EIN WHITEPAPER ÜBER SICHERHEITSERKENNUNG

exeon
Smart Cyber Security.

Mehr Sicherheit, weniger Fehlalarme

FEBRUAR 2024

exeon
Smart Cyber Security.

INHALTSVERZEICHNIS

Abschnitt 1

Abschnitt 2

Use Cases:

exeon
Smart Cyber Security.

11 Wege, alles zu sehen und nur das zu erkennen, was wichtig ist

Warum die risikobasierte Alarmierung in Ihrem Unternehmensnetzwerk beginnt

1. **Kontinuierliche Überwachung:**
Echtzeit-Überwachung des Netzwerkverkehrs und der Endpoints, so dass die Entwicklung und das Fortbestehen von Warnungen im Laufe der Zeit verfolgen wird. Wenn die Risikostufe einer Warnung aufgrund zusätzlicher verdächtiger Aktivitäten ansteigt, kann das System die Priorität automatisch erhöhen.

2. **Kontextbezogene Informationen:**
Kontextbezogene Informationen sind für die Bewertung des Risikos eines erkannten Ereignisses von entscheidender Bedeutung. So können beispielsweise Alarme mit hohem Risiko bereits ausgelöst werden, wenn ein externer Benutzer versucht, auf einen wichtigen Server innerhalb des Unternehmens zuzugreifen.

3. **Risikobewertung:**
Den erkannten Ereignissen oder Warnungen wird eine Risikobewertung auf Grundlage verschiedener Faktoren zugewiesen, darunter der Schweregrad der erkannten Aktivität, der Kontext, in dem sie auftrat, die betroffenen Anlagen oder Systeme sowie historische Daten. Ziel ist es, den potenziellen Schaden oder die Auswirkungen des erkannten Ereignisses zu bewerten.

4. **Risikogewichtung:**
Bei der Risikoerhöhung (Risk Booster) werden verschiedene Elemente, die die Risikobewertung beeinflussen, unterschiedlich gewichtet. So können beispielsweise Aktivitäten, die kritische Vermögenswerte oder privilegierte Konten betreffen, eine höhere Risikobewertung erhalten. Ereignisse, die erheblich von etablierten Baselines oder Mustern abweichen, können ebenfalls stärker gewichtet werden.

5. **Korrelierte Alarme:**
Korrelierte Alarme spielen eine entscheidende Rolle bei der Aufdeckung von versteckten Angriffen im Hintergrund der normalen Netzwerkaktivitäten. Die verstärkte Korrelation von Alarmen reduziert die Arbeitsbelastung der Analysten erheblich, da sie sich weniger mit einzelnen Alarmen befassen müssen.

11 Wege, alles zu sehen und nur das zu erkennen, was wichtig ist

exeon
Smart Cyber Security.

6. Automatisierung:
Der strategische Einsatz von Automatisierung ist von grösster Bedeutung für die Stärkung der Netzwerkabwehr gegen potenzielle Angriffe, insbesondere in Anbetracht des beträchtlichen täglichen Kommunikationsvolumens in Netzwerken, das Angreifer potenziell ausnutzen könnten.

7. Maschinelles Lernen:
Maschinelles Lernen erkennt Muster und Anomalien im Netzwerkverkehr, die Algorithmen weisen den Alarmen Risikowerte zu, die auf Abweichungen von etablierten Mustern basieren.

8. Dynamische Anpassungen:
Da Risikobewertungen nicht statisch sind, sondern sich im Laufe der Zeit ändern, können sie angepasst werden, wenn neue Informationen verfügbar werden oder sich die Sicherheitslandschaft weiterentwickelt: Wenn ein ursprünglich risikoarmes Ereignis zu einem risikoreicheren Ereignis eskaliert, wird der Risikowert entsprechend angepasst.

9. Verhaltensbasierte Analyse:
Durch das kontinuierliche Monitoring des User Verhaltens im Netzwerkverkehr können Baselines für normale Aktivitäten erstellt werden. Wenn Abweichungen von diesen Baselinien festgestellt werden, werden Warnungen werden nach dem Ausmass der Abweichung und dem mit dem Verhalten verbundenen potenziellen Risiko kategorisiert und priorisiert. Ungewöhnliche Aktivitäten, die mit höherer Wahrscheinlichkeit auf eine Bedrohung hindeuten, werden mit höheren Risikostufen versehen.

10. Integration von Bedrohungsdatenbanken:
Die integrierten Threat Intelligence Feeds wie MITRE oder ZEEK und andere Datenbanken liefern Informationen über bekannte Bedrohungen, Angriffsvektoren und Indikatoren für eine Gefährdung. Durch den Querverweis von erkannten Netzwerkaktivitäten mit Threat Intelligence-Daten kann das NDR Warnmeldungen Risikostufen zuweisen, die auf der Verbindung mit bekannten Bedrohungen basieren.

