Pressemitteilung [5.932 Zeichen inkl. Leerzeichen]

Effektiver Einsatz von KI im Security Operations Center

Var Group stellt KI-gestützte Cybersecurity-Lösungen auf der Hannover Messe vor

München, 27.02.2025 – Cyberangriffe werden durch Künstliche Intelligenz und maschinelles Lernen immer raffinierter – doch dieselben Technologien können auch für effiziente Abwehr genutzt werden. Yarix, die auf Cybersecurity-Lösungen und -Dienstleistungen spezialisierte Abteilung der Var Group, setzt mit Egyda auf eine Kombination aus Automatisierung, Künstlicher Intelligenz und menschlicher Expertise. Das modulare System optimiert die Bedrohungserkennung, priorisiert Sicherheitsanomalien und unterstützt das Security Operations Center (SOC) mit präzisen Analysen und Handlungsempfehlungen in natürlicher Sprache.

Die zunehmenden Bedrohungen und der anhaltende Fachkräftemangel stellen Security Operations Centers (SOCs) vor große Herausforderungen – insbesondere, wenn es darum geht, eine immer größer werdende Datenflut zu bewältigen. Manuelle Prozesse sind dabei oft ineffizient, da sie wertvolle Ressourcen binden und die Reaktionszeiten verzögern. Diesen Herausforderungen begegnet Yarix mit Egyda, das gezielt auf Automatisierung durch Künstliche Intelligenz (KI) und maschinelles Lernen (ML) setzt, um Bedrohungen schneller und präziser zu erkennen. Mithilfe von Hyperautomatisierung werden sicherheitsrelevante Daten intelligenter verarbeitet, während ein spezialisiertes KI-Modell Analysten bei der Risikoeinschätzung unterstützt. Ergänzend ermöglicht eine fortschrittliche Verhaltensanalyse die frühzeitige Identifikation kompromittierter Zugangsdaten. Diese Technologien entlasten das SOC, beschleunigen die Reaktionszeiten und verschaffen Unternehmen einen entscheidenden Vorsprung.

Reaktionszeit mit Egyda um 50 Prozent schneller

„In 2024 hat unser SOC etwa 500.000 Warnungen verwaltet, 52 Prozent davon mit Hilfe von Egyda. Bei diesen 52 Prozent wurde jede vierte Meldung vollständig automatisiert und ohne menschliches Eingreifen bearbeitet“, berichtet Marco Iavernaro, Global SOC-Manager bei Yarix, über die Erfahrungen mit den neu eingesetzten Technologien. „Wir haben auch die Verringerung der Mean Time To Respond, also der Zeit zwischen dem Auslösen einer Warnung und der Reaktion des SOC, gemessen. Mit Egyda ist sie um 53 Prozent geringer.“

Eine zentrale Egyda-Komponente ist die Hyperautomatisierung. Um die Analyse und Korrelation von Sicherheitsdaten zu automatisieren und SOC-Mitarbeitende zu entlasten, wurden die Erkennungsszenarien aus SIEM-, EDR- und NDR-Tools nach Industriestandards wie MITRE ATT&CK standardisiert und in ein einheitliches Taxonomiesystem überführt. Basierend auf den Taxonomieschemata führt das System dynamische Abfragen in relevanten Datenbanken durch, um Sicherheitsanomalien präziser zu bewerten und miteinander in Beziehung zu setzen. Eine intern

entwickelte Modellierungssprache, die das Herzstück des Systems ist, verarbeitet diese Daten, ergänzt sie um Metainformationen und gibt eine Bewertung der Anomalie in natürlicher Sprache (NLP) aus – inklusive Maßnahmen zur Eindämmung. Zudem wurden Eskalations- und Präsentationsprozesse automatisiert, sodass Sicherheitsvorfälle schneller und strukturiert an relevante Akteure weitergeleitet werden. Die Weiterentwicklung der NLP-Komponente soll das System künftig noch effizienter und wartungsfreundlicher machen.

Im Zusammenhang mit dem Security Operations Center hat Var Group mit seiner Abteilung für Cybersicherheit, Yarix zudem ein spezielles KI-Modell entwickelt. Dieses gibt eine Wahrscheinlichkeitsbewertung ab, ob eine von SIEM-, EDR- oder NDR-Plattformen gemeldete Anomalie ein echter positiver Befund ist. Als Basis für das Modell wurde ein einheitliches Datenformat für Sicherheitsanomalien der einzelnen Tools entwickelt. Nach der Standardisierung und der Übersetzung von Anomalien wurde das Modell, basierend auf Regressionsbäumen, mit 18 Monaten SOC-Daten trainiert. Im Einsatz bewertet es alle gemeldeten Anomalien mit einer Wahrscheinlichkeitsskala von 0 bis 100 und zeigt die entscheidenden Faktoren für die Bewertung an. Das Ziel des Modells ist es, die Analysten bei der Einstufung und Priorisierung der zu analysierenden Bedrohungen zu unterstützen. Das Modell kann bei Bedarf nach Kundenanforderungen trainiert werden.

