Managed Detection & Response (MDR) und Vulnerability Management Services (VMS)

Ein unverzichtbarer Bestandteil moderner Cybersecurity

MDR und VMS gemeinsam haben einige Vorteile die klassische SIEM-Systeme nicht bieten – dazu zählen die proaktive Bedrohungserkennung und -abwehr, eine kontinuierliche und gezielte Überwachung der Schwachstellen und die Verringerung der Angriffsfläche. MDR und VMS verbessern das Schutzniveau eines Unternehmens bei gleichzeitiger Reduzierung des Aufwands.

Durch die steigende Zahl und Komplexität von Cyberangriffen müssen Unternehmen ihre Cybersecurity-Strategie grundlegend überdenken. Dabei reicht es nicht mehr, nur auf klassische Sicherheitslösungen zu setzen, da diese zwar vor bekannten Bedrohungen schützen, aber oftmals Schwierigkeiten haben, auf neue, komplexe Angriffe zu reagieren.

Aus diesem Grund gewinnen moderne Ansätze wie Managed Detection & Response (MDR) und Vulnerability Management Services (VMS) zunehmen an Bedeutung, um sich effektiv und gleichzeitig effizient vor Cybergefahren zu schützen. In diesem Artikel wird der klassische Logdaten-basierte Ansatz in Frage gestellt, der häufig die technische Basis von SIEM-Plattformen darstellt. Zudem werden die Vorteile von MDR aufgezeigt und erläutert wie VMS ergänzend zu einer umfassenden Sicherheitsstrategie beiträgt.

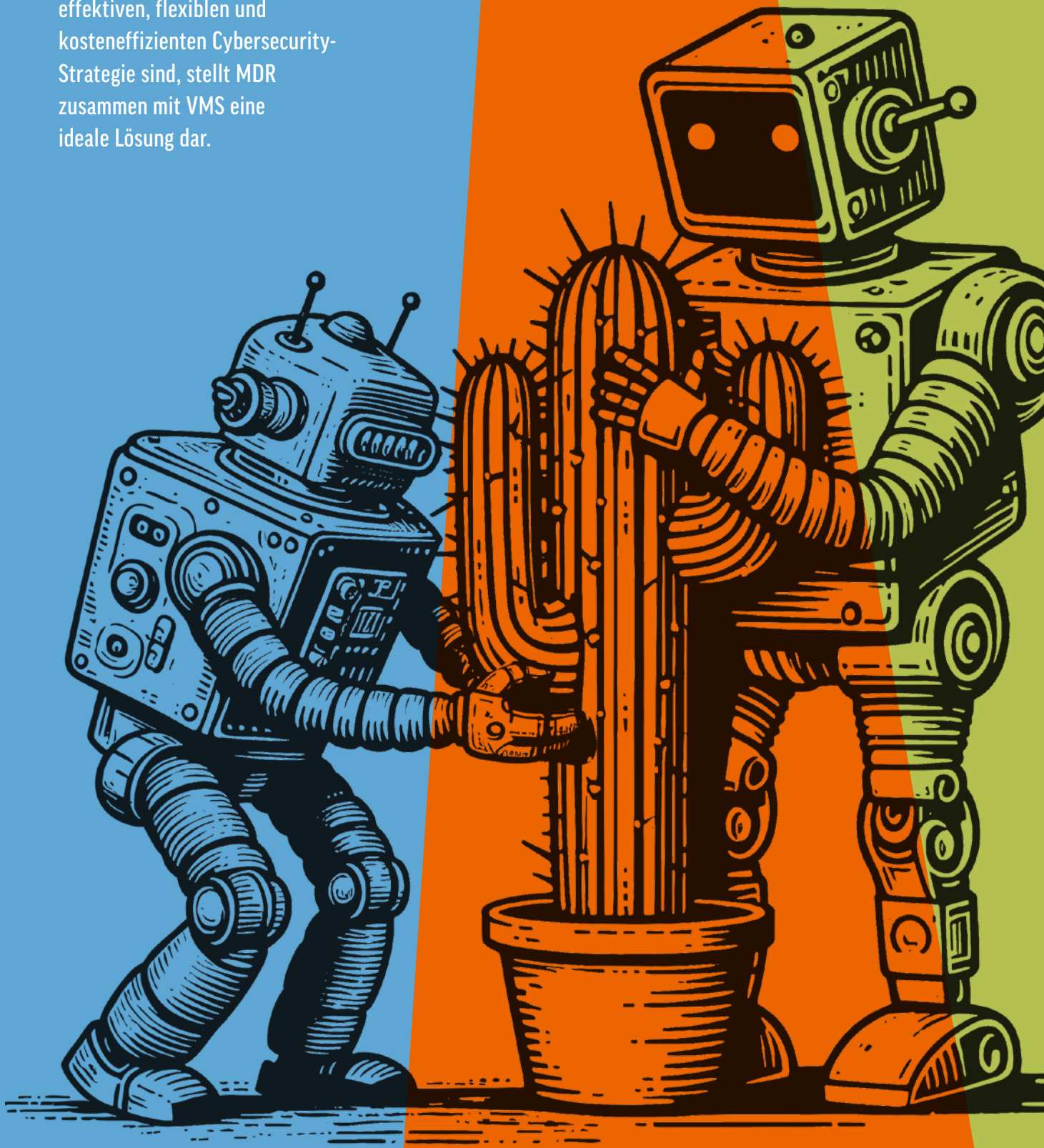
Klassische Security-Information-and-Event-Management-Systeme (SIEM) stoßen bei der Erkennung und Reaktion auf Security-Vorfälle an ihre Grenzen. SIEM-Systeme wurden entwickelt, um sicherheitsrelevante Daten aus verschiedenen Quellen zu sammeln und Use-Case-basiert bewerten und analysieren zu können. Dieser Ansatz bringt jedoch Herausforderungen mit sich, die den Nutzen einer solchen Lösung in Frage stellen:

