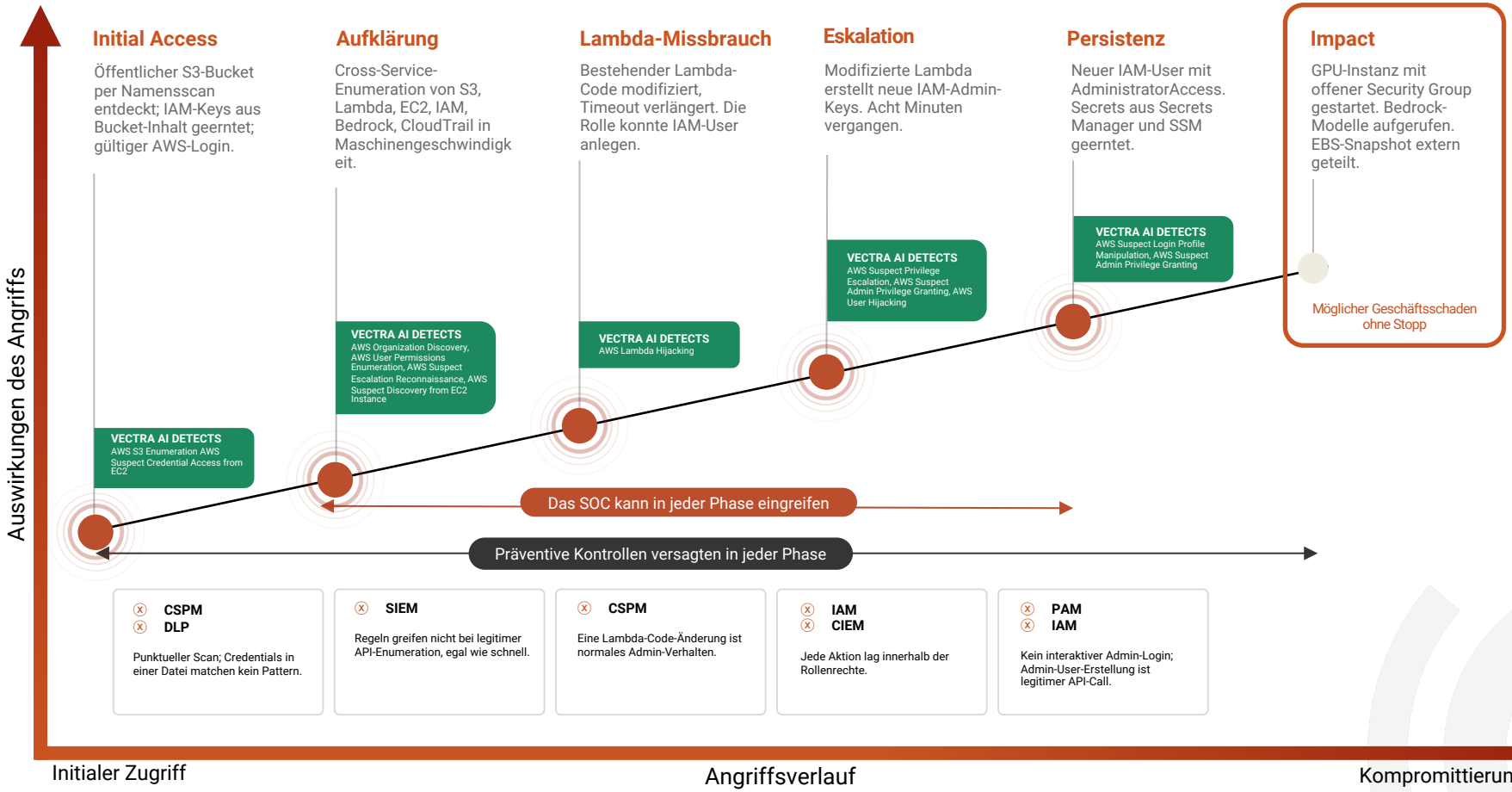
Volt Typhoon ist die der VRC zugeschriebene Kampagne, die US-Verteidigern gezeigt hat, wie „Living off the Land“ wirklich aussieht. Die CISA/NSA/FBI-Advisory von Februar 2024 dokumentierte Operatoren, die bis zu fünf Jahre in kritischer Infrastruktur saßen, ausschließlich mit nativen Windows-Tools, ohne erkennbare Malware.



Quellen: gemeinsame Advisory CISA/NSA/FBI AA24-038A (Feb. 2024); Microsoft Threat Intelligence „Volt Typhoon targets US critical infrastructure with living-off-the-land techniques“ (Mai 2023).

AWS in acht Minuten von KI-Agenten kompromittiert.

Von Sysdig dokumentierter Vorfall (2025). Gültige Credentials. Native AWS-Dienste. Aufklärung in Maschinengeschwindigkeit.



Quellen: Sysdig Threat-Research-Blog (2025); MITRE ATLAS-Techniken zu Missbrauch gültiger Konten und Cloud Service Discovery.

Warum Ihr Stack Sie blind macht.

Drei verschiedene Angreifer. Drei verschiedene Jahre. Drei verschiedene Einfallstore. Jede Attacke wirkte in jedem einzelnen Tool durchgehend legitim. Erst über Netzwerk, Identitätsebene und Cloud-Control-Plane hinweg wird die Absicht des Angreifers sichtbar.

Man könnte meinen: mit Firewalls, EDR, CASB, CSPM, IAM und SIEM seien die Gaps geschlossen. Die Realität: diese Tools wurden nicht für die Erkennung von Angreiferverhalten in Hybrid-Umgebungen gebaut, und die Daten zeigen es.

