Verbesserung der Cyber-Resilienz:

Integration von CVSS für proaktives Sicherheitslücken-Management

In der sich ständig weiterentwickelnden Landschaft der Cybersicherheitsbedrohungen stehen Unternehmen vor der gewaltigen Aufgabe, Sicherheitslücken effektiv zu verwalten, um ihre Systeme und Daten zu schützen.

Ein unschätzbares Werkzeug bei diesem Unterfangen ist das **Common Vulnerability Scoring System (CVSS)**, das einen standardisierten Rahmen für die Bewertung des Schweregrads von Sicherheitslücken bietet.

Lassen Sie uns untersuchen, wie CVSS funktioniert und wie es mit einem **risikobasierten Ansatz**, insbesondere im Kontext von ExeonTrace, integriert werden kann, um die Praktiken zum Management von Sicherheitslücken zu verbessern.

1. Alles über CVSS & Common Vulnerabilities and Exposures (CVE)

Beim CVSS geht es hauptsächlich um eine Bewertung des Risikos, das von einer Sicherheitslücke ausgeht. In manchen Fällen kann dies recht einfach sein. Im Falle einer Sicherheitslücke z. B. in Netzwerkprodukten ist es sehr wahrscheinlich, dass nicht authentifizierte Angreifer später die betroffenen Systeme aus der Ferne angreifen und mit geringem Aufwand die Kontrolle darüber ausüben.

Im Laufe der Jahre sind zahlreiche Systeme mit CVEs kompromittiert worden. Diese wurden dann oft zum Einschleusen von Ransomware genutzt.

Aber es gibt auch andere Beispiele: Manchmal waren die ausgenutzten Schwachstellen, so raffiniert die Angreifer in der Theorie waren, unter realen Bedingungen nur schwer auszuführen. Der Aufwand war hoch, das Potenzial auch, aber der Schaden beschränkte sich z.B. auf das byteweise Auslesen von Daten aus den Browsern einzelner Nutzer. Doch wie lässt sich das alles quantifizieren?

Risiko = Eintrittswahrscheinlichkeit x Schaden

Das allgemeine Prinzip der Risikoanalyse wird bei der systematischen Bewertung von Sicherheitslücken angewandt. Dabei geht es darum, Schadensereignisse zu identifizieren und abzuschätzen, wie wahrscheinlich das Eintreten dieser Ereignisse ist und wie hoch der daraus resultierende Schaden sein könnte.

Systeme zur Bewertung von Sicherheitslücken verwenden vordefinierte Faktoren, um die Wahrscheinlichkeit und das Ausmass eines Schadens so objektiv wie möglich zu quantifizieren. Ein solches System ist das CVSS, das sich international zunehmend als De-facto-Standard für die Beschreibung der wesentlichen Merkmale einer Sicherheitslücke und die Bestimmung ihres Schweregrades etabliert hat.

Metriken für eine differenzierte Bewertung

Sicherheitslücken werden mit CVSS anhand verschiedener Kriterien, sogenannter Metriken, bewertet. Für jede Metrik gibt es vordefinierte Optionen. Daraus wird ein Schweregrad von 0,0 bis 10,0 berechnet, wobei 10,0 dem höchsten Schweregrad entspricht.
Diese Zahlenwerte werden dann den qualitativen Kategorien ("Keine", "Niedrig", "Mittel", "Hoch" und "Kritisch") zugeordnet, die auch aus Berichten über Sicherheitslücken bekannt sind.

Die Metriken zur Bestimmung des Schweregrads sind in drei Gruppen unterteilt:

1. Basismetriken
2. Zeitliche Metriken
3. Umgebungsmetriken

Basismetriken beschreiben die wesentlichen technischen und unveränderlichen Merkmale einer Sicherheitslücke. Mit ihrer Hilfe lässt sich ein sogenannter "Base Score" berechnen, der den technischen Schweregrad einer Sicherheitslücke darstellt. Er kann später nachjustiert und an Veränderungen im Laufe der Zeit oder der jeweiligen Umgebung des betroffenen Systems angepasst werden.

Im Kern besteht CVSS aus mehreren Schlüsselkomponenten:

- **Basismetriken:** Bewerten die intrinsischen Eigenschaften einer Sicherheitslücke, unabhängig von Umgebung- oder Zeitfaktoren. Komponenten wie Angriffsvektor, Angriffskomplexität, erforderliche Privilegien und Benutzerinteraktion geben Aufschluss darüber, wie Sicherheitslücken ausgenutzt werden können.

