SIEM versus XDR versus NDR

Welche Systeme schützen wirklich vor Cyberattacken?

Kai-Oliver Detken

Technische Strategien gibt es viele, um Unternehmen vor Cyberattacken zu schützen. Aber viele IT-Verantwortliche steigen durch die pure Anzahl möglicher Sicherheitssysteme nicht mehr durch. Hinzu kommt, dass sich nicht immer alle Tools gegenseitig ergänzen, wenn man nicht auf einen Hersteller vertrauen möchte. Und auch die Strategie ist unterschiedlich: während SIEM-Systeme auf eine menschliche Reaktion warten, setzen XDR-Systeme auf Automation mit Künstlicher Intelligenz (KI). Dieser Artikel soll etwas Licht in die unterschiedlichen technischen Möglichkeiten bringen und Empfehlungen für Unternehmen aussprechen, die sich effektiver als bisher absichern wollen oder müssen.

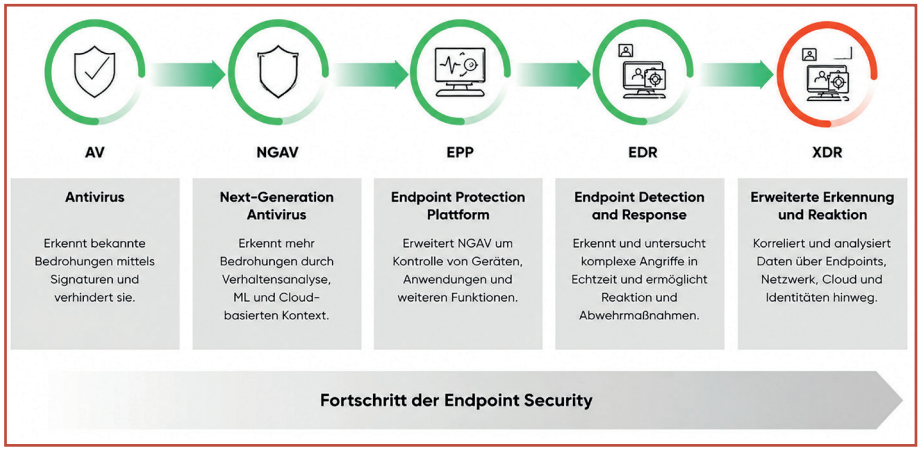

Abbildung 1: Endpunktschutz-Entwicklung – vom AV- bis zum XDR-System. XDR integriert Bedrohungsdaten und Telemetriedaten mit Sicherheitsanalysen, um Sicherheitswarnungen zu kontextualisieren und zu korrelieren

Jedes Unternehmen, unabhängig von der Größe, besitzt heute eine IT-Infrastruktur, die zumindest mit Anti-Viren-Lösungen, Firewalls, Monitoring- und Backup-Systemen abgesichert ist. Oftmals kommen Remote-Zugänge mittels VPN-Gateway hinzu, die externen Mitarbeitern ermöglichen von außen sicher auf das Unternehmensnetz und seine Dienste zuzugreifen. Sind höhere Ansprüche vorhanden, so wird auf Zugangskontrolle mittels Network Access Control (NAC) oder Angriffserkennung über Intrusion Detection- (IDS) und Intrusion Prevention Systeme (IPS) gesetzt. Allerdings sind die verschiedenen Systeme oftmals als Insellösungen implementiert, insbesondere, wenn sie nicht vom gleichen Hersteller kommen. Zusätzlich erschwert dies auch die Erkennung von Angriffsmustern.

Um dem erhöhten Schutzbedarf, zum Beispiel durch Verschlüsselungstrojaner, Rechnung zu tragen, sind in der jüngsten Vergangenheit weitere IT-Sicherheitssysteme hinzugekommen, die zu einem vollumfänglichen Schutz beitragen sollen:

- Endpoint Detection and Response (EDR): Weiterentwicklung klassischer Antivirenprogramme, überwacht Laptops, Smartphones und Server kontinuierlich auf verdächtige Aktivitäten.
- eXtended Detection and Response (XDR): Plattform, die Sicherheitsdaten aus verschiedenen Quellen (wie Endgeräten, E-Mails, Cloud-Workloads und Netzwerken) automatisch erfasst, korreliert und analysiert. Erweiterte Erkennung und Reaktion gegenüber EDR-Systemen.
- Security Information and Event Management (SIEM): Cybersicherheitslösung, die Protokolldaten aus dem gesamten IT-Netzwerk sammelt, zentralisiert und analysiert. Es erkennt potenzielle Bedrohungen und Sicherheitsvorfälle in Echtzeit, um Angriffe frühzeitig abzuwehren.
- Security Orchestration, Automation and Response (SOAR): ist eine Softwarelösung, die es Sicherheitsteams ermöglicht, separate Sicherheitstools zu integrieren und zu koordinieren, sich wiederholende Aufgaben zu auto-