82 %

der Intrusion-Erkennungen 2025 waren malware-frei.

CrowdStrike 2026 Global Threat Report

32 %

mehr identitätsbasierte Angriffe in der ersten Hälfte 2025.

Microsoft Digital Defense Report 2025

241 Tage

um eine Kompromittierung zu erkennen und einzudämmen. 292, wenn gestohlene Credentials im Spiel sind.

IBM Cost of a Data Breach Report 2025

In den folgenden Abschnitten zeigen wir genau, wo jeder Teil Ihres Stacks zu kurz greift, und wie Vectra AI diese Gaps in Netzwerk, Cloud, SaaS und Identität schließt.

Endpoint-Sicherheit

Warum EDR und EPP allein nicht reichen.

EDR: tief am Host, sonst nirgends.

Endpoint Detection and Response liefert detaillierte Telemetrie, wo es ausgerollt ist.

EDR geht über Prävention hinaus mit Telemetrie und Analytics zu Prozessen, Registry und lokaler Aktivität. Stark dort, wo es installiert ist. Realität 2025: 82 % der Intrusion-Erkennungen waren malware-frei.[1] Angreifer operieren mit gültigen Credentials in vertrauten Sessions, wo EDR nichts zu flaggen hat.

WIE ANGREIFER UMGEHEN

- Meiden den Endpoint, indem sie in Cloud-Konsolen oder SaaS-Apps operieren.
- Nutzen Abdeckungs-Gaps. EDR sieht nur Hosts, auf denen es installiert ist.
- Bewegen sich über ungemanagte oder BYOD-Geräte ohne Agent.
- Nutzen gültige Credentials für Aktivitäten, die EDR als „normal“ liest.

EDR sieht keine Cloud-Native-Angriffe, Identitätsmissbrauch oder SaaS-Aktivität.

Drei der vier meistausgenutzten Schwachstellen 2024 waren Zero-Days in Security-Produkten: Palo Alto, Ivanti, Fortinet.[2]

[1] CrowdStrike 2026 Global Threat Report. [2] Mandiant M-Trends 2025

EPP: blockt bekannte Malware, blind für den Rest.

Endpoint Protection Platforms verhindern die Ausführung bekannter Bedrohungen.

Initialer Zugriff	●
Ausführung	●
Persistenz	○
Privilege Escalation	○
Defense Evasion	○
Credential Access	○
Erkundung	○
Lateral Movement	○
Sammlung	○
Command & Control	○
Exfiltration	○
Impact	○

SICHTBARKEIT: ● Partiell ● Voll ○ Keine

EPP nutzen Signaturen, Heuristiken und einfaches Sandboxing. Modernes EPP (NGAV) ergänzt Verhaltenserkennung und Fileless-ML, bleibt aber endpoint-gebunden und blind für Cross-Domain-Bewegungen.

WIE ANGREIFER UMGEHEN

- Fileless-Malware oder sorgfältiges Staging unter dem Verhaltensradar.
- Zero-Days oder neu kompilierte Binaries ohne Signatur.
- PowerShell, WMI, RDP: nicht zuverlässig von Admin-Aktivität zu unterscheiden.

EPP erkennt Living-off-the-Land oder credential-basierte Angriffe nicht zuverlässig.

Auch modernes EPP bleibt endpoint-gebunden. Cloud-Konsolen, Identitätsebene und SaaS-zu-SaaS sind by Design unsichtbar.

Der Endpoint-Security-Gap und wie Vectra AI ihn schließt.

DER ENDPOINT-GAP

EDR und EPP sind fundamental, decken aber nur einen Teil der Kill Chain.

Sie übersehen:

- Identitätsangriffe mit gültigen Credentials in M365 oder Entra ID.
- SaaS-Privilegienmissbrauch außerhalb des Endpoints.
- Lateral Movement über Cloud, BYOD, föderierte Identität.
- Aufklärung und Exfiltration über verschlüsselte oder Nicht-HTTP-Kanäle.

Auch auf Endpoints übersieht EPP häufig anspruchsvolles Verhalten, und EDR erkennt Account-Missbrauch ohne Malware nicht immer.

WAS VECTRA AI ERGÄNZT

- Identity Threat Detection für kompromittierte Konten, die SaaS und Cloud missbrauchen.
- SaaS Misuse Detection in M365, Exchange Online, Entra ID.
- Hybride Abdeckung: Endpoint, Cloud, Netzwerk, Identität.
- Integriert mit CrowdStrike, Microsoft Defender, SentinelOne und weiteren EDR-Plattformen.

VECTRA AI

Cloud-Sicherheit

Der blinde Fleck der Hybrid Cloud.

CASB: blind für aktiven Missbrauch.

Setzt Policies auf SaaS durch. Sieht keine Angreifer in gültigen Sessions.

Initialer Zugriff	●
Ausführung	○
Persistenz	○
Privilege Escalation	●
Defense Evasion	○
Credential Access	●
Erkundung	○
Lateral Movement	○
Sammlung	●
Command & Control	○
Exfiltration	●
Impact	○

SICHTBARKEIT: ● Partiell ● Voll ○ Keine

CASB setzt Policies per API oder Inline-Proxy durch. Im API-Modus (üblich) sehen sie Aktivität nahezu in Echtzeit, mit Minutenverzögerung. So oder so operiert CASB oberhalb der Netzwerk- und Identitätsebene, blind für das, was Angreifer in einer gültigen Session tun.