- **Hoher Aufwand und komplexe Einrichtung:** Eine SIEM-Integration ist nicht nur zeitaufwendig, sondern setzt auch spezialisiertes Wissen voraus. Dadurch wird sowohl bei der Einführung als auch bei der Pflege ein hoher Aufwand erzeugt.
- **Reaktiver Sicherheitsansatz:** SIEM-Systeme erfassen Logdaten, werten diese aus (Ereignisanalyse) und generieren entsprechende Reports. Demzufolge kann zwar gut auf vergangene Aktivitäten reagiert werden, bietet allerdings keinen präventiven Schutz. Ebenso muss eine Reaktion auf erkannte Vorfälle manuell erfolgen, was zu Verzögerungen führt und Angreifern wertvolle Zeit verschafft.
- **Kostenintensive Datenmengen:** Die Datenmengen, die in SIEM-Systemen gespeichert werden, führen zu hohen Kosten, da Gebühren häufig Datenvolumen-basiert erhoben werden. Ein Großteil der gesammelten Daten ist jedoch nicht zwingend relevant für die Cybersecurity, so dass wertvolle Ressourcen für die Verarbeitung von Informationen eingesetzt werden, die für diesen Zweck irrelevant sind.

MDR als flexible und kosteneffiziente Alternative. MDR bietet eine modernere, flexiblere und kosteneffizientere Alternative, die Bedrohungen nicht nur frühzeitig erkennt, sondern auch aktiv darauf reagiert. MDR verbindet Plattformen für Endpoint Detection and Response (EDR) oder Extended Detection and Response (XDR) mit einem Rund-um-die-Uhr-SOC-Service.

EDR & XDR – Die Basis eines MDR-Ansatzes. EDR verfolgt einen Endpoint-zentrischen Ansatz und fokussiert sich auf den Schutz von Endgeräten wie Clients und Servern, die oft Ziele von Cyberangriffen sind. Durch Echtzeitüberwachung und automatisierte Reaktionen erkennt EDR verdächtige

*/ Für Unternehmen, die auf der Suche nach einer effektiven, flexiblen und kosteneffizienten Cybersecurity-Strategie sind, stellt MDR zusammen mit VMS eine ideale Lösung dar.