11. Analyse des Benutzer- und Entitätsverhaltens (UEBA):
Da die UEBA im NDR bereits integriert ist, um das Verhalten von Benutzern und Entitäten (z. B. Geräten) innerhalb des Netzwerks zu analysieren, können Insider-Bedrohungen, kompromittierte Konten oder verdächtiges Benutzerverhalten leichter erkannt werden und zur Risikobewertung herangezogen werden.

Use Cases

Beispiele für risikobasierte Warnmeldungen in einem Network Detection and Response (NDR)-System

Szenario:

Ein Unternehmen verwendet eine NDR-Lösung zur Überwachung seines Netzwerkverkehrs.

Das NDR-System verfügt über verschiedene Sensoren und Analysefunktionen, um Netzwerkaktivitäten zu erkennen und zu analysieren.

Das Unternehmen weist den erkannten Ereignissen auf der Grundlage ihrer potenziellen Auswirkungen und des Kontexts, in dem sie auftreten, Risikowerte zu.

Warnung 1: Versuch der Datenexfiltration

Ereignis: Ungewöhnliche Muster der Datenübertragung von einem internen Server zu einer externen IP-Adresse.

Risikofaktoren:

- Betroffenes Asset: Ein Datenbankserver mit sensiblen Kundeninformationen.
- Umfang der Daten: Grosse Datenmengen werden übertragen.
- Tageszeit: Geschieht ausserhalb der Geschäftszeiten.

Risikowert: Mittel bis hoch

Ergebnis:

Das NDR-System erkennt den potenziellen Datenexfiltrationsversuch und vergibt eine Risikobewertung auf der Grundlage der Kombination von Faktoren.

Die Warnung wird zur Untersuchung eskaliert, da das Datenvolumen, die Art des betroffenen Objekts und der ungewöhnliche Zeitpunkt das Gesamtrisiko erhöhen.

exeon
Smart Cyber Security.

Use Cases

Beispiele für risikobasierte Warnmeldungen in einem Network Detection and Response (NDR)-System

Warnung 2: Bösartige Insider-Aktivitäte

Ereignis: Ein Mitarbeiter greift von seinem Arbeitsplatz aus auf mehrere vertraulichen Ordner und Dateien zu, die nicht in seinem normalen Aufgabenbereich liegen.

Risikofaktoren:

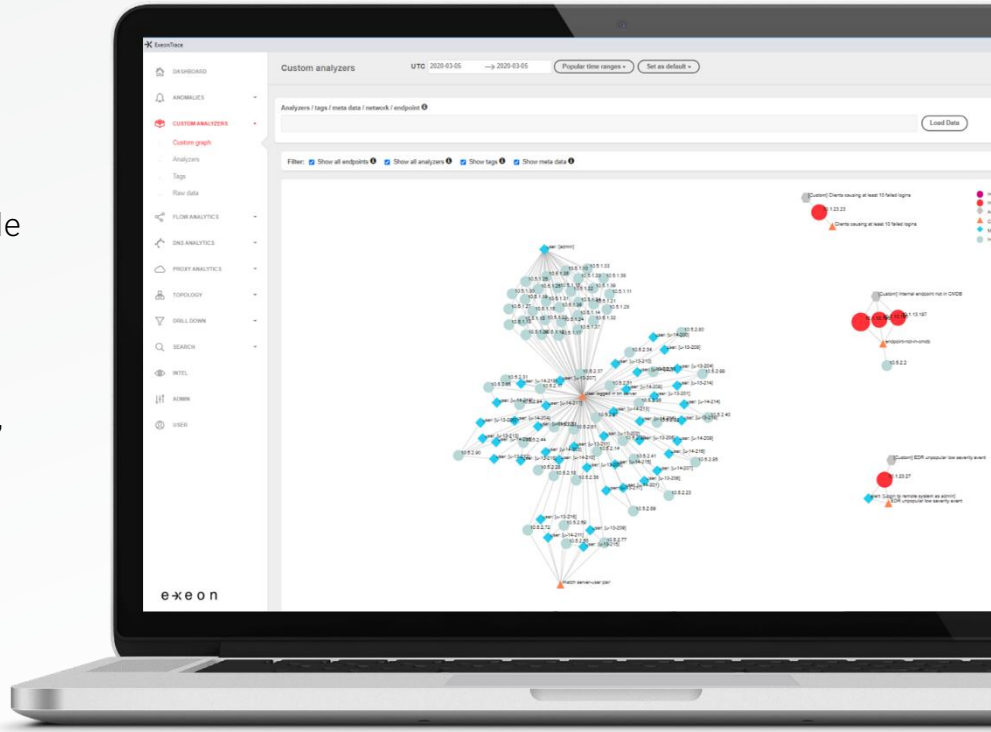
- Benutzerrolle: Der Mitarbeiter benötigt normalerweise keinen Zugriff auf diese Dateien.
- Zeitpunkt der Aktivität: Der Zugriff erfolgt ausserhalb der regulären Arbeitszeit des Mitarbeiters.
- Musterabweichung: Ungewöhnliche Aktivität im Vergleich zum bisherigen Verhalten des Mitarbeiters.