WIE ANGREIFER UMGEHEN

- Nutzen gültige Credentials für genehmigtes SaaS (M365, Box, Salesforce).
- Nutzen Berechtigungen von innen aus (Mailbox-Delegation).
- Missbrauchen föderiertes Vertrauen, um per SSO einzuloggen.

CASB liefert keine Sichtbarkeit auf Netzwerkebene.

Erkennt Live-Privilegienmissbrauch, Identitätsmanipulation oder Insider-Verhalten nicht immer.

CSPM: findet Misskonfigurationen, kein Verhalten.

Identifiziert riskante Settings. Gut für Prävention, nicht für Erkennung.

Initialer Zugriff	○
Ausführung	○
Persistenz	○
Privilege Escalation	●
Defense Evasion	○
Credential Access	●
Erkundung	○
Lateral Movement	○
Sammlung	○
Command & Control	○
Exfiltration	○
Impact	○

SICHTBARKEIT: ● Partiell ● Voll ○ Keine

CSPM flaggt offene S3-Buckets, exponierte SSH-Ports, deaktivierte Logs. Es ist präventionsorientiert, scannt Bedingungen, die Angriffe ermöglichen, nicht die Angriffe selbst.

WIE ANGREIFER UMGEHEN

- Nutzen eine Misskonfiguration, bevor sie behoben wird.
- Eskalieren in Cloud-Diensten über API-Tokens oder OAuth.
- Missbrauchen über-privilegierte IAM-Rollen, die CSPM zwar flaggt, aber nicht in Echtzeit überwacht.

CSPM liefert keine Sichtbarkeit auf Netzwerkebene.

Sieht keine Runtime-Aktivität, keinen Credential-Missbrauch, kein Lateral Movement. Es flaggt Bedingungen, keine Angriffe.

CWPP: schützt Workloads, wenn überall ausgerollt.

VMs, Container, Serverless, sofern Agenten ausgerollt sind.

Initialer Zugriff	●
Ausführung	●
Persistenz	●
Privilege Escalation	●
Defense Evasion	○
Credential Access	○
Erkundung	●
Lateral Movement	○
Sammlung	●
Command & Control	●
Exfiltration	○
Impact	●

SICHTBARKEIT: ● Partiell ● Voll ○ Keine

CWPP sichern Compute-Instanzen mit Runtime-Sichtbarkeit auf Cloud-Workloads. Die Abdeckung hängt von der Konsistenz des Rollouts ab.

WIE ANGREIFER UMGEHEN

- Verlagern sich auf ungemanagte Workloads oder Regionen ohne Agenten.
- Nutzen legitime Tools innerhalb eines Workloads (PowerShell, bash) zur Tarnung.
- Operieren ausschließlich in SaaS- oder Identitätsebenen, außerhalb der CWPP-Reichweite.

CWPP liefern keine Sichtbarkeit auf Netzwerkebene.

Blind für SaaS-Missbrauch und Cloud-IAM-Missbrauch.

CNAPP: konsolidiert, übersieht weiter Verhalten.

Kombiniert CSPM, CWPP, zunehmend CIEM und Runtime-Erkennung.

Initialer Zugriff	●
Ausführung	●
Persistenz	●
Privilege Escalation	●
Defense Evasion	●
Credential Access	●
Erkundung	●
Lateral Movement	●
Sammlung	●
Command & Control	●
Exfiltration	●
Impact	●

SICHTBARKEIT: ● Partiell ● Voll ○ Keine

Moderne CNAPP ergänzen Runtime-Erkennung (CDR) zum Posture-Scan. Doch die Runtime-Erkennung bleibt workload-gebunden. Sie sieht, was auf einem Workload passiert, nicht die Identitäts- und Netzwerk-Pivots zwischen Workloads.

WIE ANGREIFER UMGEHEN

- Nutzen föderierte Identität oder SaaS-Manipulation, die CNAPP nicht tief verfolgt.
- Operieren zwischen Workloads, der Erkennung entgehend, wenn Ost-West-Traffic nicht inspiziert wird.
- Bewegen sich schnell, bevor der nächste Konfig-Scan läuft.

CNAPP verbessert die Sichtbarkeit, aber nicht genug.

Es fehlt weiterhin Erkennung von Angreiferverhalten in Netzwerk, Cloud-Identität und SaaS.

CIEM: verwaltet Rechte, nicht das Verhalten darin.

Eigene Kategorie seit 2023.

Initialer Zugriff	○
Ausführung	○
Persistenz	○
Privilege Escalation	●
Defense Evasion	○
Credential Access	●
Erkundung	○
Lateral Movement	○
Sammlung	○
Command & Control	○
Exfiltration	○
Impact	○

SICHTBARKEIT: ● Partiell ● Voll ○ Keine

CIEM analysiert Cloud-Identitätsrechte: wer in AWS, Azure, GCP was tun darf. Flaggt über-privilegierte Rollen, ruhende Zugriffe, übermäßige Berechtigungen.