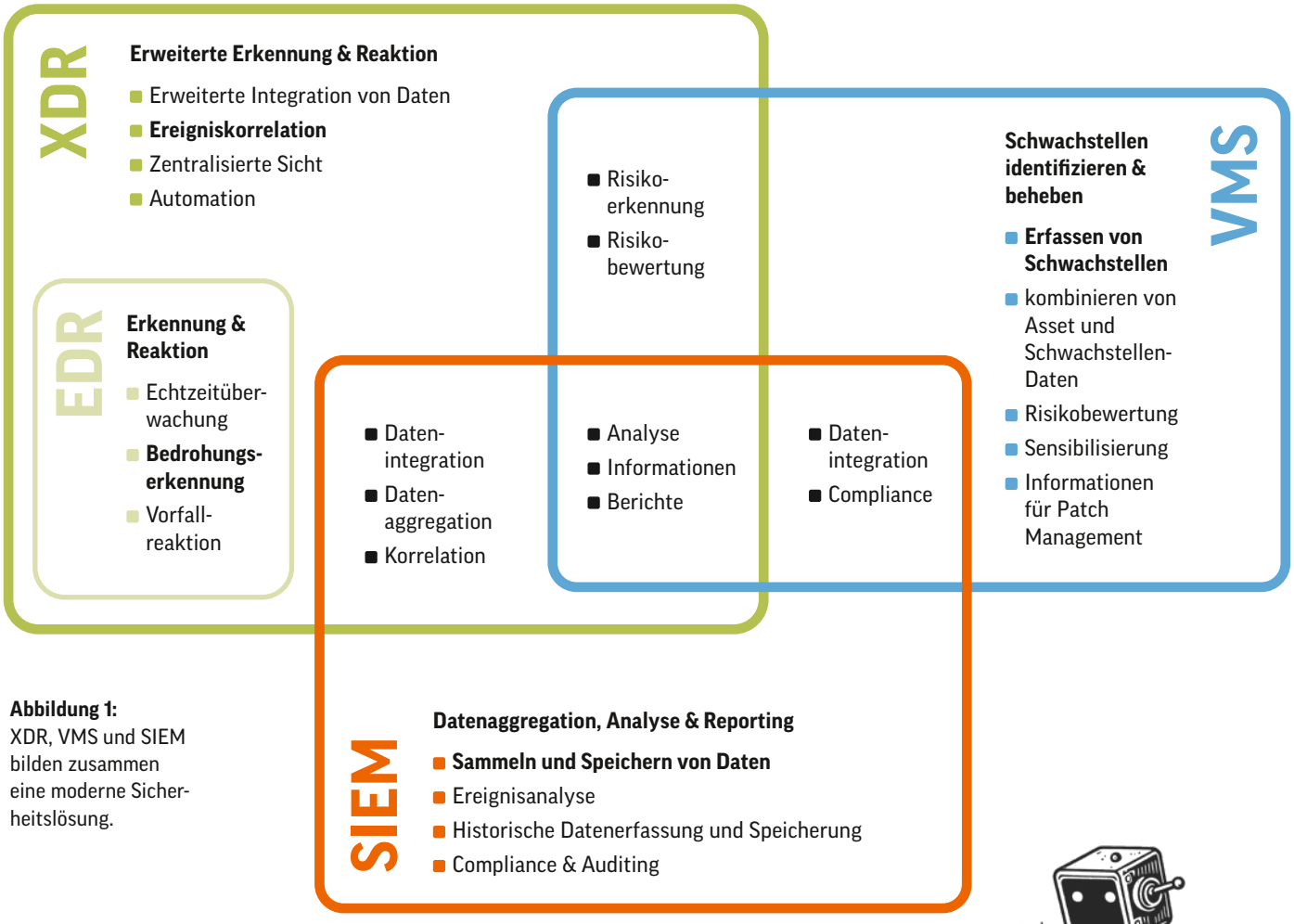


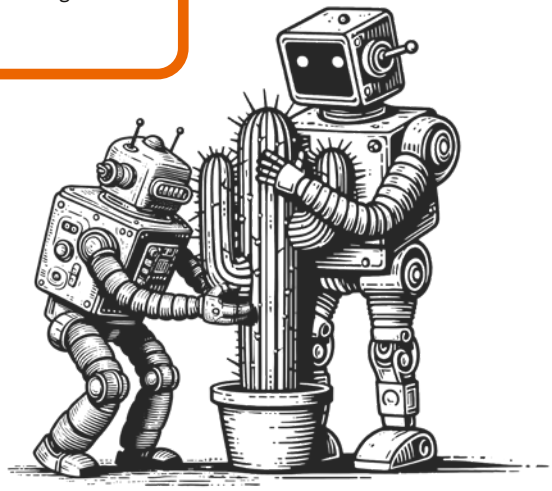
Abbildung 1:
XDR, VMS und SIEM bilden zusammen eine moderne Sicherheitslösung.

