Warum SIEM/UEBA in der modernen Arbeitswelt unverzichtbar ist

Traditionelle Security-Lösungen zielen auf den Schutz der Außengrenzen des eigenen Netzwerks, des Perimeter. Dieser ist jedoch nicht beliebig erweiterbar. Was ist beispielsweise mit all denen, die remote aus dem Homeoffice oder an häufig wechselnden Orten arbeiten? Oder auch mobil von unterwegs – im Lande oder am letzten Zipfel der Welt? Spätestens hier geht mit dem „Burgmauerprinzip" einfach gar nichts mehr. Also braucht es Technologien, die unabhängig vom Perimeter funktionieren. Eine abgestimmte Kombination aus Ereignisüberwachung/-management und Verhaltensanalysen zeigt hier hervorragende Ergebnisse.

SIEM und UEBA – das perfekte Duo für sicheres Arbeiten

Genau das leisten SIEM/UEBA. Die erste Komponente für eine solide Bewachung ist das Security Incident and Event Management (SIEM). SIEM sammelt und korreliert Daten aus Logs, Paketen und Bedrohungsmeldungen. Als Plattform liefert SIEM Einblicke darüber, welche Bedrohungen im Netzwerk lauern, wo schon Probleme aufgetreten sind, wer betroffen war, welche Ressourcen gefährdet sind und einiges mehr. SIEM hilft so Security-Analysten dabei, beim Bedrohungsmanagement und bei der Behebung von Bedrohungen die richtigen Entscheidungen zu treffen.

Auf Basis eines gelernten Normalbetriebs erkennen entsprechende Tools, wenn ungewöhnliche Aktivitäten im Datenverkehr stattfinden und machen Meldung. Wenn also beispielsweise von einem Microsoft 365-Account, der normalerweise eher moderaten Datenverkehr produziert, plötzlich zig GByte am Daten abgerufen werden, wird das SIEM dort genauer hinsehen.

Mehr Sichtbarkeit mit UEBA

Eine noch genauere Analyse liefert die zweite Komponente, die User Behavior Analytics (UBA) oder User and Entity Behavior Analytics (UEBA). Alles beginnt mit Sichtbarkeit! Aber was bedeutet das? Wer würde in ein autonomes Fahrzeug steigen, wenn klar ist, dass dieses während der Fahrt keinerlei Informationen über andere Fahrzeuge hat?

Ebenso ist es in einem Netzwerk sehr riskant, wenn das Sicherheitssystem immer nur einen einzigen Nutzer oder eine einzige Einheit gleichzeitig auf dem Radar hat. UEBA bietet diese tiefe Sichtbarkeit auf alle Nutzer in einem Netzwerk. Es erlaubt damit umfassende Einblicke in die Bedrohungssuche, Risikoeskalation und Untersuchungsprozesse.

Diese leistungsstarke Kombination rüstet Analysten mit den Erkenntnissen über Benutzer und Unternehmen aus, die sie benötigen, um Bedrohungen immer einen Schritt voraus zu sein und zeitnah und sicher auf jeden Vorfall zu reagieren.

Was bedeutet das? SIEM-Lösungen sind ähnlich wie Verkehrskameras auf den Straßen – sie geben ein großartiges Bild des typischen Straßenverkehrs und vermitteln über aufgezeichnete Videos Einblicke in Fahrgewohnheiten, das Geschehen in einem bestimmten Zeitraum – was passiert ist und wer daran beteiligt war. Für die Untersuchung eines Unfalls ist das sehr hilfreich. Aber was wäre, wenn es dazu noch korrelierte Daten gäbe, die alle Ziele, Routen und Zeiten zeigt, die jedes Auto auf der Straße in den letzten 60 Tagen gefahren ist? Außerdem noch Infos über Aussehen und technischen Zustand der Fahrzeuge, Häufigkeit und Qualität der Wartung, Fahrtüchtigkeit der Fahrer und einiges mehr? So entsteht ein vollständiges Bild, welche Autos und Fahrer in der Umgebung ein Risiko darstellen und wann und wo sie zu einer potenziellen Gefahr für die Sicherheit werden. Ein Netzwerk ist nicht anders. SIEM und UEBA liefern diese Tiefe des Benutzer- und Entitätsnetzwerkverhaltens, damit Analysten schnell und präzise auf potenzielle Bedrohungen reagieren können und immer wissen, wo sich die gefährlichen Fahrer/Benutzer befinden und was sie vorhaben.

Laut Gartner handelt es sich bei UEBA um eine spezielle Art der Sicherheitsanalytik, deren Fokus auf das Verhalten von Systemen und Menschen ausgerichtet ist, die sie nutzen. Entsprechende Tools arbeiten heute vermehrt mit Technologien wie maschinellem Lernen (ML)und Deep Learning (DL), um abnormales und riskantes Verhalten von Benutzern, Gruppen, Maschinen und anderen Entitäten in einem Unternehmensnetzwerk zu erkennen. Da sie nicht nur die vordefinierten Korrelationsregeln oder Angriffsmuster verwenden, sondern selbst logische Relationen herstellen und gleichzeitig mehrere Organisationssysteme und Datenquellen einbeziehen, können UEBA-Lösungen Sicherheitsvorfälle finden, die andere Tools nicht erkennen. Natürlich können sie auch Entwarnung geben, wo ein SIEM-System allein eine Meldung generieren würde.

