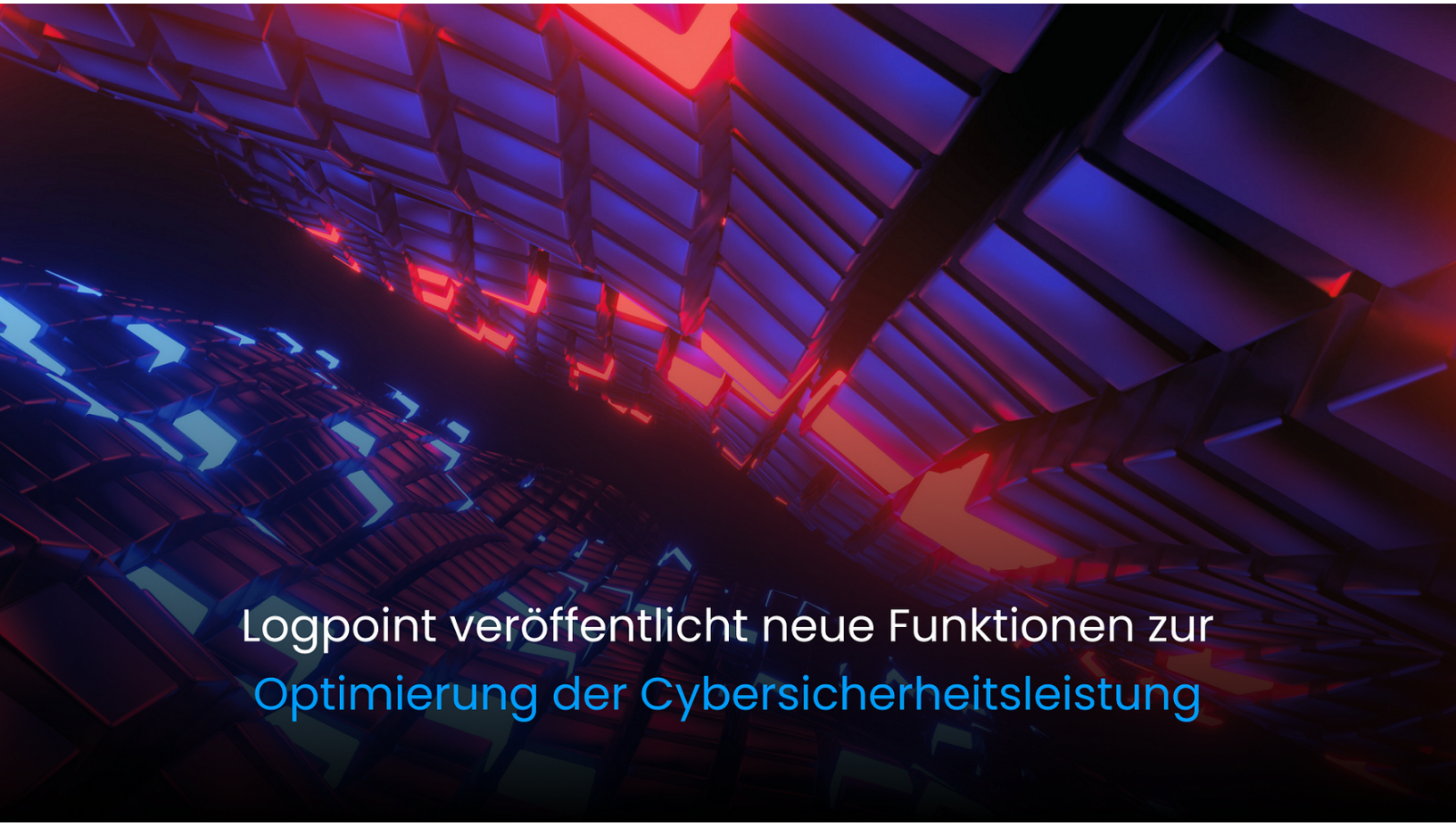

30.01.2024 10:00 CET

Logpoint veröffentlicht neue Funktionen zur Optimierung der Cybersicherheitsleistung

- **Logpoint erweitert seine Converged SIEM-Plattform, um Unternehmen und MSSPs dabei zu helfen, die Cybersicherheitsleistung zu verbessern sowie Zeit und Ressourcen im Sicherheitsbetrieb freizusetzen.**
- **Die neue Version reduziert die Arbeitsbelastung bei operativen Aufgaben und ermöglicht es SOC-Teams, die Effizienz bei der Erkennung, Untersuchung und Reaktion auf Bedrohungen zu steigern.**

KOPENHAGEN & LONDON, den 30. Januar 2024 – Logpoint kündigt die

Einführung neuer Funktionen für seine Converged SIEM-Plattform an, die die Erkennung von Bedrohungen und Sicherheitsoperationen verbessern sowie die Fallverwaltung optimieren. Unternehmen können sich mit den neuen Funktionen auf wesentliche Sicherheitsbelange konzentrieren, indem sie den Workload reduzieren, die Automatisierung vereinfachen und Ressourcen freisetzen.

Die neue Version bietet eine höhere Systemstabilität und Zuverlässigkeit sowie eine effizientere Ressourcennutzung durch die Einführung einer adaptiven Speicherverwaltung, die die Speichernutzung automatisch optimiert. Dies ermöglicht es den Nutzern, Serviceunterbrechungen zu vermeiden und den Zeitaufwand für die manuelle Speichereinstellung zu verringern. Außerdem können sie weitere Nodes hinzufügen und die Sichtbarkeit durch die Freigabe von zusätzlichem Speicher erhöhen.