Aktivitäten frühzeitig und unterstützt dabei, Bedrohungen schnell einzudämmen. Zu den wichtigsten Funktionen gehören:

- **Echtzeitüberwachung:** Kontinuierliche Analyse von Endgeräten, um ungewöhnliche Aktivitäten und potenzielle Bedrohungen frühzeitig zu erkennen.
- **Bedrohungserkennung:** Identifikation verdächtiger Muster und Verhaltensweisen, die auf Sicherheitsrisiken oder laufende Angriffe hinweisen.
- **Vorfallreaktion:** Automatisierte Maßnahmen wie die Isolierung betroffener Geräte oder das Blockieren schädlicher Prozesse, um die Auswirkungen eines Angriffs zu minimieren.

XDR erweitert EDR, indem Daten aus weiteren Quellen wie Netzwerken, Cloud-Umgebungen und Anwendungen integriert werden. Durch diese ganzheitliche Betrachtung bietet XDR:

- **Erweiterte Integration von Daten:** XDR kombiniert Informationen aus verschiedenen Quellen, beispielsweise Endgeräte, Netzwerke und Cloud-Dienste, um ein umfassenderes Sicherheitsbild zu schaffen.



- **Ereigniskorrelation und Automation:** Durch die Verknüpfung und Analyse von Sicherheitsereignissen lassen sich komplexe und koordinierte Angriffe leichter erkennen.
- **Automation:** Automatisierte Prozesse ermöglichen schnelle und effiziente Reaktionen auf Bedrohungen, reduzieren manuelle Eingriffe und steigern die Effektivität der Abwehrmaßnahmen.

Durch die Kombination von EDR und XDR in MDR-Services erhalten Unternehmen eine leistungsstarke Lösung, die

