Separate SIEM/EDR-Architektur vs. integrierte SIEM/XDR-Plattform

Traditionell oder integriert

Moderne Security Operations Center stehen vor der Wahl zwischen getrennten SIEM/EDR-Architekturen und integrierten SIEM/XDR-Plattformen. Während integrierte Lösungen eine schnellere und effizientere Erkennung sowie Reaktion auf Cyberbedrohungen ermöglichen, bieten klassische Ansätze mehr Flexibilität und Datenhoheit – insbesondere bei komplexen Compliance-Anforderungen und Multi-Vendor-Umgebungen.

In modernen Security Operations Centern (SOC) spielt die korrekte Konsolidierung von Datenquellen bei der Erkennung von Cybergefahren eine zentrale Rolle. Unternehmen setzen häufig sowohl Endpunkt-Sicherheitslösungen (EDR/XDR) als auch zentrale Log- und Ereignis-Managementsysteme (SIEM) ein beziehungsweise stehen vor der Entscheidung, solche Lösungen im Eigenbetrieb oder als Managed Service zu implementieren – im letzteren Fall häufig in Verbindung mit einem Managed SOC.

Anfangs wurde dabei EDR/XDR nur als eine weitere Informationsquelle für ein zentrales SIEM gesehen. Mit dem Aufkommen von modernen integrierten Lösungen lautet die strategische Fragestellung in diesem Zusammenhang: Soll das SIEM die von der EDR-Lösung generierten Alarmmeldungen lediglich empfangen und korrelieren, oder ist eine integrierte Plattform der bessere Ansatz, bei dem SIEM und XDR-native Komponenten auf derselben Basis arbeiten?

Die Antwort hängt von den betrieblichen Zielen, der Skalierung und gegebenenfalls den Compliance-Vorgaben ab.

Nachfolgend werden die Vorteile integrierter SIEM/XDR-Plattformen im Detail beschrieben, aber auch die Grenzen dieses Ansatzes betrachtet.

Architektur und Datenfluss. Bei klassischen, getrennten SIEM/EDR-Architekturen sammelt das EDR (Detection Domain 1) die Endpunkttelemetrie (Prozessinformationen, Dateiaktivitäten, Netzwerkverbindungen, Registry-Änderungen) und leitet ausgewählte Ereignisse über APIs oder Syslog-Konnektoren an das zentrale SIEM (Detection Domain 2) weiter. Das SIEM aggregiert diese Daten zusammen mit Logs aus Firewalls, Cloud-Diensten und Identitätsmanagement-Systemen und versucht, Korrelationsregeln in Suchabfragen – so genannte Use Cases – abzubilden.

