VECTRA
SECURITY THAT THINKS.

KURZVORSTELLUNG

# Die bestmögliche SOC-Transparenz

Das enorme Aufkommen von Cyber-Kriminalität zeigt, dass herkömmliche Sicherheitsmaßnahmen keinen effektiven Schutz mehr bieten. Bedrohungen agieren im Verborgenen und langfristig. Sie verstecken sich in verschlüsseltem Traffic oder in Tunneln. Da Angreifer immer raffinierter vorgehen, benötigen Security-Teams einen schnellen Überblick über die Bedrohungen in ihren Umgebungen.

Im Gartner-Untersuchungsbericht „*Applying Network-Centric Approaches for Threat Detection and Response*“ (Anwenden netzwerkorientierter Ansätze für Bedrohungserkennung und Response), der am 18. März 2019 (ID: G00373460) von Augusto Barros, Anton Chuvakin und Anna Belak veröffentlicht wurde, wurde des Konzept der SOC-Transparenz-Triade (SOC Visibility Triad) vorgestellt.

In diesem Bericht macht Gartner klar:

„Die zunehmende Raffinesse der Bedrohungen zwingt Unternehmen dazu, für Bedrohungserkennung und Response mehrere Datenquellen zu verwenden. Mit netzwerkbasierten Technologien können Technikexperten schnell – und ohne Agenten einsetzen zu müssen – einen Überblick über die Bedrohungen in der gesamten Umgebung erhalten.“[1]

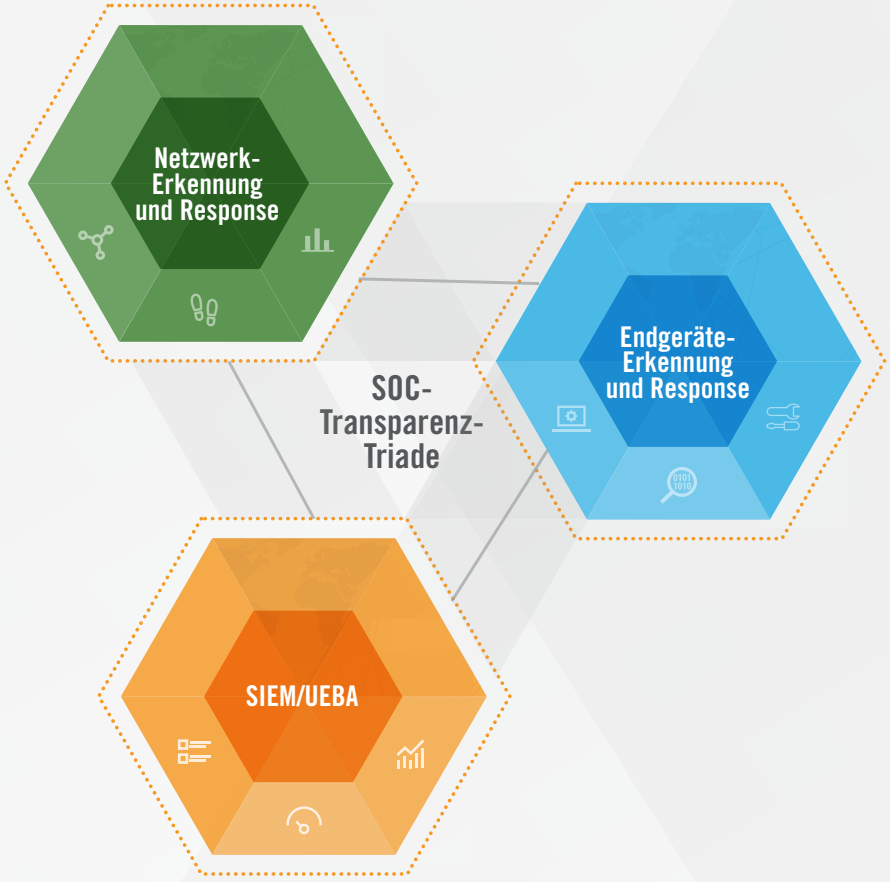


Abbildung 1. SOC-Transparenz-Triade

Quelle: Gartner: „Applying Network-Centric Approaches for Threat Detection and Response“, Augusto Barros et al., 18. März 2019, ID G00373460

Die Untersuchung kommt zu folgendem Ergebnis: „Moderne Security Operations-Tools sind mit der ‚Atom-Triade' (einem Konzept aus dem kalten Krieg) vergleichbar, die aus strategischen Bombern, Interkontinentalraketen und U-Boot-gestützten ballistischen Raketen bestand. Wie Abbildung 1 zeigt, verfügt ein modernes SOC über eine eigene Transparenz-Triade aus folgenden Komponenten:

1. **SIEM/UEBA** ermöglicht die Erkennung und Analyse von Protokollen, die von der IT-Infrastruktur sowie von Anwendungen und anderen Sicherheitstools generiert wurden.

2. **Endgeräte-Erkennung und Response** ermöglicht die Erfassung von Dateiausführungen, lokalen Verbindungen, Systemänderungen, Arbeitsspeicheraktivitäten und anderen Prozessen auf Endgeräten.

3. **Netzwerkbasierte Erkennung und Response (NTA, NFT und IDPS)** wird von Tools bereitgestellt, die den Netzwerk-Traffic erfassen bzw. analysieren."[2]

Durch diesen dreiteiligen Ansatz erhalten SOCs einen besseren Überblick über Bedrohungen sowie mehr Möglichkeiten für Erkennung, Response, Untersuchung und Behebung.