RSA Netwitness Suite

Die RSA NetWitness Suite integriert die Fähigkeiten von SIEM/UEBA: Umfassende Sicht auf die Bedrohungslandschaften, Erkennen früher Bedrohungsindikatoren und automatische, beziehungsweise systematische Behebung der Bedrohung.

Umfassende Sicht auf die Bedrohungslage

Umfassende Sicht gewinnt der Security-Analyst, da NetWitness nicht nur die üblichen Log-Daten aus den Security-Controls und Betriebssystem- und Anwendungs-Logs für seine Analysen heranzieht. Vielmehr hat das System auch Zugriff auf NetFlows, was tiefe Einblicke in die Vorgänge direkt im Netzwerk erlaubt. Über Deep Paket Inspection im Datenfluss auf der Netzwerk-Session-Ebene lassen sich Vorgänge in Echtzeit erkennen.

Darüber hinaus nutzt das System auch Informationen aus den Endpoints und deren Betriebssystemen, untersucht diese nach Auffälligkeiten und meldet sie an die „NetWitness-Zentrale“. Einen weiteren Security-Block bildet die in nahezu jedem Security-Gewerk vorhandene Threat Intelligence, wo bekannte Ereignisse und Bedrohungen gesammelt werden. Das ist zwar technologisch nicht besonders anspruchsvoll, verhindert aber, dass der gleiche Fehler zweimal das Netzwerk bedroht.

Das Geheimnis hinter den umfangreichen Fähigkeiten von NetWitness ist die automatische Anreicherung von Event-Informationen aus den überwachten Systemen um die entsprechenden Metadaten. Mit dieser Fähigkeit macht das System aus unübersichtlichen Rohdaten aussagekräftige und leicht verständliche Informationen. Die NetWitness Suite unterstützt die Security-Verantwortlichen zusätzlich durch Verhaltensanalyse und maschinellem Lernen, um Indikatoren zu korrelieren. In Verbindung mit der Nutzung aller verfügbaren Metadaten ist das bislang einzigartig.

Früherkennung von Bedrohungsindikatoren

Eine noch genauere Analyse liefert die zweite Komponente, die User Behavior Analytics (UBA) oder User and Entity Behavior Analytics (UEBA). Alles beginnt mit Sichtbarkeit! Aber was bedeutet das? Wer würde in ein autonomes Fahrzeug steigen, wenn klar ist, dass dieses während der Fahrt keinerlei Informationen über andere Fahrzeuge hat?

Den Kern der Früherkennung von Bedrohungsindikatoren bildet eine Live-Engine. Diese vereint die Echtzeit-Erkennung mit einer Art UEBA und unterstützt damit die SOC-Analysten. Alles zielt darauf ab, Angriffe, deren Ziele und involvierte Entitys möglichst sofort zu erkennen, um entsprechend zeitnah auch gezielte Abwehrmaßnahmen einleiten zu können.

Die schnellsten Ergebnisse liefert natürlich die Threat-Intelligence – die vergleichsweise statischen Vergleiche lassen Bösartiges sofort aufpoppen. Parallel arbeitet hier die Regel-basierte Echtzeiterkennung, die bekannte Bedrohungen durch Korrelation über alle Datentypen findet. In der durch unsupervised Machine Learning (das heißt, das System lernt selbständig, ohne Einspeisung von Informationen durch einen Data-Scientist) getriebenen UEBA-Komponente führt das System ein automatisches Monitoring über alle Anwender und Entitäten aus, um nach Auffälligkeiten zu suchen und diese sofort zu melden. Diese Komponente wird als lernende Instanz naturgemäß immer intelligenter und präziser, je länger sie im Unternehmen im Einsatz ist.

Nicht zuletzt bietet NetWitness für die Früherkennung fortschrittliche Tools, um SOC-Analysten sehr schnell alle für ihre Arbeit relevanten Informationen übersichtlich zu präsentieren und gegebenenfalls unverzügliches Eingreifen zu erleichtern.

Auch das Business-Risiko im Blick

Das Sahnehäubchen bildet die Einfügung von Business-Kontext in die Analysedaten, über den sich das effektive Schadpotenzial für das Business in Form eines Risiko-Scores bewerten lässt. Menschliches Eingreifen lässt sich so auf Fälle beschränken, die tatsächlich relevant sind und eine echte Bedrohung für das Geschäft darstellen. Das ist eine erhebliche Entlastung für das SOC-Team (Security Operations Center), das ansonsten oft stark überlastet ist, da es Massen irrelevanter Alarme verfolgen muss. Insgesamt erfüllt die RSA NetWitness Suite damit alle Anforderungen, die Gartner für die Sichtbarkeit von Bedrohungen in einem SOC definiert hat. Hier sind neben SIEM/UEBA auch Network Detection and Response (NDR) und Endpoint Detection and Response (EDR) als unabdingbare Komponenten aufgeführt (2). NetWitness bietet alle drei Bereiche unter einer einheitlichen Nutzeroberfläche und auf Basis eines gemeinsamen Datenmodells.

Bei Fragen wenden Sie sich bitte direkt an die Security Experten

Mailadresse: bu-security@techdata.com
Telefon: 089 4700 3222