Veröffentlicht auf Presseportal Schweiz - Presse und Medienmitteilungen (https://www.presseportal-schweiz.ch)

20.01. 2026

Exeon.UEBA erkennt identitätsbasierte Angriffe in Echtzeit

Von Zscheile



Bild Rechte
Exeon Analytics

Neue UEBA-Lösung von Exeon Analytics ergänzt Exeon.NDR um die gezielte Erkennung interner und identitätsgetriebener Bedrohungen durch die Verhaltensanalyse von Nutzern, Anwendungen und Unternehmensressourcen

(Zürich)(PPS) Moderne Cyberangriffe erfolgen heute immer seltener durch das Ausnutzen technischer Schwachstellen. Stattdessen nutzen Angreifer kompromittierte Zugangsdaten, legitime Berechtigungen oder interne Konten. Angriffe kommen damit zunehmend von innen – und bleiben für klassische Sicherheitslösungen oft lange unentdeckt. Mit Exeon.UEBA stellt der Schweizer Cybersecurity-Spezialist Exeon Analytics deshalb nun eine neue Lösung zur Analyse von Nutzer-, Entitäten- und Anwendungsverhalten vor, die genau diese Angriffsform adressiert. UEBA (User and Entity Behavior Analytics) ergänzt die etablierte Network Detection & Response Lösung Exeon.NDR und erweitert die Sicherheitsanalyse gezielt um die Identitäts- und Anwendungsebene.

Während Exeon.NDR seit mehreren Jahren Netzwerkaktivitäten analysiert und Bedrohungen anhand von Metadaten erkennt, fokussiert sich Exeon.UEBA auf verdächtiges Verhalten innerhalb legitim genutzter Systeme. Dazu analysiert die

Lösung Logdaten aus Benutzer- und Administratoridentitäten, Unternehmensanwendungen – inklusive SaaS-, Custom- und Legacy-Applikationen –, APIs, Dienstkonten sowie Zugriffs- und Infrastruktursystemen wie VPNs oder IAM-Plattformen.

Verhaltensanalyse statt isolierter Events

Exeon.UEBA korreliert Ereignisse kontextbasiert über verschiedene Systeme hinweg und bewertet sie als zusammenhängende Verhaltensmuster. So lassen sich beispielsweise Passwort-Spraying-Angriffe über mehrere Anwendungen, missbräuchliche Zugriffe auf geschäftskritische Systeme oder auffällige Berechtigungsänderungen zuverlässig erkennen – auch dann, wenn einzelne Logeinträge für sich genommen unauffällig erscheinen. Durch das die stream-basierte Analyse verarbeitet Exeon.UEBA auch sehr große Log-Datenmengen in Echtzeit. Security-Teams erhalten präzise, priorisierte Warnmeldungen mit Kontext, anstatt einer Vielzahl isolierter Events.

Effizienteres Incident Handling und geringere SIEM-Kosten

Ein zentraler Vorteil von Exeon.UEBA liegt in der Entlastung von Security Operations Teams. Die intelligente Korrelation reduziert False Positives deutlich und hilft, reale Bedrohungen schneller zu identifizieren. Gleichzeitig sinkt das Risiko von False Negatives, da auch komplexe, mehrstufige Angriffsmuster erkannt werden.

Darüber hinaus trägt Exeon.UEBA zur Reduktion von SIEM-Kosten bei. Durch intelligentes Datenhandling – inklusive Normalisierung, Deduplikation und Verdichtung von Logdaten – werden nur sicherheitsrelevante Ergebnisse an nachgelagerte SIEM- oder SOAR-Systeme weitergegeben. Das reduziert Datenvolumen, Lizenzkosten und manuellen Analyseaufwand erheblich.

Flexible Bereitstellung mit Fokus auf Datensouveränität

Exeon.UEBA lässt sich vollständig on-premises, in privaten Cloud-Umgebungen oder air-gapped betreiben. Die gesamte Analyse erfolgt innerhalb der Exeon-Appliance. Sensible Identitätsinformationen können verschlüsselt oder anonymisiert verarbeitet werden, sodass Organisationen auch in regulierten Branchen Verhaltensanalysen datenschutzkonform einsetzen können.

„Angriffe nutzen heute Vertrauen statt Schwachstellen“, sagt Gregor Erismann, Co-CEO von Exeon Analytics. „Mit Exeon.UEBA schaffen wir Transparenz über Nutzer- und Anwendungsverhalten und ermöglichen Security-Teams, interne und identitätsbasierte Bedrohungen frühzeitig, effizient und mit deutlich weniger Aufwand zu erkennen.“

Über die Organisation:

Über Exeon Analytics
Exeon Analytics liefert ganzheitliche Sicherheitsanalysen für Organisationen, die mit wachsenden blinden Flecken, verschlüsseltem Datenverkehr und regulatorischem Druck konfrontiert sind. Die Exeon Produkte vereinen umfassende Datenerfassung, hocheffiziente und skalierbare Verarbeitung sowie intelligente Korrelation, um vollständige Transparenz über Netzwerke, Nutzer und Anwendungen zu bieten – inklusive kundenspezifischer Anwendungen, Legacy-Systeme und hybrider Umgebungen.

Durch die Verbindung von KI-basierter Verhaltensanalyse mit flexibler Regel-Logik erkennt Exeon zuverlässig bekannte und unbekannte Bedrohungen, selbst bei großen Datenmengen. Die Alerts sind kontextbezogen und handlungsorientiert, sodass Reaktionen sowohl schnell als auch zuverlässig erfolgen können. Als Experten-Systeme, die vollständig in bestehende SOC- und SIEM-Lösungen integriert werden können, reduziert Exeon die Komplexität, senkt SIEM-Kosten und unterstützt die Einhaltung von NIS2, DORA, DSGVO und Datensouveränität – on-prem oder in Cloud-Umgebungen. Kunden wie Postfinance, SWISS International Airlines, BonnNetz, Klinikum Dortmund und die Schweizer Bundesverwaltung vertrauen auf die Systeme von Exeon Analytics zur effektiven Angriffserkennung.

Pressekontakt:

Weitere Informationen und Kontakt:
Exeon Analytics AG

Grubenstrasse 12
C-8045 Zürich

Gregor Erismann, Co-CEO
+41 44 500 77 21
gregor.erismann @ exeon.com
www.exeon.com

Kategorie
IT & Software & Neue Medien

Source URL: *https://www.presseportal-schweiz.ch/pressemeldungen/exeonueba-erkennt-identitaetsbasierte-angriffe-echtzeit*