Zuverlässige Erkennung kompromittierter Zugriffsdaten

Ein weiteres Egyda-Tool ist YUBA: Das System nutzt Verhaltensanalyse und KI, um eine fortschrittlichere und genauere Anomalieerkennung als herkömmliche SIEM-Systeme zu gewährleisten. Es sammelt automatisch Rohprotokolle und erstellt ein detailliertes Zugriffsprofil basierend auf Benutzer, Zeitpunkt und IP-Adresse. Zusätzlich werden weitere Attribute auf Basis der IP-Adresse, wie Geodaten, APN, ISP und Geräteinformationen berücksichtigt. Dadurch kann YUBA Anomalien identifizieren, die auf einen möglichen Identitätsdiebstahl oder eine Kompromittierung der Zugangsdaten hinweisen. Die KI-basierte Datenverarbeitung erfolgt in zwei Phasen: Zuerst wird die Authentifizierung mit dem bisherigen Nutzerverhalten verglichen; Abweichungen werden als potenziell anomal markiert. Danach wird ein speziell entwickelter Entscheidungsbaum genutzt, um weitere Kontextfaktoren zu prüfen und eine fundierte Bewertung der Authentizität vorzunehmen. YUBA liefert nicht nur Wahr/Falsch-Ergebnisse, sondern begründet erkannte Anomalien – dank der Integration in bestehende Hyperautomatisierungssysteme in natürlicher Sprache.

Als Cybersicherheitsexperte der Var Group präsentiert Yarix auf der Hannover Messe in Halle 16, Stand C06, modernste Sicherheitslösungen und lädt Besucher dazu ein, ihr Wissen auf die Probe zu stellen. Im Escape Game „Cyber Nightmare: Can you escape?“ erleben sie einen simulierten Cyberangriff und müssen sich in Bereichen wie Compliance, Incident Response und IT-Sicherheitstaktiken beweisen. Unterstützung gibt es von Egyda – die KI hilft, falsche Fährten zu eliminieren und den Angriff erfolgreich abzuwehren.

Über Var Group

Die Var Group ist ein internationaler Anbieter digitaler Dienstleistungen und IT-Lösungen. Seit mehr als 50 Jahren unterstützt die Var Group Unternehmen jeder Größe bei der digitalen Evolution. Dabei liegt der Fokus auf Smart Services, Digital Cloud, Cyber Security, Multimedia Workspaces, Data Science, Digital Experience, Var Industries, Business Application International, Industry Solution Retail & Logistik in der Food-Branche. Als 360° IT-Dienstleister – von Beratung und Strategie über Implementierung bis Service und Wartung – bedient das Unternehmen den industriellen Sektor in Branchen wie Automotive, Maschinenbau, produzierendes Gewerbe, Pharma, Lebensmittel, Textilien, Mode, Luxus und Möbel sowie den Einzelhandel.

Die Var Group S.p.A. mit Sitz in Empoli (Italien) und einem Jahresumsatz von 823 Mio. Euro ist der italienische Marktführer für Software- und Systemintegrationslösungen und über ihre Muttergesellschaft Sesa an der italienischen Börse notiert. Über 3.850 hochqualifizierte Mitarbeitende in 13 Ländern unterstützen Kunden dabei, sich erfolgreich für den Wettbewerb in der Zukunft aufzustellen. Auf dem deutschen Markt agiert die Var Group durch ihre Tochter Var Group GmbH mit Sitz in München.

Als Mitglied des UN Global Compact setzt sich der IT-Spezialist aktiv für Nachhaltigkeit und soziale Gerechtigkeit ein. Die Var Group verfolgt einen integrativen Ansatz und fördert Individualität, Vielfalt und Chancengleichheit, u. a. mit Programmen zur Förderung von Frauen in der IT-Branche und in Führungspositionen.

Weitere Informationen unter www.vargroup.de

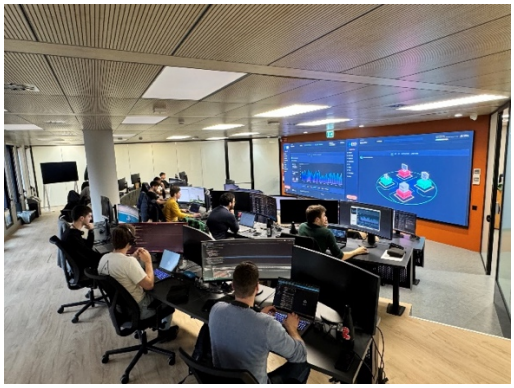
[Bilder und Text zur freien Verwendung]

Bildmaterial

[Hyperautomatisierungsprozess]

Bildunterschrift: Hyperautomatisierung in Security Operations Center: Egyda verarbeitet Sicherheitsvorfälle in Sekunden und gibt Handelsempfehlungen in natürlicher Sprache aus.
Bildnachweis: Var Group

[SOC-Mitarbeitende]



Bildunterschrift: Der Einsatz von KI entlastet die SOC-Analysten, verhindert Überlastung und steigert die Gesamtproduktivität des Teams.
Bildnachweis: Var Group

[Marco_Iavernaro]

Bildunterschrift: Mit über 10 Jahren Erfahrung im SOC-Bereich erkennt Marco Iavernaro das Potenzial von KI, um die Effizienz und Reaktionsfähigkeit in der Cyberabwehr zu steigern.
Bildnachweis: Var Group

Pressekontakt

Maura Możejko

Carta GmbH
www.carta.eu
Iggelheimer Straße 26
67346 Speyer
Deutschland

Mail: var@carta.eu
Tel.: +49 (0) 6232 / 100 111-13

Unternehmenskontakt

Franziska Unterfrauner

Var Group
www.vargroup.de
Mies-van-der-Rohe-Straße 8
80807 München
Deutschland

Mail: f.unterfrauner@vargroup.com
Tel.: +49 (0) 1512 5021562