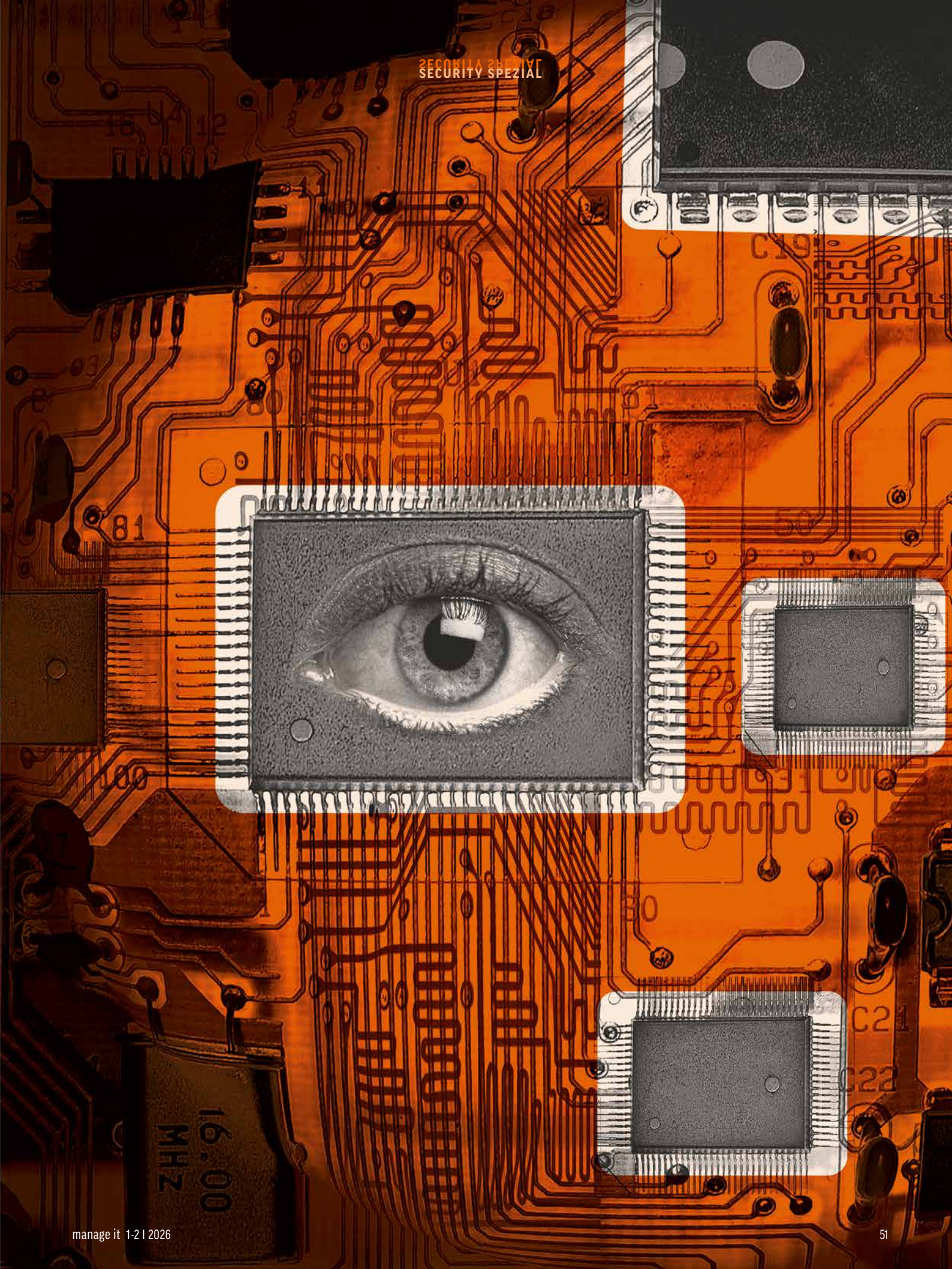
Dieses Vorgehen hat sich in der Praxis durchaus bewährt, erfordert jedoch umfangreiche Anpassungen: Event-Typen müssen gemappt, Feldnamen normalisiert und Formate transformiert werden. Dadurch entsteht erheblicher Integrationsaufwand, und wertvolle Kontextinformationen gehen häufig verloren. Zusätzlich verlangen die Use Cases nach kontinuierlicher Pflege, um auch neue oder nur leicht veränderte Angriffsmuster sicher erkennen zu können.

Integrierte SIEM/XDR-Plattformen hingegen nutzen ein einheitliches Datenmodell. Alle Ereignisse, unabhängig von Quelle oder Sensor, werden mit identischen Zeitstempeln und Metadaten erfasst. Dadurch stehen sie für Analysen und Response in Echtzeit zur Verfügung, ohne dass Daten über Konnektoren oder Schnittstellen bewegt werden müssen. In vielen Fällen kann sogar auf ein vollumfängliches SIEM-System verzichtet werden, da einige moderne XDR-Plattformen bereits grundlegende SIEM-Funktionalitäten bereitstellen, die die oben genannten Anforderungen an ein einheitliches Datenmodell erfüllen, und somit ebenfalls als integrierte Plattform angesehen werden können.

Vorteile integrierter SIEM/XDR-Plattformen.

1. **Einheitliches Datenmodell und präzise Korrelation**
   Die native Verbindung ermöglicht eine konsistente Sicht auf alle sicherheitsrelevanten Ereignisse. Endpoint-, Netzwerk-, Identitäts- und Cloud-Logs teilen denselben Kontext. Das verbessert die Erkennungsqualität deutlich, weil komplexe Angriffsketten (zum Beispiel Lateral Movement, Privilege Escalation) schneller, früher und sicherer erkannt werden können.