WIE ANGREIFER UMGEHEN

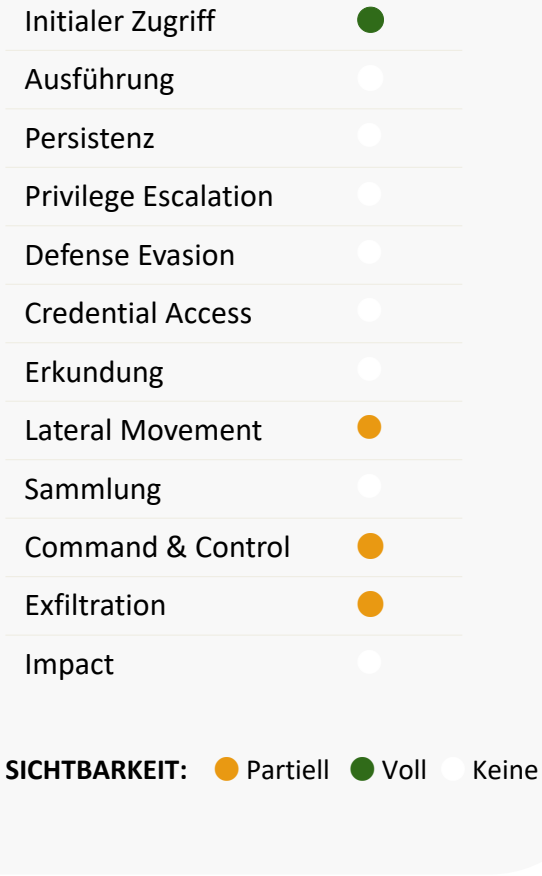
- Nutzen Rechte mit niedriger Risikoeinstufung, die in Verkettung zur Privilege Escalation reichen.
- Handeln innerhalb genehmigter Grenzen auf Wegen, die die Baseline nie modelliert hat.
- Missbrauchen föderierte Rollen und Cross-Account-Trust. CIEM kartiert sie, überwacht aber nicht in Echtzeit.

CIEM flaggt Über-Privilegien. Es erkennt keinen Missbrauch legitimer Privilegien.

Wie CSPM und CNAPP arbeitet CIEM auf Posture-Ebene. Rechte sind statisch; Angriffe sind dynamisches Verhalten innerhalb dieser Rechte.

SASE: steuert Zugriff, nicht was danach passiert.

SWG + ZTNA + CASB + DLP, vereint.



SASE steuert, wie Nutzer auf Apps zugreifen, erkennt aber nicht, was sie in der Cloud tun, sobald der Zugriff gewährt ist.

WIE ANGREIFER UMGEHEN

- Authentifizieren sich mit gestohlenen Credentials und umgehen Trust-Modelle.
- Missbrauchen legitime SaaS-Funktionen (Mailbox-Regeln, Sharing) zum Halten und Stehlen.
- Bewegen sich lateral über Cloud-Native-Pfade (IAM-Rollen-Chaining, föderiertes Trust).

SASE sieht Zugriffspfade, nicht das Angreiferverhalten darin.

Der Cloud-Security-Gap und wie Vectra AI ihn schließt.

DER CLOUD-GAP

Cloud-Tools sind stark in Prävention, schwach in Erkennung.

Sie übersehen:

- SaaS-Privilegienmissbrauch (Mailbox-Delegation in M365).
- Föderierte Identitäts-Backdoors (Entra-ID-Trust-Manipulation).
- Ost-West-Traffic in der Cloud (zwischen VPCs, Containern, Konten).
- Cross-Account-API-Patterns und IAM-Rollen-Chaining.
- Cloud-Native Command-and-Control (AWS-STS-Tokens, Entra-ID-Rollen).

Missbrauch gültiger Konten machte 2025 35 % der Cloud-Vorfälle aus. Cloud-bewusste Eindringlinge stiegen um 37 % im Jahresvergleich, 266 % bei Staatsakteuren.[1]

WAS VECTRA AI ERGÄNZT

- Echtzeit-Erkennung in M365, Entra ID, AWS, Azure, GCP, Föderation.
- Sieht, was Posture-Tools übersehen: wer tut gerade was.
- Verhaltenskorrelation über Identität, Netzwerk, Cloud.

[1] CrowdStrike 2026 Global Threat Report.

Netzwerk-Sicherheit

Wenn Traffic normal aussieht, aber nicht ist.

Email Security: stoppt Spam, kein Social Engineering.

Blockiert bekannt-böse Nachrichten. Übersieht die Kompromittierung nach erfolgreichem Phishing.

Initialer Zugriff	●
Ausführung	○
Persistenz	○
Privilege Escalation	○
Defense Evasion	○
Credential Access	○
Erkundung	○
Lateral Movement	○
Sammlung	○
Command & Control	○
Exfiltration	○
Impact	○

SICHTBARKEIT: ● Partiell ● Voll ○ Keine

Secure Email Gateways und Anti-Phishing-Filter blockieren bekannt-böse Nachrichten. Doch Angreifer setzen auf gut gemachtes Phishing und Social Engineering, das die klassische Erkennung umgeht.