Logpoint verbessert die Konfiguration von Alarmen durch ein einziges Fenster und weniger Klicks. Darüber hinaus wurde die Art und Weise, wie Benutzer Listen auffüllen und aktualisieren, vereinfacht. Jetzt können sie eine Liste von z.B. IoCs, bösartigen Domains, IPs, etc. in einer .CSV oder .TXT Datei hochladen. Dies bietet den Benutzern eine flexible Möglichkeit, Listen aus verschiedenen Quellen hinzuzufügen, erleichtert ihre Arbeit und trägt dazu bei, die Bedrohungserkennung auf dem neuesten Stand zu halten.

„Sichtbarkeit, Reaktionszeit und Vertrauen in die Untersuchung sind wichtige Faktoren bei der erfolgreichen Abwehr von Cyberangriffen, und wir freuen uns, Unternehmen mit der neuen Logpoint-Version dabei zu helfen, dies zu verbessern“, sagt Edy Almer, Director of Products bei Logpoint. „Wir helfen Unternehmen im Wesentlichen dabei, mehr Ressourcen zu erhalten, um sich auf das zu konzentrieren, was für ihre Sicherheit wichtig ist. Das ist essentiell, da der Druck auf Cybersecurity-Experten durch die wachsenden Daten- und Cybersecurity-Vorschriften und die sich ständig ändernden und innovativen Methoden der Bedrohungsakteure zunimmt.“

Mit dem neuen Update optimiert Logpoint die Sicherheitsorchestrierung, Automatisierung und Reaktion (SOAR) sowie das Fallmanagement. So werden beispielsweise Vorfall-Artefakte automatisch in Fälle extrahiert, was zusätzlichen Kontext schafft, die Arbeitsbelastung der Analysten verringert und die Erkennung und Reaktion verbessert. Benutzer können eine neue Playbook-Aktion hinzufügen, um Vorfälle zu lesen und alle extrahierbaren Daten als Artefakte zu dem Fall hinzuzufügen. Darüber hinaus können

Sicherheitsteams Protokolle direkt über das Fallmanagement-Tool durchsuchen und die Ergebnisse in den Fall zurückführen, was die Untersuchungen zusätzlich vereinfacht.

Das neue Update ermöglicht es MSSPs und denjenigen, die mit verschiedenen Tenants arbeiten, Zeit zu sparen und Fehler bei der Verteilung von Playbooks an Kunden zu reduzieren. Logpoint veröffentlicht generische Playbooks für typische Sicherheitsanwendungsfälle, die einmal aktualisiert und an die Kunden verteilt werden können. Diese Playbooks sind integrationsunabhängig, so dass Tenants mit unterschiedlichen Integrationen von ihnen profitieren können. Darüber hinaus können MSSPs bei der Verteilung der Playbooks viel Zeit sparen.

Logpoint führt auch neue Funktionen für das Produkt Director ein, die Plattform für die Verwaltung großer Implementierungen mit der Möglichkeit, Protokollquellen über mehrere Mandanten hinweg zu generieren und zu verwalten sowie Protokollquellen nach Vorlage zu erstellen, um die Komplexität zu verringern.

Logpoint Converged SIEM ist eine End-to-End-Cybersicherheitsplattform, die den gesamten Prozess der Bedrohungserkennung und Vorfallsreaktion (TDIR) abdeckt. Die Plattform fügt automatisch Bedrohungsdaten, Unternehmenskontext und Unternehmensrisiken zu den Beobachtungen hinzu, um schwache Signale in aussagekräftige Untersuchungen umzuwandeln, und ermöglicht es Analysten, durch Automatisierung und Orchestrierung schneller zu reagieren.

Um mehr über alle Upgrades und Verbesserungen der Logpoint-Plattform für Cybersecurity-Operationen zu erfahren, besuchen Sie den Blogbeitrag von Logpoint hier.

Über Logpoint

Logpoint⊠ist Hersteller einer zuverlässigen, innovativen Plattform für Cybersecurity-Operationen – die Organisationen weltweit befähigt, in einer sich ständig wandelnden Bedrohungswelt erfolgreich zu agieren. Durch die Kombination anspruchsvoller Technologie und eines tiefen Verständnisses für die Herausforderungen der Kunden stärkt⊠Logpoint⊠die Fähigkeiten der

Sicherheitsteams und hilft ihnen,⊠aktuelle⊠und zukünftige Bedrohungen zu bekämpfen.⊠Logpoint⊠bietet⊠SIEM-,⊠UEBA,⊠SOAR- und SAP-Technologien in einer umfassenden Plattform, die Bedrohungen effizient erkennt, falsch-positive Ergebnisse minimiert, Risiken automatisch priorisiert, auf Vorfälle reagiert und vieles mehr. Mit Hauptsitz in Kopenhagen, Dänemark und Büros auf der ganzen Welt ist⊠Logpoint⊠ein multinationales, multikulturelles und inklusives Unternehmen. Für weitere Informationen gehen Sie auf⊠www.logpoint.com.⊠

Kontaktpersonen

Maimouna Corr Fonsbøl
Pressekontakt
PR Manager
PR & Communications
mcf@logpoint.com
+45 25 66 82 98