- **Metriken zu den Auswirkungen:** Messen die potenziellen Auswirkungen der Ausnutzung einer Sicherheitslücke auf die Vertraulichkeit, Integrität und Verfügbarkeit des betroffenen Systems.

- **Zeitliche Metriken:** Hier werden Faktoren berücksichtigt, die sich im Laufe der Zeit entwickeln, wie z.B. die Verfügbarkeit von Patches und die Reife des Exploit-Codes.

- **Umgebungsmetriken:** Dieser Aspekt passt die CVSS-Scores so an, dass sie die einzigartige Umgebung eines Unternehmens und die potenziellen Auswirkungen auf seine Systeme widerspiegeln.

Bei der Berechnung des CVSS werden diese Metriken nach einer bestimmten Formel zusammengefasst, um eine Gesamtbewertung des Schweregrads einer Sicherheitslücke zu erhalten.

2. Die Bedeutung und Benefits von CVSS

Die Vorteile eines Verständnisses über das CVSS und CVE bieten Unternehmen und Security Teams mehrere Vorteile bei der Sicherung von Systemen.

Zuweisung von Ressourcen	Durch die Nutzung von CVE-Kennungen können Unternehmen bekannte Sicherheitslücken in ihren Systemen nachverfolgen und die Ressourcen für Patches und Abhilfemassnahmen nach dem Grad der von jeder Sicherheitslücke ausgehenden Gefahr priorisieren. Auf diese Weise wird sichergestellt, dass begrenzte Ressourcen effizient für die dringendsten Sicherheitsprobleme eingesetzt werden.
Interoperabilität	Die Standardisierung durch CVSS und CVE ermöglicht eine bessere Interoperabilität zwischen Sicherheitstools und -systemen. NDR-Tools können CVE-Kennungen verwenden, um Netzwerkereignisse mit bekannten Sicherheitslücken zu korrelieren, was eine genauere Erkennung und Reaktion auf potenzielle Bedrohungen ermöglicht.
Integration von Bedrohungsdaten	CVSS und CVE erleichtern die Integration von Threat Intelligence Feeds in etwa in NDR-Tools. Durch die Zuordnung von Netzwerkaktivitäten zu bekannten Sicherheitslücken können die eingesetzten Lösungen Threat Intelligence nutzen, um potenzielle Bedrohungen auf der Grundlage ihrer Verbindung zu bekannten CVEs zu identifizieren und zu priorisieren.
Verbesserte Incident Response	Die Kenntnis von CVSS-Scores und CVE-Identifikatoren ermöglicht eine schnellere und effektivere Reaktion auf Vorfälle. Sicherheits-Tools, z.B. NDRs können Netzwerkereignisse automatisch mit relevanten CVEs korrelieren und so Sicherheitsteams mit verwertbaren Informationen versorgen, um potenzielle Sicherheitsvorfälle umgehend zu untersuchen und zu entschärfen.
Compliance-Anforderungen	Viele rechtliche Rahmenbedingungen verlangen von Unternehmen, dass sie bekannte Sicherheitslücken verfolgen und beheben. Die Kenntnis von CVSS und CVE hilft Unternehmen dabei, diese Compliance-Anforderungen zu erfüllen, indem sie Sicherheitslücken rechtzeitig identifizieren, priorisieren und beheben können.
Risikobewertung	Unternehmen können mit CVSS den Schweregrad von Sicherheitslücken bewerten, indem sie Punkte auf der Grundlage von Faktoren wie Ausnutzbarkeit und Auswirkungen zuweisen. Auf diese Weise lassen sich Patches und Massnahmen zur Risikominderung effektiv priorisieren und die Ressourcen auf die Beseitigung der kritischsten Sicherheitslücken konzentrieren.

3. EDR und CVEs

Endpoint Detection and Response (EDR) sollten regelmässig Daten aus seriösen CVE-Datenbanken (wie der National Vulnerability Database - NVD) einlesen. Diese Datenbanken liefern Informationen über bekannte Sicherheitslücken, einschliesslich ihrer CVE-Kennungen und zugehörigen CVSS-Scores. Bei der Zuordnung von CVEs zu Signaturen erstellen EDRs Signaturen oder Regeln auf der Grundlage von CVE-Informationen, wobei jede Signatur einer bestimmten Sicherheitslücke (gekennzeichnet durch ihre CVE) entspricht.

