Microsoft und Vectra vervollständigen die Vision der SOC-Transparenz-Triade

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]

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 auf der rechten Seite 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 (weitere Details siehe ‚SIEM-Technologie-Analyse‘).
2. **Endgeräte-Erkennung und Response** ermöglicht die Erfassung von Dateiausführungen, lokalen Verbindungen, Systemänderungen, Arbeitsspeicheraktivitäten und anderen Prozessen auf Endgeräten (weitere Details siehe ‚Architektur und Einsatz von Endgeräte-Erkennung und Response‘).
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.

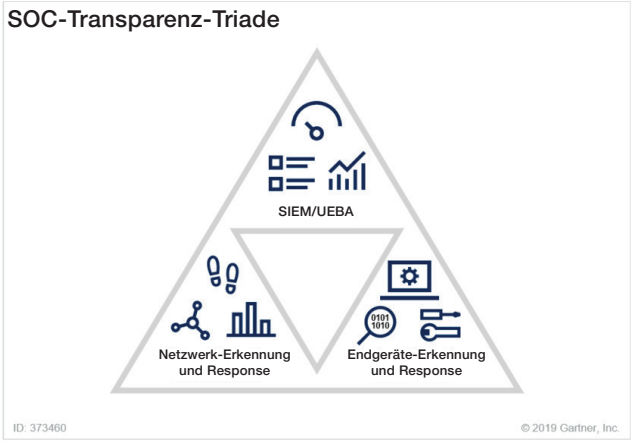

Abbildung 1. SOC-Transparenz-Triade

Quelle: Gartner: „Applying Network-Centric Approaches for Threat Detection and Response“ (Anwenden netzwerkorientierter Ansätze für Bedrohungserkennung und Response), Augusto Barros et al., 18. März 2019, ID G0037346

Microsoft Defender Advanced Threat Protection

Endgeräte werden recht häufig durch Malware, nicht gepatchte Schwachstellen, Konfigurationsfehler 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.

Microsoft Defender Advanced Threat Protection (ATP) ist eine einheitliche Plattform für Endgerätesicherheit, die präventiven Schutz bietet, erfolgreiche Kompromittierungen erkennt sowie Untersuchungen und Response automatisiert.

Der verhaltensbasierte Cloud-gestützte Bedrohungs- und Malware-Schutz von Microsoft Defender ATP verhindert, dass raffinierte und neuartige Bedrohungen Geräte infizieren können. Die Software bietet umfassende Einblicke in das Betriebssystem (einschließlich Arbeitsspeicher und Kernel) und erkennt Zero-Day-Attacken, hochentwickelte Angriffe und Datenkompromittierungen.

---

1 Quelle: Gartner: „Applying Network-Centric Approaches for Threat Detection and Response“ (Anwenden netzwerkorientierter Ansätze für Bedrohungserkennung und Response), Augusto Barros et al., 18. März 2019, ID G00373460
2 Ebenda.

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.

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.

Die Vectra-Plattform erfasst die Interaktionen zwischen allen Geräten im Netzwerk in einer Übersicht. Die Verhaltensmodelle der Vectra-KI basieren auf Sicherheitsforschung sowie Datenwissenschaft und erkennen laufende Angriffe, die sie priorisieren und mit den kompromittierten Host-Geräten korrelieren. Verdächtige Aktivitäten in Unternehmensnetzwerken lassen sich aufdecken, indem wichtige Netzwerk-Metadaten erfasst, gespeichert und mit maschinellem Lernen und hochentwickelten Analysen kombiniert werden.

Dank der nativen Integration in Microsoft Defender ATP haben Security-Teams die Möglichkeit, die allgemeine Übersicht von Vectra mit der Detailanzeige von Microsoft Defender ATP zu verknüpfen. Analysten zeigen Kontext der Microsoft-Software in der Vectra-Plattform an und können Konten automatisch deaktivieren oder die Host-Isolierung von Microsoft Defender ATP direkt über die Vectra-Konsole auslösen. Die Untersuchung durch die Security-Teams lässt sich zusätzlich durch einen sofortigen Wechsel zu Microsoft Defender ATP mit lokalem Vectra-Kontext beschleunigen, der als Parameter für die Detailanalyse in Microsoft Defender ATP dient.

Microsoft Azure Sentinel

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.

Azure Sentinel verarbeitet Systemprotokolle aus Vectra Cognito und Microsoft Defender ATP. Bei einem Zwischenfall können Analysten mithilfe von vorkonfigurierten Anwendungen sowie Vectra-Dashboard-Widgets die betroffenen Host-Geräte und -Konten schnell identifizieren. Das vereinfacht die Untersuchung eines Angriffs und die Feststellung, ob er erfolgreich war.

Ein SIEM-System kann auch mit anderen Netzwerksicherheits-kontrollen 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.

Microsoft und Vectra vervollständigen die Vision der SOC-Transparenz-Triade

Security-Teams setzen die Vision der SOC-Transparenz-Triade mit nativen Integrationen zwischen der Vectra Cognito-Plattform, Microsoft Defender ATP und Azure Sentinel um. Dadurch können sie eine größere Bandbreite an 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?

Durch die nativen Integrationen dieser Lösungen erhalten Sie Kontext aus allen Datenquellen, koordinierte Durchsetzungsmaßnahmen wie Kontodeaktivierungen und Host-Isolierung sowie vorkonfigurierte SOC-Übersichts-Dashboards. Die integrierten Lösungen ermöglichen eng koordinierte Reaktionen, eine höhere Effizienz der Sicherheitsabläufe und eine geringere Verweildauer der Bedrohung. Dadurch sinkt das Risiko für Ihr Unternehmen.

VECTRA®
Security that thinks®

E-Mail: info_dach@vectra.ai **Telefon:** +1 408 326 2020 vectra.ai/de