WIE ANGREIFER UMGEHEN

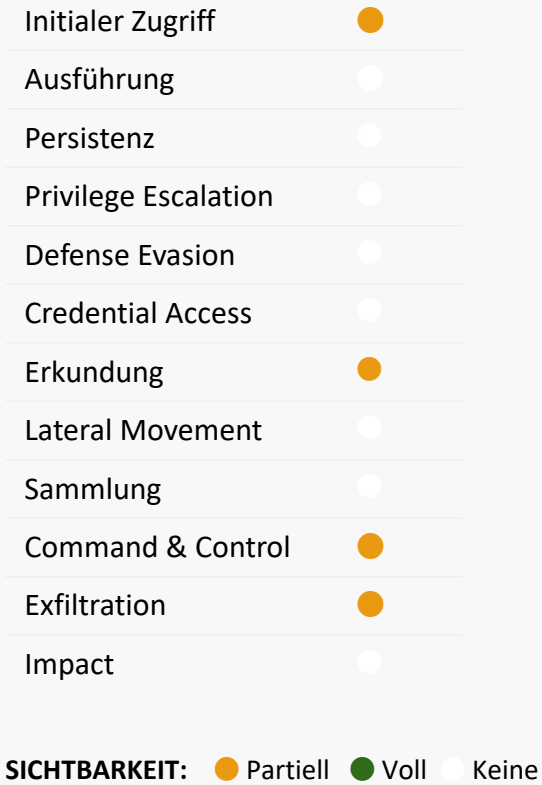
- Schicken Credential-Phishing per SMS, LinkedIn oder privater Mail, an Firmenfiltern vorbei.
- Nutzen Lookalike-Domains oder MFA-Fatigue, um Credentials zu erlangen.
- Nutzen Vertrauen aus, keine Malware. Kein Anhang, kein Link wird geflaggt.

Email Security erkennt keine Kompromittierung nach Phishing.

Genau dort spielen sich die meisten modernen Kompromittierungen ab.

Firewalls: kontrollieren den Rand, nicht das Innere.

Klassische und Next-Gen-Firewalls beschränken am Perimeter; passiert ein vertrauter Nutzer, sind sie blind.



Klassische Firewalls filtern nach IP, Port, Protokoll. NGFW ergänzen Application-Layer-Inspection und TLS-Decryption. In beiden Fällen hat die Firewall ihren Job getan, sobald ein vertrauter Nutzer mit gültigen Credentials passiert.

WIE ANGREIFER UMGEHEN

- Erlaubte Protokolle (HTTPS, DNS, RDP) zur unbemerkten Bewegung.
- Verschlüsselte Kanäle, die Firewalls nicht vollständig inspizieren können.
- VPNs oder SSO, um sich als vertraute Nutzer zu authentifizieren.

Firewalls erkennen kein C2 in genehmigten Protokollen, kein Lateral Movement, keinen SaaS-Zugriff mit gültigen Credentials.

IDPS: findet Signaturen, keine Tarnung.

Signatur-Matching erfasst bekannte Muster, nicht das, was anspruchsvolle Angreifer nutzen.

Initialer Zugriff	●
Ausführung	○
Persistenz	○
Privilege Escalation	○
Defense Evasion	○
Credential Access	○
Erkundung	◐
Lateral Movement	◐
Sammlung	○
Command & Control	◐
Exfiltration	◐
Impact	○

SICHTBARKEIT: ◐ Partiell ● Voll ○ Keine

Intrusion Detection and Prevention Systems suchen bekannte Angriffsmuster. Anspruchsvolle Angreifer nutzen sie selten.

WIE ANGREIFER UMGEHEN

- Maßgeschneiderte oder verschlüsselte Payloads, die Signaturen umgehen.
- Living off the Land mit legitimen Tools und Ports.
- Drosseln Aktivität, um unter Erkennungsschwellen zu bleiben.

IDPS scheitert an neuen Techniken und verschlüsseltem Ost-West-Traffic.

NAC: entscheidet, wer verbindet, nicht was danach passiert.

Validiert Geräte-Posture und Identität bei Verbindung. Verliert Sichtbarkeit drinnen.

Initialer Zugriff	●
Ausführung	
Persistenz	
Privilege Escalation	
Defense Evasion	
Credential Access	
Erkundung	
Lateral Movement	
Sammlung	
Command & Control	
Exfiltration	
Impact	

SICHTBARKEIT: ● Partiell ● Voll ○ Keine

Network Access Control validiert Geräte-Posture und Identität vor Zugriffsfreigabe. Sobald der Nutzer verbunden ist, verliert NAC die Sichtbarkeit.

WIE ANGREIFER UMGEHEN

- Kapern vertraute Credentials oder Geräte für Zugriff ohne NAC-Auslösung.
- Bewegen sich zwischen vertrauten Systemen, die NAC nicht überwacht.
- Nutzen ungemanagte oder BYOD-Geräte, die durch Posture-Checks rutschen.

NAC erkennt kein Lateral Movement, keinen verdächtigen Traffic, kein Post-Authentifizierungsverhalten.

SSE: der moderne Perimeter, mit alten Gaps.

Security Service Edge: SWG + ZTNA + CASB + FWaaS, aus der Cloud. Der Ersatz für Firewall + VPN.

Initialer Zugriff	●
Ausführung	○
Persistenz	○
Privilege Escalation	○
Defense Evasion	○
Credential Access	○
Erkundung	○
Lateral Movement	◐
Sammlung	○
Command & Control	◐
Exfiltration	◐
Impact	○

SICHTBARKEIT: ◐ Partiell ● Voll ○ Keine

Security Service Edge konsolidiert Secure Web Gateway, Zero Trust Network Access, CASB und Firewall-as-a-Service zu einer Cloud-Plattform. SSE hat in vielen Unternehmen den klassischen Firewall-+-VPN-Stack ersetzt aber erbt denselben blinden Fleck jedes Perimeter-Tools.

WIE ANGREIFER UMGEHEN

- Authentifizieren sich mit gestohlenen Credentials.. ZTNA genehmigt: das Credential ist gültig.
- Operieren in genehmigten Apps.. SWG sieht das Ziel, nicht die Aktivität in der Session.
- Pivot über Cloud-Native (IAM-Chaining, OAuth) am SSE-Proxy vorbei.
- Exfiltrieren über SaaS-zu-SaaS, für SSE unsichtbar.