Prof. Dr.-Ing. Kai-Oliver Detken studierte Informationstechnik an der Universität Bremen und promovierte im Fachbereich Informatik. Heute ist er Geschäfts-führer der DECOIT GmbH, doziert an der Hochschule Bremen und arbeitet als freier Autor im IT-Umfeld

matisieren und Workflows bei der Reaktion auf Vorfälle und Bedrohungen zu optimieren.

EDR- und XDR-Systeme

EDR-Systeme werden oftmals auch als Endpoint Threat Detection and Response (ETDR) bezeichnet und sind darauf ausgelegt Endpoint-Security herzustellen. Damit sind Komponenten wie Laptops, Smartphones, Arbeitsplatzrechner und IoT-Geräte gemeint, die kontinuierlich überwacht werden müssen.

EDR-Techniken dienen der Erkennung verdächtigten Verhaltens und fortgeschrittener, persistenter Bedrohungen (Advanced Persistent Threat, APT) auf Endgeräten und alarmieren die IT-Administratoren entsprechend. Dies geschieht durch das Sammeln und Aggregieren von Daten von Endgeräten und anderen Quellen. Diese Daten können durch zusätzliche Cloud-Analysen angereichert werden. EDR-Lösungen sind primär ein Alarmierungstool und keine Schutzschicht, wobei die Funktionen je nach Anbieter kombiniert werden können. Die Daten können in einer zentralen Datenbank gespeichert oder zur Cyberüberwachung an ein SIEM-Tool weitergeleitet werden.

Jede EDR-Plattform verfügt über spezifische Funktionen. Zu den gemeinsamen Funktionen gehören die Überwachung von Endpunkten im Online- und Offline-Modus, die Echtzeit-Reaktion auf Bedrohungen, die Verbesserung der Transparenz von Benutzerdaten, die Erkennung gespeicherter Endpunktereignisse und Malware-Einschleusungen, die Erstellung von Sperr- und Zulassungslisten sowie die Integration mit anderen Technologien. Einige Anbieter von EDR-Technologien nutzen die kostenlose MITRE ATT&CK-Klassifizierung und das zugehörige Framework zur Bedrohungsanalyse. Es handelt sich dabei um eine weltweit zugängliche Wissensdatenbank zu Taktiken und Techniken von Angreifern, die auf Beobachtungen aus der Praxis basiert.

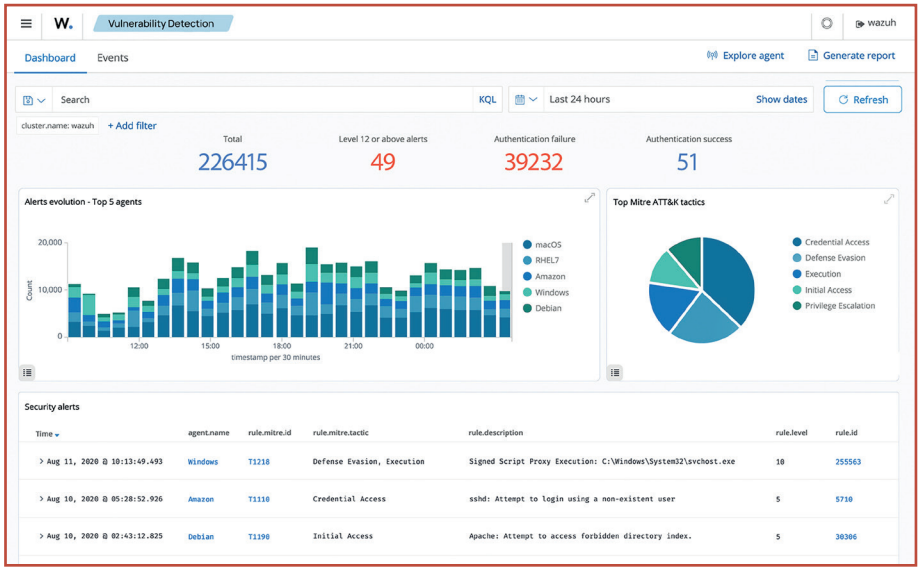

Abbildung 2: Das XDR-System Wazuh enthält verschiedene Sicherheitslösungen und -technologien, wodurch Echtzeit-Monitoring, Bedrohungserkennung, Compliance-Management und Schwachstellenanalyse miteinander kombiniert wird (Grafiken: Detken)