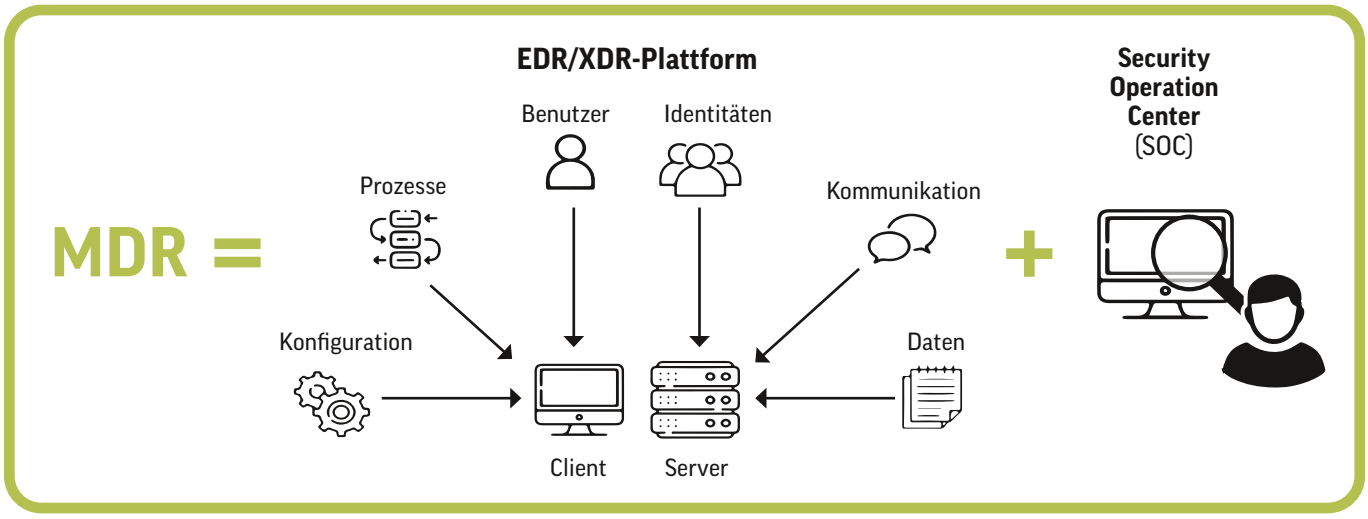


Abbildung 2: Durch die Kombination von EDR und XDR in MDR-Services erhalten Unternehmen eine leistungsstarke Lösung, die Bedrohungen frühzeitig erkennt und automatisiert reagiert – ergänzt durch Experten, die auf aktuelle Bedrohungslagen eingehen und klare Handlungsempfehlungen geben.

Bedrohungen frühzeitig erkennt und automatisiert reagiert - ergänzt durch Experten, die auf aktuelle Bedrohungslagen eingehen und klare Handlungsempfehlungen geben.

Vulnerability Management Services (VMS) – Proaktive Schwachstellenbeseitigung. VMS ist eine sinnvolle Ergänzung von MDR, indem potenzielle Schwachstellen in der IT-Infrastruktur eines Unternehmens frühzeitig identifiziert und behoben werden, bevor es zu einer Ausnutzung kommen kann. VMS beinhaltet:

- **Erfassen von Schwachstellen:** VMS führt regelmäßige Scans durch, um Sicherheitslücken in der IT-Infrastruktur zu identifizieren. Diese Scans decken häufige Schwachstellen auf, zum Beispiel unbekannte oder nicht aktuelle Systeme und Software sowie unsichere oder falsche Konfigurationen.
- **Risikobewertung:** Basierend auf den Ergebnissen der Scans wird eine Risikobewertung vorgenommen, die es Unternehmen ermöglicht, Schwachstellen nach ihrer Gefährdungslage zu priorisieren.
- **Patch Management:** VMS sorgt dafür, dass sich Schwachstellen schnell und effizient durch das Aufspielen von Sicherheits-Patches oder durch Konfigurationsanpassungen beheben lassen.

Durch die regelmäßige und proaktive Beseitigung von Schwachstellen wird das Risiko von erfolgreichen Angriffen erheblich verringert und die Angriffsfläche eines Unternehmens minimiert.

Zusammenfassung – MDR und VMS als effektive Kombination. MDR und VMS erschließen Unternehmen eine Reihe von Vorteilen, die klassische SIEM-Systeme nicht bieten. Einer der größten Vorteile von MDR ist wie beschrieben die proaktive Bedrohungserkennung und -abwehr, die durch den Einsatz von EDR/XDR-Plattformen ermöglicht wird. Mit der Erweiterung des MDR-Ansatzes durch VMS lässt sich eine kontinuierliche und gezielte Überwachung der Schwachstellen gewährleisten. Unternehmen können durch diese Kombination nicht nur Angriffe entdecken und abwehren, sondern zusätzlich die Angriffsfläche verkleinern, indem sie Schwachstellen erkennen und schließen.

Für bestimmte Anwendungsfälle kann ein SIEM-System auch weiterhin eine sinnvolle Ergänzung sein, wenn es zum Beispiel als übergreifende Ebene fungiert, umfassende Reporting-Funktionen bereitstellt und die Einhaltung von Compliance-Vorgaben unterstützt.

Ohne Frage lässt sich das Schutzniveau eines Unternehmens durch MDR und VMS erheblich verbessern und der Aufwand reduzieren. Und nicht zu vergessen - die hohen Kosten von traditionellen SIEM-Systemen können eingespart werden. Für Unternehmen, die auf der Suche nach einer effektiven, flexiblen und kosteneffizienten Cybersecurity-Strategie sind, stellt MDR zusammen mit VMS eine ideale Lösung dar. Managed Service Provider wie Controlware bieten in diesem Bereich umfassende Lösungen zur Schwachstellenerkennung und Bedrohungsabwehr. Das Cyber-Defense-Portfolio von Controlware umfasst unter anderem umfangreiche Services wie MDR-Services & VMS sowie entsprechende Assessments und Security-Consulting-Leistungen.

Marius Doppler,
Senior Consultant Managed Services,
Controlware GmbH

www.controlware.de
blog.controlware.de