2. **Schnellere Detektion und Reaktion**
   Bei getrennten Systemen vergehen oft Sekunden oder Minuten, bis ein EDR-Alarm im SIEM erscheint – bei großen Datenmengen sogar länger. In einer integrierten Umgebung kann die Reaktion unmittelbar erfolgen: Ein Analyst kann



> Trotz der Vorteile ist eine integrierte SIEM/XDR-Lösung nicht unbedingt für jedes Umfeld optimal. Wer verschiedene Anbieter kombinieren oder Spezial-Tools nutzen möchte, bleibt mit einer offenen, SIEM-zentrierten Architektur flexibler.

den betroffenen Host isolieren oder Prozesse beenden, ohne zwischen Tools zu wechseln. Die »Mean Time to Respond« (MTTR) sinkt erheblich. Viele moderne integrierte Plattformen beinhalten darüber hinaus bereits automatisierte Playbooks. Aktionen wie Quarantäne, Ticket-Erstellung oder Threat-Intel-Abgleich lassen sich direkt aus der Oberfläche heraus durchführen. Diese native Automatisierung und Orchestrierung (SOAR) spart Zeit und senkt den manuellen Einsatz bei Routinevorgängen.

3. **Einheitliche Benutzererfahrung und effiziente SOC-Abläufe**
   Integrierte Plattformen bieten ein gemeinsames Dashboard, Case-Management und Alert-Priorisierung. Analysten müssen nicht mehr zwischen verschiedenen Oberflächen wechseln. Das fördert die Effizienz, reduziert Schulungsaufwand und senkt Fehlerquoten.

4. **Optimierte Threat Intelligence und zentrale Sichtbarkeit**
   Indicators of Compromise (IoCs) und Verhaltenserkennungen können über alle Datenströme hinweg angewendet werden. Manuelle Updates oder Formatkonvertierungen entfallen. Dadurch entsteht ein konsistenter Lageüberblick, der nicht durch Schnittstellenbrüche eingeschränkt wird.

5. **Vereinfachter Betrieb und Skalierung**
   Die Plattform nutzt ein abgestimmtes Speicher- und Lizenzmodell. Doppeltes Datenmanagement oder separate Datenhaltung sind nicht erforderlich. Besonders Cloud-native Lösungen skalieren dynamisch mit Datenvolumen und Nutzerzahl.

Grenzen integrierter Lösungen. Trotz der Vorteile ist eine integrierte SIEM/XDR-Lösung nicht unbedingt für jedes Umfeld optimal. Wer verschiedene Anbieter kombinieren oder Spezial-Tools nutzen möchte, bleibt mit einer offenen, SIEM-zentrierten Architektur flexibler. Eine SIEM-zentrierte Architektur bietet zudem den Vorteil, dass sich branchenspezifische Use Cases abdecken lassen und gesetzliche Anforderungen bei regulierten Unternehmen erfüllt werden können, für die XDR-Lösungen keine Erkennungslogiken bereitstellen.