## Netzwerk-Erkennung und Response von Vectra

Netzwerk-Metadaten sind die aussagekräftigste Quelle zum Aufspüren von Bedrohungen. Der tatsächliche Traffic enthüllt zuverlässig und unabhängig verborgene Bedrohungen. Detailarme Quellen wie Protokollanalysen zeigen nur, was bereits erfasst wurde. Sie erkennen jedoch nicht die grundlegenden Verhaltensweisen von Angreifern beim Spionieren, Ausbreiten und Diebstahl.

Mit einer NDR-Lösung lassen sich verdächtige Aktivitäten in Unternehmensnetzwerken aufdecken, indem wichtige Netzwerk-Metadaten erfasst, gespeichert und mit maschinellem Lernen und hochentwickelten Analysen kombiniert werden.

Die Lösung erstellt Modelle des normalen Benutzerverhaltens und reichert diese Modelle mit Echtzeit- und historischen Metadaten an.

NDR erfasst die Interaktionen zwischen allen Geräten im Netzwerk in einer Übersicht. Laufende Angriffe werden erkannt, priorisiert und mit den kompromittierten Host-Geräten korreliert.

NDR liefert einen unternehmensweiten Rundumblick – von Public Cloud und Workloads in privaten Rechenzentren bis zu Benutzern und IoT-Geräten (Internet of Things).

## Endgeräte-Erkennung und Response

Endgeräte werden recht häufig durch Malware, nicht gepatchte Schwachstellen oder unaufmerksame Anwender kompromittiert. Mobilgeräte können ganz einfach in öffentlichen Netzwerken kompromittiert werden und verbreiten die Infektion weiter, sobald sie sich erneut mit dem Unternehmensnetzwerk verbinden. IoT-Geräte sind berüchtigt für ihre Sicherheitslücken.

Eine EDR-Lösung bietet umfassendere Funktionen als herkömmlicher Virenschutz, beispielsweise die Überwachung auf böswillige Aktivitäten auf Endgeräten und Host-Geräten. Mit EDR erhalten Sie einen detaillierten Echtzeit-Überblick über die Prozesse auf dem Host oder Gerät sowie die Interaktionen zwischen diesen Prozessen.

EDR erfasst Ausführungen, Speicheraktivitäten sowie Veränderungen und Aktivitäten auf Systemebene. Dank dieser Transparenz können Security-Analysten Muster, Verhaltensweisen, Kompromittierungsindikatoren und andere verborgene Hinweise erkennen. Diese Daten können mit anderen Sicherheitsdaten-Feeds abgeglichen werden, um Bedrohungen zu identifizieren, die nur innerhalb des Hosts sichtbar sind.

## SIEM für Großunternehmen

Seit Jahrzehnten nutzen Security-Teams die SIEM-Systeme als Dashboard für sicherheitsbezogene Aktivitäten in der gesamten IT-Umgebung. Diese SIEM-Lösungen erfassen Ereignisprotokolldaten anderer Systeme und ermöglichen Datenanalysen, Ereigniskorrelation, Aggregation und Reporting.

Durch die Integration von Bedrohungserkennungen aus EDR und NDR können Security-Analysten mit dem SIEM-System Angriffe noch schneller stoppen. Bei einem Zwischenfall können Analysten die betroffenen Host-Geräte schnell identifizieren. Das vereinfacht die Untersuchung eines Angriffs und die Feststellung, ob er erfolgreich war.

Ein SIEM-System kann auch mit anderen Netzwerksicherheitskontrollen wie Firewalls oder NAC-Enforcement-Points kommunizieren, damit böswillige Aktivitäten blockiert werden. SIEM-Systeme können jedoch auch mithilfe von Threat-Intelligence-Feeds proaktiv Angriffe verhindern.

## Ein integrierter Ansatz zum Aufdecken und Abwehren von Cyber-Angriffen

Security-Teams, die auf die Triade aus NDR, EDR und SIEM setzen, können bei der Reaktion auf Zwischenfälle oder der Suche nach Bedrohungen noch mehr Fragen beantworten, zum Beispiel:

- Hat sich ein anderes Asset auffällig verhalten, nachdem es mit dem potenziell kompromittierten Asset kommuniziert hat?
- Welcher Service und welches Protokoll wurden verwendet?
- Welche anderen Assets oder Konten sind möglicherweise betroffen?
- Hat ein anderes Asset dieselbe externe Command & Control-IP-Adresse kontaktiert?
- Wurde das Nutzerkonto auf anderen Geräten auf ungewöhnliche Weise verwendet?

Dadurch sind schnelle und koordinierte Reaktionen für alle Ressourcen möglich. Das steigert die Effizienz der Sicherheitsabläufe und verkürzt die Verweildauer, sodass das Risiko für das Unternehmen insgesamt sinkt.

Schätzungen des Weltwirtschaftsforums zufolge werden die wirtschaftlichen Schäden durch Cyber-Kriminalität bis 2020 auf 3 Billionen US-Dollar steigen. Staatliche Angreifer und Kriminelle nutzen die Vorteile der grenzenlosen digitalen Welt zu ihrem Vorteil aus. Doch dank der Transparenz-Triade kann ein Unternehmens-SOC seine sensiblen Daten und wichtigen Prozesse zuverlässig schützen.

**Weitere Informationen erhalten Sie von unseren Servicemitarbeitern unter sales-inquiries@vectra.ai.**

E-Mail: info_dach@vectra.ai  vectra.ai/de