Wenn ein EDR eine Aktivität entdeckt, die einer Signatur entspricht, löst er eine Warnung aus. EDRs können Endpunkte auf der Grundlage von CVE-bezogenen Warnungen blockieren oder unter Quarantäne stellen. Sobald ein Endpunkt ein Verhalten zeigt, das mit einer bekannten CVE in Verbindung steht, kann der EDR handeln (wie z. B. den Netzwerkverkehr blockieren, den Endpunkt isolieren).

Die meisten EDR-Sicherheitsteams verwenden verschiedene CVE-Datenbanken, um Sicherheitslücken aufzuspüren und ihre Sicherheitstools zu aktualisieren, um die Kunden vor diesen Lücken zu schützen. Wenn eine neue CVE auftaucht, wird die EDR-Lösung mit der entsprechenden Signatur aktualisiert, so dass Zero-Day-Angriffe am Netzwerkrand blockiert werden können, manchmal sogar, bevor ein Hersteller-Patch herausgegeben oder auf das anfällige System angewendet wurde. EDRs und Firewalls können zwar Versuche blockieren, bekannte CVEs auszunutzen, auch wenn die zugrunde liegende Sicherheitslücke noch nicht behoben wurde, aber sie verfügen meist nicht über generische Regeln und Verhaltensanalysen, um Angriffe von neuen und noch mehr von unbekannten Bedrohungsvektoren zu erkennen.

4. Viel mehr als EDR: Wie NDR mit Machine Learning die Extrameile geht

Network Detection and Response (NDR) geht über die typischen Angebote von EDR hinaus, indem es einen ganzheitlichen Ansatz für die Cybersicherheit verfolgt. NDR kombiniert die Leistung von Scoring (wie CVSS) und **Machine Learning (ML)**.

Während EDRs in erster Linie auf signaturbasierter Erkennung beruhen, wird dies bei NDR durch verhaltensbasierte Anomalieerkennung ergänzt.

Dadurch können Bedrohungen nicht nur durch bekannte CVEs, sondern auch durch neue und aufkommende Angriffsvektoren erkannt werden. Durch die Analyse von Abweichungen und Anomalien erkennt das NDR verdächtige Verhaltensmuster, noch bevor spezifische Signaturen verfügbar sind. Es verlässt sich nicht nur auf historische Daten, sondern passt sich an die sich entwickelnden Bedrohungen an.

Mehr als nur bekannte Sicherheitslücken
Während EDRs vor allem bekannte Sicherheitslücken blockieren, erweitert NDR seine Fähigkeiten auf Zero-Day-Angriffe und unbekannte Bedrohungsvektoren.
Es beobachtet den Netzwerkverkehr, das Benutzerverhalten und die Systeminteraktionen. Wenn eine Aktivität von der Norm abweicht, löst es Warnungen aus, unabhängig davon, ob ein bestimmtes CVE damit verbunden ist.
Das NDR lernt kontinuierlich aus dem Netzwerkverhalten. Es passt sich an Veränderungen an und ist daher auch gegen neue Angriffstechniken wirksam. Selbst wenn ein Angriffsvektor noch nie zuvor gesehen wurde, kann NDR aufgrund eines anomalen Verhaltens Warnungen auslösen.

Und last but not least: NDR beschränkt sich nicht nur auf Endpunkte. Es überwacht netzwerkweite Aktivitäten und bietet einen breiteren Kontext. Die NDR-Funktionen ermöglichen es, Ereignisse in der gesamten Infrastruktur zu korrelieren.

In Verbindung mit EDR kann NDR schnell auf Bedrohungen reagieren. Es stützt sich nicht nur auf endpunktbasierte Regeln, sondern berücksichtigt netzwerkweite Muster.