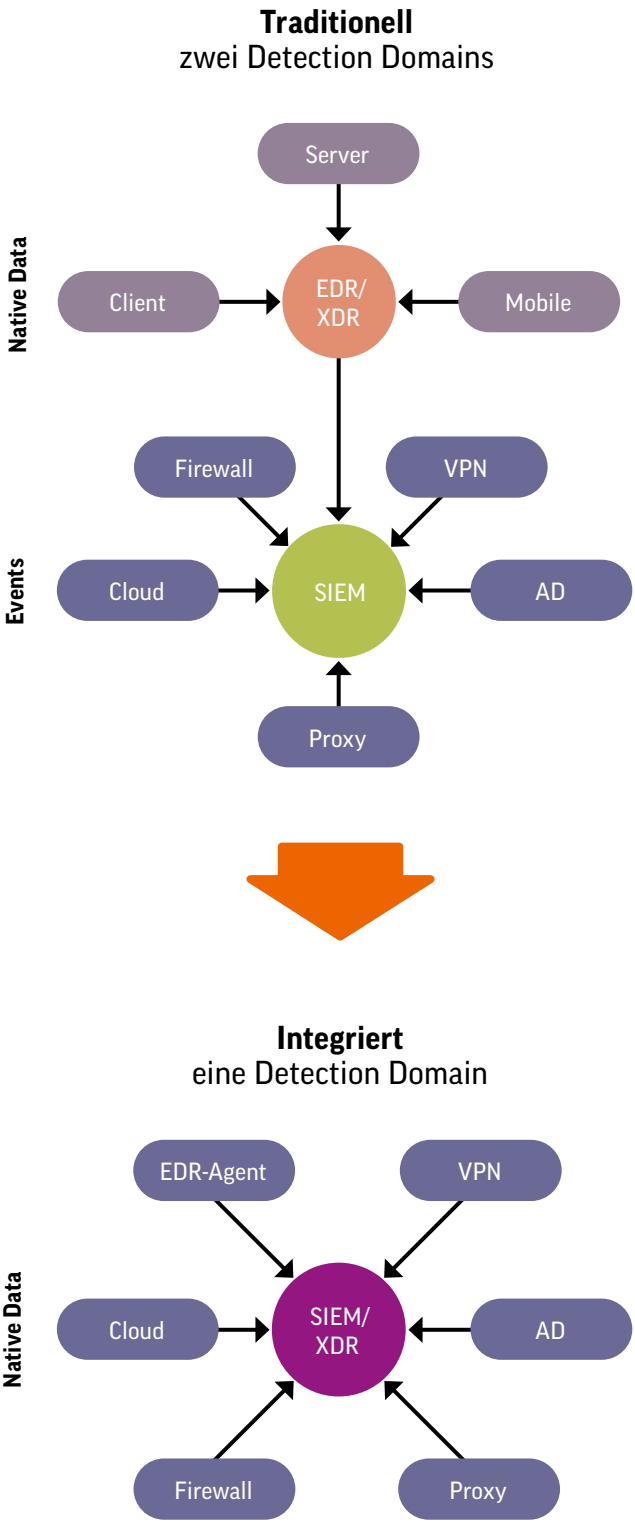


Abbildung: Klassische SIEM/EDR-Architekturen erfordern umfangreiche Anpassungen und führen oft zu Integrationsaufwand sowie dem Verlust von Kontextinformationen. Integrierte SIEM/XDR-Plattformen hingegen ermöglichen eine Echtzeit-Analyse aller Ereignisse durch ein einheitliches Datenmodell und vereinfachen so die Sicherheitsprozesse.

Controlware – Managed Detection & Response made in Germany

Die Controlware GmbH gehört zu den führenden Cyber-Defense-Anbietern in Deutschland und bietet Managed Detection & Response Services auf Basis moderner integrierter SIEM- und XDR-Plattformen an. Das international renommierte Marktforschungsinstitut ISG zeichnete Controlware im Rahmen der aktuellen Studie »ISG Provider Lens: Cybersecurity – Services and Solutions 2025« als »Leader« aus und würdigte die Managed Security Services bereits zum fünften Mal in Folge in den Kategorien »Technical Security Services«, »Next-Gen SOC/MDR Services« sowie »Next-Gen SOC/MDR Services (Midmarket)«.

Eine integrierte Plattform führt zwangsläufig zu engerer Herstellerbindung (Vendor Lock in) und kann einzelne Funktionen ausschließen, wenn sie außerhalb des Eco-Systems der Lösung liegen. Aber auch die Wahl einer SIEM-Plattform führt zu einer Herstellerbindung, da der Wechsel einer solchen Plattform keinesfalls einfach umzusetzen ist.

Bei integrierten Plattformen handelt es sich heute praktisch immer um Cloud-basierte Lösungen, die eine lokale Datenhaltung und Logdaten-Speicherung nicht oder nur eingeschränkt erlauben, wodurch sich Einschränkungen in Bezug auf die Datenhoheit ergeben. Bei sehr großen Datenvolumina oder hohen Anforderungen an die Langzeitspeicherung haben integrierte Plattformen zudem noch Kostennachteile im Vergleich zu speziell dafür ausgelegten und optimierten lokalen Speichersystemen, die aber wiederum hohe Einmalinvestitionen erfordern.

Fazit. Integrierte SIEM/XDR-Plattformen verbessern die operative Effizienz und Datenqualität erheblich. Sie ermöglichen schnellere Incident-Response-Prozesse, konsistente Analysen, einfache Automatisierung und vereinfachten Betrieb.

Die Weiterleitung von EDR-Alarmen an ein zentrales SIEM bleibt dann attraktiv, wenn Multi-Vendor-Integrationen, Compliance-Reporting, volle Datenhoheit oder individuelle Analysen im Vordergrund stehen.

Christian Bohr,
Head of Managed Services Consulting,
Controlware GmbH

www.controlware.de
blog.controlware.de