SSE ersetzt die Firewall, nicht die fehlende Erkennungsschicht dahinter.

Dasselbe Vectra-schließt-den-Gap-Argument gilt für SSE-geschützte Umgebungen wie für klassische Firewall-Umgebungen.

Der Netzwerk-Security-Gap und wie Vectra AI ihn schließt.

DER NETZWERK-GAP

Ihre Netzwerk-Tools sind Prävention und Kontrolle, keine Erkennung.

Sie übersehen:

- Lateral Movement zwischen Workloads und Regionen, Cloud und Hybrid.
- Command-and-Control über verschlüsselte oder vertraute Protokolle.
- Datenexfiltration als Geschäftsverkehr getarnt.
- Verhaltensanomalien in Ost-West-Bewegung, privilegiertem Zugriff, Credential-Nutzung.
- Post-Authentifizierungsverhalten in SSE-geschützten Sessions.

WAS VECTRA AI ERGÄNZT

- Echtzeit-Analyse: On-Prem, Cloud, SaaS.
- Erkennt Lateral Movement, Eskalation, Exfiltration, (auch verschlüsselt, per Metadaten).
- Integriert mit SIEM und SOAR für hochpräzise Alerts.
- Integriert sich nativ in jede Firewall, die das Einlesen externer dynamischer Blocklisten unterstützt.

Identitäts-Sicherheit

Wenn gültige Logins zu unsichtbaren Bedrohungen werden.

IAM: verhindert unautorisierten Zugriff, keinen missbrauchten.

Kontrolliert den Zugang, setzt danach aber Vertrauen voraus.

Initialer Zugriff	●
Ausführung	○
Persistenz	○
Privilege Escalation	●
Defense Evasion	○
Credential Access	○
Erkundung	○
Lateral Movement	○
Sammlung	○
Command & Control	○
Exfiltration	○
Impact	○

SICHTBARKEIT: ● Partiell ● Voll ○ Keine

IAM steuert, wer sich von wo mit welchen Rechten anmelden darf. Moderne IdP ergänzen Risiko-Signale (Impossible Travel, geleakte Credentials, ungewohnte Geräte) doch diese arbeiten am Authentifizierungspunkt. Sobald eine gültige Session existiert, setzt IAM Vertrauen voraus. MFA blockt über 99 % der Identitätsangriffe, und doch stiegen Identitätsangriffe in der ersten Hälfte 2025 um 32 %[1] : gestohlene Tokens, genehmigte OAuth-Apps, Device-Code-Flows und AiTM-Proxies umgehen MFA.

WIE ANGREIFER UMGEHEN

- Stehlen gültige Credentials oder Session-Tokens und melden sich als Legitime an.
- Bewegen sich lateral mit über-privilegierten Konten oder fehl-konfigurierten Policies.
- Authentifizieren sich über vertraute IdP, inklusive Federation und SSO.
- Zielen auf Session-Cookies (z. B. ESTSAUTHPERSISTENT), die MFA umgehen.

IAM setzt Login-Policies durch. Es sieht nicht, was nach dem Login passiert.

97 % der Identitätsangriffe sind Passwort-Angriffe[1]. MFA stoppt den Passwort-Angriff. Nichts in IAM stoppt den anschließenden Missbrauch.

[1] Microsoft Digital Defense Report 2025:

PAM: schützt privilegierte Konten, wenn man weiß welche.

Schränkt privilegierten Zugriff ein. Doch Angreifer brauchen ihn nicht immer zur Eskalation.

Initialer Zugriff	○
Ausführung	○
Persistenz	○
Privilege Escalation	●
Defense Evasion	○
Credential Access	◐
Erkundung	○
Lateral Movement	○
Sammlung	○
Command & Control	○
Exfiltration	○
Impact	○

SICHTBARKEIT: ◐ Partiell ● Voll ○ Keine

PAM-Lösungen schränken ein, wie Nutzer auf kritische Systeme zugreifen: Passwort-Vaults, Session-Aufzeichnung, Just-in-Time-Zugriff. Doch Angreifer brauchen nicht zwingend ein privilegiertes Konto, um zu eskalieren.

WIE ANGREIFER UMGEHEN

- Missbrauchen nicht-privilegierte Konten zur Eskalation über SaaS-Rechte (Mailbox-Delegation, OAuth-Scopes).
- Nutzen föderiertes Trust für Zugriff ohne PAM-kontrollierte Konten.
- Nutzen Shadow Admins (Rollen mit faktischen Privilegien, die nicht als „privilegiert“ markiert sind).

PAM erkennt keinen Identitätsmissbrauch außerhalb vordefinierter Privilegiengrenzen.

UEBA: berechnet Risiko, aber nicht in Echtzeit.

Zunehmend Feature in SIEM/XDR statt eigene Kategorie.

Initialer Zugriff	●
Ausführung	○
Persistenz	●
Privilege Escalation	●
Defense Evasion	●
Credential Access	●
Erkundung	●
Lateral Movement	●
Sammlung	○
Command & Control	○
Exfiltration	●
Impact	○

SICHTBARKEIT: ● Partiell ● Voll ○ Keine

UEBA baut Profile normalen Verhaltens und vergibt Risiko-Scores bei Abweichungen. Es benötigt vollständige Daten und reagiert oft zu spät. Gartner pflegt keinen separaten UEBA-Magic-Quadrant mehr.