Risikowert: Hoch

Ergebnis:

Das NDR-System identifiziert das anomale Verhalten, weist ihm einen hohen Risikowert zu und löst eine sofortige Reaktion aus.

Das Unternehmen untersucht den Vorfall, um festzustellen, ob es sich um ein kompromittiertes Konto oder eine potenzielle bösartige Insider-Aktivität handelt.



exeon
Smart Cyber Security.

Use Cases

Beispiele für risikobasierte Warnmeldungen in einem Network Detection and Response (NDR)-System

Warnung 3: Reconnaissance-Aktivität

Ereignis: Mehrere fehlgeschlagene Anmeldeversuche über verschiedene Server von derselben externen IP-Adresse aus.

Risikofaktoren:

- Anzahl der Fehlversuche: Überschreitung des von der Organisation festgelegten Schwellenwerts.
- Zielserver: Versuch, auf Server mit hoher Empfindlichkeit zuzugreifen.
- Häufigkeit: Ungewöhnliche Häufigkeit der Anmeldeversuche.

Risikowert: Mittel

Ergebnis:

Das NDR-System identifiziert die Reconnaissance-Aktivität, weist ihr eine mittlere Risikobewertung zu und löst eine Untersuchung aus.

Obwohl das Risiko nicht so hoch ist wie in anderen Szenarien, deutet das Verhaltensmuster auf mögliche böswillige Absichten hin und rechtfertigt eine weitere Untersuchung.

exeon
Smart Cyber Security.

Use Cases

Beispiele für risikobasierte Warnmeldungen in einem Network Detection and Response (NDR)-System

Warnung 4: Routinemässiges Software-Update

Ereignis: Ein internes Gerät initiiert ein routinemässiges Software-Update von einer vertrauenswürdigen Quelle.

Risikofaktoren:

- Betroffenes Asset: Eine nicht kritische Benutzer-Workstation.
- Routinemässiges Verhalten: Das Software-Update stammt aus einer vertrauenswürdigen Quelle und folgt einem Standardverfahren.

Risikowert: Niedrig

Ergebnis:

Das NDR-System stuft diesen Alarm als risikoarm ein, da es sich um eine nicht kritische Anlage handelt und das Verhalten routinemässig und erwartet ist.

Dieser Alert mit geringem Risiko kann protokolliert und überwacht werden, erfordert aber keine sofortige Aufmerksamkeit.

exeon
Smart Cyber Security.

Use Cases

Beispiele für risikobasierte Warnmeldungen in einem Network Detection and Response (NDR)-System

Warnung 5: Ungewöhnliche Datenübertragung

Ereignis: Ein internes Gerät überträgt eine grosse Menge an Daten an einen externen Server.

Risikofaktoren:

- Betroffenes Asset: Ein Datenbankserver mit sensiblen Finanzdaten.
- Ungewöhnliches Verhalten: Die Datenübertragung ist deutlich grösser als bei typischen Mustern.

Risikowert: Mässig

Ergebnis:

Das NDR-System weist dieser Warnung einen mässigen Risikowert zu, da es sich um einen kritischen Vermögenswert handelt und das Verhalten ungewöhnlich ist, aber nicht unbedingt auf eine Sicherheitsverletzung hinweist.