5. CVSS und Risikobewertung

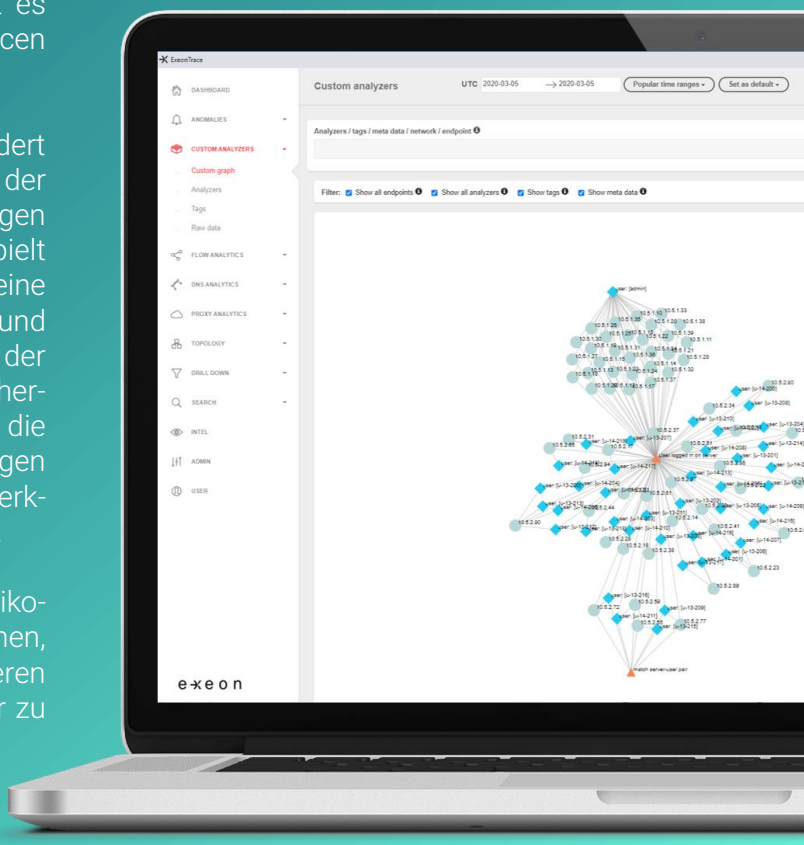
Risiko-basierte Alarmierung (RBA) ist ein Highlight an Effizienz im Bereich der Cybersicherheit und bietet einen dynamischen Ansatz zur Erkennung von und Reaktion auf Bedrohungen. Durch die Priorisierung von Alarmen auf der Grundlage vordefinierter Risikostufen stellt RBA sicher, dass Sicherheitsteams ihre Bemühungen auf die wichtigsten Punkte konzentrieren können. Diese Strategie reduziert nicht nur die Anzahl der Warnmeldungen, sondern ermöglicht es Unternehmen auch, ihre Ressourcen effektiver zu nutzen.

Ein wirksames Risikomanagement erfordert ein umfassendes Verständnis sowohl der Wahrscheinlichkeit als auch der Folgen potenzieller Sicherheitsvorfälle. Hier spielt CVSS eine zentrale Rolle, da es eine standardisierte Methode zur Bewertung und Priorisierung von Sicherheitslücken auf der Grundlage ihrer Risikostufen bietet. Sicherheitslücken mit hohen Werten für die Ausnutzbarkeit oder die Auswirkungen erfordern beispielsweise sofortige Aufmerksamkeit und robuste Schutzmassnahmen.

Die Integration von CVSS mit einem risikobasierten Ansatz ermöglicht es Unternehmen, Sicherheitslücken proaktiv zu identifizieren und zu beheben und so ihre Cyberabwehr zu stärken. Das Verständnis des CVSS und CVE bietet Unternehmen und **Network Detection and Response (NDR)-Tools** mehrere wichtige Vorteile. Es ermöglicht eine verbesserte Risikobewertung durch die Verwendung von CVSS-Scores zur Bewertung des Schweregrads von Sicherheitslücken, was eine effektive Ressourcenzuweisung unterstützt.

Dies erleichtert eine optimierte Ressourcenzuweisung, indem bekannte Sicherheitslücken systemübergreifend anhand von CVE-Kennungen verfolgt und Patches und Abhilfemassnahmen je nach Risikostufe priorisiert werden.

Darüber hinaus verbessert die Standardisierung durch CVSS und CVE die Interoperabilität zwischen Sicherheitstools, so dass NDR-Tools Netzwerkereignisse mit bekannten Sicherheitslücken unter Verwendung von CVE-Kennungen genau erkennen und korrelieren können.



6. Rationalisierung der Sicherheitsermittlung: Die Synergie von risikobasiertem Alerting und NDR

NDR integriert die Risikobewertung in sein Herzstück. Es werden nicht alle Warnmeldungen gleichbehandelt. Stattdessen wird eine Priorisierung nach Schweregrad und potenziellen Auswirkungen vorgenommen. Ereignisse mit hohem Risiko erhalten sofortige Aufmerksamkeit. Unternehmen können die Schwellenwerte für Warnmeldungen je nach Risikotoleranz feinabstimmen. NDR sorgt ausserdem für relevante Warnmeldungen, reduziert das Rauschen und optimiert die Ressourcenzuweisung.