Ein XDR-System kann hingegen als weiterer Evolutionsschritt von einem DER-System angesehen werden (siehe Abbildung 1). Es handelt sich dabei weniger um ein weiteres Tool, sondern vielmehr um eine Sammlung und Integration mehrerer Konzepte in eine einzelne Lösung. Dabei können die Komponenten je nach Anbieter variieren und beinhalten häufig die Netzwerkanalyse und Intrusion Detection Systeme (IDS). Der Unterschied ist, dass Funktionen zur Erkennung von Sicherheitsvorfällen und zur automatisierten Reaktion auf Sicherheitsvorfälle in der Sicherheitsinfrastruktur bereitgestellt werden. XDR integriert dabei Bedrohungsdaten und Telemetriedaten aus verschiedenen Quellen mit Sicherheitsanalysen, um Sicherheitswarnungen zu kontextualisieren und zu korrelieren. XDR benötigt native Sensoren und kann lokal oder als SaaS-Lösung bereitgestellt werden. Typischerweise wird es von Organisationen mit kleineren Sicherheitsteams eingesetzt.

Abbildung 2 zeigt als XDR-Beispielsystem Wazuh, welches auch als leichtgewichtiges SIEM-System bezeichnet werden kann. Es vereint Bedrohungserkennung sowie Überwachung und Reaktion. Wazuh enthält verschiedene Sicherheitslösungen und -technologien, wodurch Echtzeit-Monitoring, Bedrohungserkennung, Compliance-Management und Schwachstellenanalyse miteinander kombiniert wird. Die Sicherheitsplattform ist hoch skalierbar und kann auch in großen Unternehmensnetzen eingesetzt werden.

Als typische Herstellerbeispiele im Bereich EDR und XDR lassen sich nennen: CrowdStrike mit Falcon Insight/XDR, Microsoft mit Microsoft Defender for Endpoint und Microsoft Defender XDR, Wazuh sowie Palo Alto Networks mit Cortex XDR/XSIAM.

SIEM- und SOAR-Systeme

SIEM-Systeme hingegen sammeln die Daten von Netzwerk- und Sicherheitskomponenten, um diese zu analysieren und in einem übersichtlichen Dashboard zu präsentieren. Individuelle Informationen werden dabei aus Datenströmen extrahiert, korreliert und bewertet. Die ganzheitliche Sicht auf sicherheitsrelevante Vorfälle bietet IT-Sicherheitsverantwortlichen den Vorteil Muster zu erkennen und Schäden von der IT-Infrastruktur abwenden zu können. Das SIEM-System sammelt alle technischen Protokolle (Log-Dateien) sicherheitsrelevanter Systeme in den unterschiedlichsten Formaten, überführen sie in eine einheit-

liche und lesbare Form (Normalisierung) und indizieren sie. So stehen konsolidierte Informationen für Suchabfragen, Mustererkennung und Korrelationsanalyse zur Verfügung.

Die Leistungsmerkmale eines SIEM-Systems lassen sich wie folgt zusammenfassen:

- Registrierung und zentrale Sammlung aller sicherheitsrelevanten Vorgänge
- Umfangreiche Suchfunktion, Mustererkennung und Korrelationsanalysen sorgen für eine ganzheitliche Sicht auf die IT-Sicherheit
- Vordefinierte Handlungsanweisungen zur schnellen und effizienten Reaktion auf typische Sicherheitsvorfälle (Playbooks)

Als typische Herstellerbeispiele im SIEM-Bereich lassen sich nennen: ArcSight, Exabeam, LogPoint, LogRhythm, IBM QRadar, Wazuh, Elastic Inc. und Splunk.

SOAR-Systeme stehen hingegen für den Sammelbegriff von IT-Sicherheitslösungen, die Orchestrierung, Automatisierung und Koordination von Incident-Response-Prozessen in einer einheitlichen Plattform verbinden. Dabei wird ein Case in einer SOAR-Plattform automatisch angelegt, wenn ein Alarm von beispielsweise einem SIEM-System erzeugt wird. Anschließend wird ein Kontext zum Vorfall hergestellt und über Threat Intelligence APIs (zum Beispiel MISP, VirusTotal, OpenCTI) ein Anreichern der Informationen (Enrichment) vorgenommen. Das Analyse-Playbook entscheidet dann, ob beispielsweise der Hash als Malware bekannt ist und ob der Vorfall als kritisch eingestuft werden muss. Anschließend kommt es bei einem positiven Befund zu automatisierten Aktionen, die das betroffene Endgerät in die Quarantäne schieben, die IP-/Domain-Adresse blockieren, das Netzwerk isolieren und das SOC-Team benachrichtigen können. Jeder Schritt wird in einem Case-Log festgehalten, der auch einen exakten Zeitstempel enthält und ausführliche Ergebnisdaten. Abschließend wird ein Abschlussbericht erzeugt und die vorhandenen Playbooks entsprechend angepasst.