WIE ANGREIFER UMGEHEN

- Imitieren normales Nutzerverhalten (gleicher Ort, Gerät, Pattern).
- Agieren langsam oder außerhalb der Bürozeiten, ohne sichtbare Spitzen.
- Nutzen unvollständige Log-Quellen, sodass UEBA das Gesamtbild nie sieht.

UEBA verzögert die Erkennung und liefert keine Echtzeit-Sicht auf Identitätsmissbrauch.

Der Identity-Security-Gap und wie Vectra AI ihn schließt.

DER IDENTITY-GAP

Die meisten Tools fokussieren auf Zugriffskontrolle oder Risiko-Scoring, nicht auf Angreiferverhalten. ITDR (Identity Threat Detection and Response) ist entstanden, um zu sehen, was IAM nicht sehen kann.

Sie sehen nicht:

- Credential-Missbrauch über SaaS und Cloud.
- Privilege Escalation in Entra ID oder Exchange Online.
- Missbrauch von Trust-Beziehungen zwischen IdP.
- Identitätsbasiertes Lateral Movement ohne Endpoint-Berührung.

WAS VECTRA AI ERGÄNZT

- AD, Entra ID, M365 / Exchange Online, Azure / AWS, Cloud-IAM-Rollen, föderierte Identität.
- Erkennung von SaaS-Privilegienmissbrauch (Delegation, OAuth).
- Erkennung von Föderationsmanipulation (Trust, Role Impersonation).
- Credential-Missbrauch in Hybrid, auch nach erfolgreicher MFA.

Regulatorischer Druck: Erkennung ist der Beweis.

Compliance ist kontinuierlich, und kontinuierliche Compliance braucht kontinuierliche Erkennung.

Policy-Ordner und jährliche Attestierungen reichen nicht für eine 24-Stunden-Meldepflicht. Sieht Ihr Stack den Angriff nicht, löst kein Compliance-Rahmen das Problem.

NIS2

In Kraft seit Oktober 2024

Verlangt geeignete technische Maßnahmen für Erkennung und Reaktion. Schreibt die Meldung erheblicher Vorfälle binnen 24 Stunden vor. Artikel 21(2)(b) verlangt explizit eine Incident-Handling-Fähigkeit.

DORA

In Kraft seit Januar 2025

Kapitel II verlangt operative Resilienz. Meldefenster für IKT-Vorfälle sind kurz. Erwartet wird kontinuierlicher Beweis, dass die Erkennung funktioniert, kein Stichtags-Audit.

IT-Sicherheitsgesetz 2.0 / BSI-Gesetz (KRITIS)

SiG 2.0 seit 2021, KRITIS-V seit 2017

KRITIS-Betreiber (Energie, Wasser, Ernährung, IT/TK, Finanz, Verkehr, Gesundheit) müssen erhebliche IT-Sicherheitsvorfälle unverzüglich an das BSI melden. Verlangt nachweisbare Erkennung und Reaktion, nicht nur Prävention.

Die Frage der Compliance ist heute eine Frage der Erkennung.

Fazit

Schließen Sie den Gap, bevor er ausgenutzt wird.

Was Sie nicht sehen, können Sie nicht verteidigen.

Heutige Angreifer setzen nicht auf Malware. Ihre klassischen Tools waren dafür nicht gebaut.

Angreifer nutzen Credentials, missbrauchen SaaS-Misskonfigurationen, manipulieren Identitätsvertrauen und bewegen sich durch Cloud-Workloads ungesehen.

Klassische Tools sehen diese Aktivität nicht, nicht weil sie defekt sind, sondern weil sie nicht dafür gebaut wurden.

- EDR sieht keinen Identitätsmissbrauch in M365.
- CASB und SASE sehen kein Lateral Movement in Cloud-Workloads.
- SIEM kann nicht alarmieren auf das, was vorgelagerte Tools nicht sehen.

Und Ihr SOC bleibt zurück mit zu vielen Alerts, zu wenig Kontext und keiner echten Sichtbarkeit über die Hybrid-Infrastruktur.

Wie Vectra AI Ihren Stack vervollständigt.

Und was Kunden messen, wenn sie es einsetzen. IDC Business Value Study, 2025.

SECURITY-FÄHIGKEIT	WAS FEHLT	WAS VECTRA AI ERGÄNZT
Endpoint-Threat-Detection	Blind für Netzwerk und Cloud	Echtzeit-Erkennung im gesamten Traffic (agentenlos)
Identity-Threat-Detection	Keine Sichtbarkeit nach der Authentifizierung	Erkennt Missbrauch gültiger Konten und Privilege Escalation
Cloud-Threat-Sichtbarkeit	Blind für Hybrid-Angreiferverhalten	Erkennt Cloud-Native, Hybrid, SASE, SaaS, IaaS
Lateral-Movement-Erkennung	Unsichtbar im Hybrid	Echtzeit-Erkennung von Lateral Movement
Rauschreduktion	Alert-Fatigue	KI-getriebene Signalklarheit, hochpräzise Detektionen

WAS VECTRA MESSBAR LEISTET — IDC 2025

391 %
ROI über 3 Jahre

6 Mon.
Payback

3,4 Mio. $
jährlicher Nutzen

40 %
effizienteres SOC

60 %
weniger Zeit für Alerts

69,4 %
weniger Kompromittierungen

99,9 %
Produktivitätsverlust vermieden

Quelle: IDC Business Value Study of Vectra AI, April 2025

Vectra AI schließt Ihre Attack-Gaps.

Observability. Signal. Kontrolle. Und echte Ergebnisse von echten Kunden.