In Verbindung mit NDR-Lösungen erreicht die Effektivität von RBA neue Dimensionen.

NDR-Lösungen nutzen kontinuierliche Überwachung und Machine-Learning Algorithmen, um in Echtzeit Einblicke in den Netzwerkverkehr und das Benutzerverhalten zu erhalten. Durch die Analyse von Kontextinformationen und Bedrohungsdaten können NDRs das mit erkannten Ereignissen verbundene potenzielle Risiko einschätzen und so schnelle und gezielte Reaktionen auf potenzielle Bedrohungen ermöglichen.

In der dynamischen Landschaft der Cybersecurity-Bedrohungen stehen Unternehmen vor der wichtigen Aufgabe, Sicherheitslücken effektiv zu verwalten, um ihre Systeme und Daten zu schützen. Die Synergie von ExeonTrace aus Scoring, ML und risikobasierten Ansätzen stärkt die Cyberabwehr und sorgt für Widerstandsfähigkeit angesichts der sich entwickelnden Bedrohungen. ExeonTrace verfolgt einen neuartigen Ansatz zur Bewertung von Sicherheitslücken, indem Komponenten wie Angriffsvektor, Komplexität, erforderliche Berechtigungen und Benutzerinteraktion bewertet werden.

ExeonTrace weist numerische Punktzahlen zu, die mithilfe von Umge-bungsmetriken angepasst werden können, um den einzigartigen Kontext eines Unternehmens und die potenziellen Auswirkungen auf das System zu berücksichtigen.

ML-basierte NDR-Lösungen, sind ein Beispiel für die Leistungsfähigkeit dieser Synergie. Durch verhaltensbasierte Anomalieerkennung und dynamische Analyse identifiziert ExeonTrace Bedrohungen auf der Grundlage von Abweichungen vom normalen Netzwerkverhalten.

Ausserdem ermöglicht die risiko-basierte Funktion den Sicherheitsteams die Priorisierung von Alarmen auf der Grundlage des wahrgenommenen Bedrohungsgrads verschiedener Netzwerke, wodurch die Ermüdung durch Alarme verringert und sichergestellt wird, dass kritische Vorfälle sofort beachtet werden.

Durch den Einsatz von CVSS kann ExeonTrace die mit Sicherheitslücken verbundenen Risiken abschätzen und bewerten, so dass Unternehmen die Behandlung auf der Grundlage der Wahrscheinlichkeit und der Folgen der einzelnen Szenarien priorisieren können.

Die Integration von CVSS in bestehende Risikomanagement-Rahmenwerke gewährleistet Konsistenz und Nachvollziehbarkeit während der gesamten Bewertungs- und Abschwächungsphase.

ExeonTrace kann CVSS-Bewertungen durch die Einbeziehung zusätzlicher Faktoren ergänzen, z. B. durch fragebogenbasierte Wahrscheinlichkeitsbewertungen, um ein differenzierteres Risikoverständnis zu ermöglichen.

Darüber hinaus können spezifische Herausforderungen, die durch unterschiedliche Umgebungen wie IoT, OT oder industrielle Steuerungssysteme (ICS) entstehen, durch massgeschneiderte Bewertungen der Sicherheitslücken angegangen werden.

NDR, ML, RBA und CVS: Mehrwert für Ihre Sicherheit

14 Gründe, warum diese Kombination zu einem zukunftssicheren Schutz führt.

1. **Frühzeitige Erkennung:** ML-Algorithmen von ExeonTrace analysieren verhaltensbasierte Anomalien und Abweichungen. Diese Früherkennung ermöglicht proaktive Sicherheitsmassnahmen.

2. **Risikobewertung:** ML-gesteuerte Erkenntnisse verbessern die Risikobewertung durch kontinuierliche Überwachung des Netzwerk-verkehrs und des Nutzerverhaltens. ExeonTrace bewertet potenzielle Risiken im Zusammenhang mit erkannten Ereignissen und ermöglicht schnelle und gezielte Reaktionen.

3. **Proaktive Verteidigung:** ExeonTrace versetzt Unternehmen in die Lage, Sicherheitslücken zu erkennen, bevor sie eskalieren. Die mit hoher Trefferquote erfordern sofortige Aufmerksamkeit und robuste Schutzmassnahmen.