Im Gegensatz zu einem SIEM-System, welches oftmals ähnliche Aufgaben wahrnimmt, werden bei einem SOAR die Routineaufgaben automatisiert, wodurch die Fachkräfte entlastet werden und sich auf die komplexeren Aufgabenstellungen konzentrieren können. Vollständige, nachvollziehbare Protokolle erleichtern die Compliance-Prüfungen und das Auditieren nach DSGVO oder ISO 27001. Typische Hersteller im SOAR-Umfeld sind: Palo Alto Networks mit Cortex XSOAR / XSIAM, Splunk mit Splunk SOAR, IBM mit QRadar SOAR, Microsoft mit Microsoft Sentinel, Google mit Google Chronicle SOAR / Google SecOps und Rapid7 mit InsightConnect.

Typische Auswahlkriterien bei SOAR-Systemen sind:

- Integrationen zu SIEM-/EDR-/Cloud-Diensten
- Playbook-Automatisierung
- Low-Code-/No-Code-Workflows
- Case-Management
- KI-gestützte Analyse und Incident Response
- Cloud- versus On-Prem-Betrieb
- MSSP-/Mandantenfähigkeit

Fazit

Es gibt sehr unterschiedliche Sicherheitssysteme am Markt, die das Sammeln von Informationen und Ereignissen ermöglichen, um Bedrohungen zu erkennen und dadurch auf Schwachstellen reagieren zu können. Hier wurden daher EDR, XDR, SIEM und SOAR exemplarisch dargestellt. Der Markt verschiebt sich dabei aktuell stark in Richtung integrierter Plattformen, das heißt SIEM, XDR und SOAR werden in einem Produkt angeboten. Die bekanntesten Hersteller zeigt dabei die Tabelle 1. Neuere Anbieter (zum Beispiel Torq, D3 Security, 7AI, Radiant Security) setzen verstärkt auf KI-gestützte Automatisierung und KI-basierte SOC-Ansätze. Es wird daher immer schwieriger zwischen den Systemen eine klare Trennung vorzunehmen. Einsetzen lassen sich aber alle mit gutem Gewissen.

Hersteller	Produkt	Stärken	Schwächen	Zielgruppe
Palo Alto Networks	Cortex XSOAR / XSIAM	Automatisierung, große Integrationsbibliothek, gutes Incident-Handling, enge Verzahnung mit XDR	Komplex, hoher Betriebsaufwand, kostspielig	Große Unternehmen, SOCs
Splunk	Splunk SOAR	Sehr flexibel, gute SIEM-Integration, komplexe Workflows möglich	Hohe Lizenzkosten, benötigt erfahrende Analysten	Großunternehmen mit Splunk-Landschaft
Microsoft	Microsoft Sentinel	Gute Cloud-Integration, unterstützt M365/Azure, gutes Preis-/Leistungsverhältnis	Weniger flexibel außerhalb des Microsoft-Ökosystems	Mittelstand bis Großunternehmen
IBM	QRadar SOAR	Gute Incident-Response-Prozesse, unterstützt Compliance	User-Interface gilt als schwerfällig	Regulierte Branchen
Rapid7	InsightConnect	Einfacher Einstieg, gute Automatisierung	Weniger tief als Enterprise-SOARs	Mittelstand
CrowdStrike	Fusion SOAR	Mit EDR/XDR gekoppelt, KI-gestützte Reaktion	Stark an CrowdStrike-Stack gebunden	Unternehmen mit Falcon-DER
Google	Google SecOps / Chronicle SOAR	Sehr skalierbar, gute Telemetrie, Cloud-native Architektur	Wenig verbreitet	Cloud-First-Unternehmen

Der Markt verschiebt sich aktuell stark in Richtung integrierter Plattformen, das heißt SIEM, XDR und SOAR werden in einem Produkt angeboten. Die Tabelle zeigt eine Auswahl bekannter SOAR-Hersteller im Vergleich