Observability

Vectra AI analysiert die Netzwerkaktivität laufend und macht jede Identität, jedes Gerät und jeden KI-Agenten in Echtzeit sichtbar, sodass SecOps-Teams jederzeit wissen, wer im Netzwerk was tut.

Signal

Durch Korrelation und Kontextualisierung von Aktivitäten in Hybrid-Umgebungen hilft Vectra AI Teams, echte Risiken zu priorisieren, schneller zu untersuchen, sicher zu jagen und Angriffe vor dem Schaden zu stoppen.

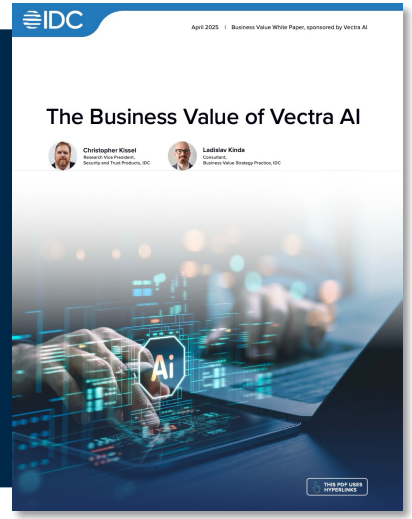
Kontrolle

Vectra AI zeigt, wer und was im Netzwerk ist, welche Aktivität auf einen Angriff hindeutet und wo sich Exponierung verändert, damit Sie Risiko senken, effizienter werden und Compliance belegen können.

AUS EINEM IDC-INTERVIEW · GLOBALER KOSMETIKKONZERN

„Vor Vectra AI bekamen wir keine Alerts und erfuhren von Red-Team-Zugriffen erst aus deren Jahresreports, die regelmäßig Domain-Admin- und Root-Zugang zeigten. Im ersten Jahr mit Vectra haben wir das Red Team erkannt, ausgeworfen und vollständig besiegt. Vectra ist mein wichtigstes Security-Tool."

Dasselbe SOC-Team läuft mit 7 Vollzeitäquivalenten (FTEs). Ihr Benchmark sagt, sie bräuchten 14.



Self-Assessment: welche Gaps exponieren Sie?

Lesen Sie jede Aussage. Haken Sie an, was auf Ihre Umgebung zutrifft. Die Haken sind die Gaps, die Sie tragen.

GAP 1

Nichts wirkt verdächtig.

- [ ] Wir sehen PowerShell, RDP und WMI in EDR-Alerts, und gehen meist von Admin-Aktivität aus.
- [ ] Wir haben keine dokumentierte Baseline für „normales" Admin-Verhalten.
- [ ] EDR-Alerts zu „potenziell unerwünschten" Prozessen bleiben manchmal länger als einen Tag ungeprüft.
- [ ] Bei zwei Wochen Living-off-the-Land mit signierten Binaries: nicht sicher, ob wir es bemerken.
- [ ] Detection-Regeln unterscheiden angreifer-erstellte Scheduled Tasks nicht zuverlässig von legitimen.

GAP 2

Die Authentifizierung ist erfolgreich.

- [ ] MFA ist für menschliche Nutzer erzwungen, aber bei Service Accounts und Workload Identities sind wir uns weniger sicher.
- [ ] Unser primäres Identitätssignal ist der IdP-Risk-Score (Impossible Travel, ungewohntes Gerät).
- [ ] Wir nehmen M365-, Entra-ID- oder Okta-Audit-Logs nicht in eine Erkennungsschicht jenseits des IdP auf.
- [ ] Bei einem von Infostealer gestohlenen und wiederverwendeten Session-Token: keine spezifische Erkennung.
- [ ] Nach Reset eines Credentials oder MFA-Faktors überwacht nichts automatisch das Account-Verhalten in den nächsten 24 Stunden.

GAP 3

Die Bewegung ist nicht sichtbar.

- [ ] Unsere Netzwerkerkennung ist nur Nord-Süd, wir sehen keinen Ost-West-Traffic zwischen Workloads.
- [ ] SMB- oder RDP-Lateral-Movement zwischen Segmenten mit ungleichmäßiger EDR-Abdeckung erkennen wir nicht zuverlässig.
- [ ] Cloud-Control-Plane-API-Calls (AWS STS, Entra-ID-Rollen) speisen unsere Erkennung nicht in Echtzeit.
- [ ] Für OAuth-App-Pivots zwischen genehmigten SaaS haben wir keine Erkennung.
- [ ] „Dwell Time" in SOC-Reports kommt aus Vorfallsrekonstruktion, nicht aus kontinuierlicher Messung.

So lesen Sie Ihren Score: **0–3 angekreuzt** = sinnvolle Abdeckung. **4–7 angekreuzt** = der Gap exponiert Sie messbar. **8–11 angekreuzt** = primärer Angreiferpfad in Ihre Umgebung. **12+ angekreuzt** = die Erkennung ist über die gesamte Angriffskette unvollständig.

Über Vectra AI

Die Vectra AI Plattform schützt moderne Unternehmen, indem sie Angriffe auf Netzwerk, Identität und Cloud als einheitliche Angriffsfläche erkennt und stoppt. Sie kombiniert Threat Exposure Management, KI-gestützte Detection und Response sowie Posture Improvement, um das Risiko vor Angriffsbeginn zu reduzieren und laufende Bedrohungen zu stoppen. Security-Teams gewinnen klares Signal, schnellere Reaktion und messbare Resilienzfortschritte. Mehr Informationen unter www.vectra.ai.