4. **Vertrauen in komplexe Landschaften:** Durch die Kombination von CVSS und ML versetzt ExeonTrace die Benutzer in die Lage, sich in der komplexen Cybersicherheitslandschaft zurechtzufinden.

5. **Ressourceneffizienz:** Rationalisierte, auf vordefinierten Risikostufen basierende Alarmierung reduziert das Alarmvolumen und optimiert die Ressourcenzuweisung.

6. **Granulare Risikobewertung:** CVSS bietet eine standardisierte Methode zur Bewertung der Schwere von Sicherheitslücken unter Berücksichtigung von Faktoren wie Ausnutzbarkeit und Auswirkungen.

7. **NDR-Anpassung:** ExeonTrace nutzt CVSS-Scores, um Netzwerkereignissen, die mit bekannten Sicherheitslücken verbunden sind, Risikostufen zuzuweisen. Diese Granularität ermöglicht es Unternehmen, Alarme auf der Grundlage der potenziellen Auswirkungen zu priorisieren.

8. **CVE-Korrelation:** Durch die Verknüpfung von Netzwerkereignissen mit CVE Identifikatoren priorisiert ExeonTrace Warnungen nach dem Schweregrad der Sicherheitslücken.

9. **Rasche Reaktion:** CVE-Warnungen mit hohem Schweregrad erhalten sofortige Aufmerksamkeit, während CVE-Warnungen mit geringerem Schweregrad entsprechend eingestuft werden. Sicherheitsteams konzentrieren ihre Bemühungen auf die wichtigsten Punkte.

10. **Risikogerechte Einstellungen:** Unternehmen können die Schwellenwerte für Warnungen auf der Grundlage von CVSS-Scores feinabstimmen. So generiert ExeonTrace beispielsweise nur Warnungen für Sicherheitslücken, die einen bestimmten CVSS-Schwellenwert überschreiten.

11. **Relevanz und Handlungsfähigkeit:** Relevante Warnmeldungen gewährleisten eine effiziente Ressourcenzuweisung und gezielte Reaktionen.

12. **Kontextabhängige Warnungen:** Dank CVSS-Scores und CVE-Identifikatoren erhalten die Sicherheitsteams einen Kontext. Sie verstehen die potenziellen Auswirkungen der erkannten Netzwerkereignisse.

13. **Informierte Entscheidungsfindung:** Während der Reaktion auf einen Vorfall steuert dieser Kontext die effiziente Zuweisung von Ressourcen.

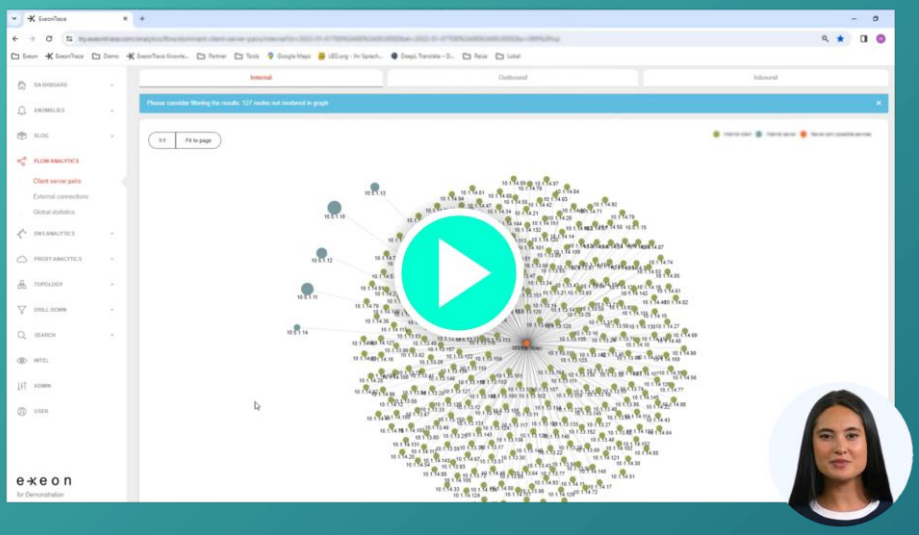
14. **Vom Schweregrad abhängige Bemühungen:** Unternehmen priorisieren Abhilfemassnahmen auf der Grundlage des Schweregrads der damit verbundenen Risiken.

Ihren Leitfaden zur risiko-basierten Alarmierung

Ihr Exemplar runterladen

exeon
Smart Cyber Security.

Sehen Sie ExeonTrace in Aktion



Zum Video