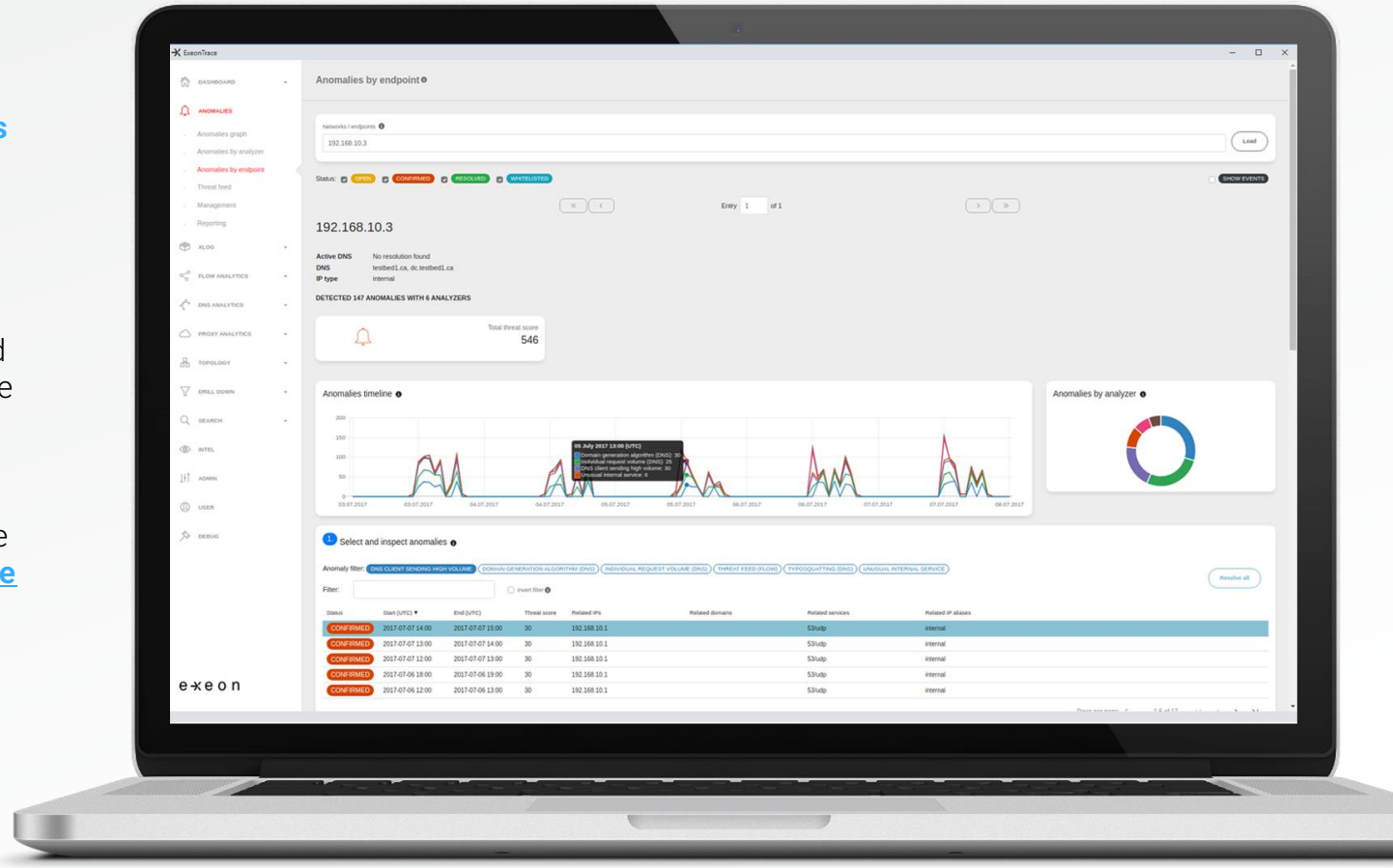
Die Sicherheitsanalysten werden benachrichtigt, um diese Warnung zeitnah zu untersuchen.

Use Cases – Fazit

Durch die Verwendung risikobasierter Warnmeldungen kann sich das Unternehmen sofort auf Warnmeldungen mit hohem Risiko, wie z.B. den unberechtigten Zugriffsversuch, konzentrieren, während Warnmeldungen mit geringem Risiko, wie routinemässige Software-Updates, zu einem späteren Zeitpunkt überprüft werden können.

Mit diesem Ansatz können die Sicherheitsteams ihre Bemühungen und Ressourcen effektiv nach Prioritäten ordnen und sicherstellen, dass die kritischsten Sicherheitsrisiken umgehend angegangen werden.

Die Durchführung automatischer Maßnahmen aufgrund dieser Informationen und Alerts kann sich also auf den Betrieb auswirken. Die Leistungsfähigkeit von Threat-analysen kann bei Tools wie **ExeonTrace** je nach Umgebung angepasst werden und die Security je nach Umgebung z.B. in IoT-Umgebungen, angepasst werden.



exeon
Smart Cyber Security.

RISIKOBASIERTE ALARMIERUNG

von Klaus Nemelka

RESSOURCEN:

Die neuesten Blogs zu Sicherheit und Netzwerkerkennung
Der Newsletter zum Thema Sicherheitserkennung