Proofpoint Managed SIEM

Verbesserte Sicherheit für Ihre Splunk-Umgebung

Wichtige Vorteile

- Umfassender Überblick durch bessere Erkennung: Identifizieren Sie verborgene Bedrohungen dank Kompromittierungsindikatoren aus Proofpoint Emerging Threat Intelligence.
- Proaktive Reaktion dank intelligenter Bedrohungssuche: Wir analysieren die Bedrohungsakteure und suchen nach entsprechenden Indizien in Ihrer Umgebung. Durch umfassende Einblicke in kontextbezogene Faktoren wie Ziele, Zeitrahmen und andere Aspekte ermöglichen wir die proaktive Reaktion und Behebung.
- Überwachung und Erkennung rund um die Uhr: Wir optimieren Ihre Umgebung in kürzester Zeit. Unsere Threat Hunter unterstützen Ihr SIEM-System mit kontinuierlicher Überwachung und verkürzen die durchschnittliche Zeit bis zur Behebung.
- Erstklassige Sicherheitsexpertise: Unsere erstklassigen Sicherheitsexperten gewährleisten die Sicherheit Ihrer Splunk-Umgebung.

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die sich auf die Behebung der vier wichtigsten personenbezogenen Risiken konzentriert.

Mit Proofpoint Managed SIEM erhalten Sie Zugang zu einem Expertenteam, das sich ausschließlich auf die Erkennung, Analyse und Abwehr von Bedrohungen konzentriert. Der Service bietet verbesserten Bedrohungsschutz für Splunk-Umgebungen, sodass Sie einen Teil der SIEM-Aufgaben (Sicherheitsinformations- und Ereignis-Management) abgeben können. Außerdem profitieren Sie von erweiterter Bedrohungssuche.

Proofpoint Managed SIEM unterstützt Ihr IT- und Sicherheitsteam bei der Bewältigung der täglichen Herausforderungen, die bei der Verwaltung großer Mengen von Warnmeldungen und der schnellen Reaktion auf damit verbundene Ereignisse auftreten. Ohne unseren Service lassen sich diese Aufgaben häufig kaum bewältigen. Hinzu kommt, dass sich die Situation durch neue Erkennungstechnologien und die dadurch weiter wachsende Menge an Warnmeldungen noch weiter verschärft. Dies kann dazu führen, dass Ihre Mitarbeiter durch zu viele Warnmeldungen überlastet werden – selbst wenn sie sich an Best Practices, Runbooks und die neuesten Tools und Analysen halten.

Vereinfachung der Sicherheitsabläufe

Splunk-Kunden, die Proofpoint Managed SIEM einsetzen, profitieren unter anderem von folgenden Vorteilen:

- **Verbesserte Erkennung:** Im Gegensatz zu anderen Services, die nur die Warnmeldungen anderer SIEM-Lösungen verarbeiten, verbessert Proofpoint Managed SIEM die Erkennung durch Bedrohungsdaten und -indikatoren. Dadurch sehen wir Bedrohungen, die anderen verborgen bleiben.
- **Bedrohungssuche und Aufdeckung von Zusammenhängen:** Unser Portfolio an Sicherheitsprodukten deckt zahlreiche Erkennungsvektoren ab und bietet eine äußerst umfangreiche Bedrohungslandkarte mit mehr als einer Billion Knoten, die von über 100 Bedrohungsforschern mithilfe von Machine Learning und künstlicher Intelligenz erstellt wird. Dank des großen Umfangs und der detaillierten Daten erkennen wir nicht nur Bedrohungen, sondern auch Verbindungen zwischen scheinbar unzusammenhängenden Ereignissen.
- **Bedrohungsschutz rund um die Uhr:** Hinter Proofpoint Managed SIEM steht ein globales Expertenteam für Sicherheit und Bedrohungserkennung. Unsere Experten befinden sich in Sicherheitskontrollzentren auf der ganzen Welt und identifizieren, triagieren und analysieren rund um die Uhr Bedrohungen für unsere Kunden.

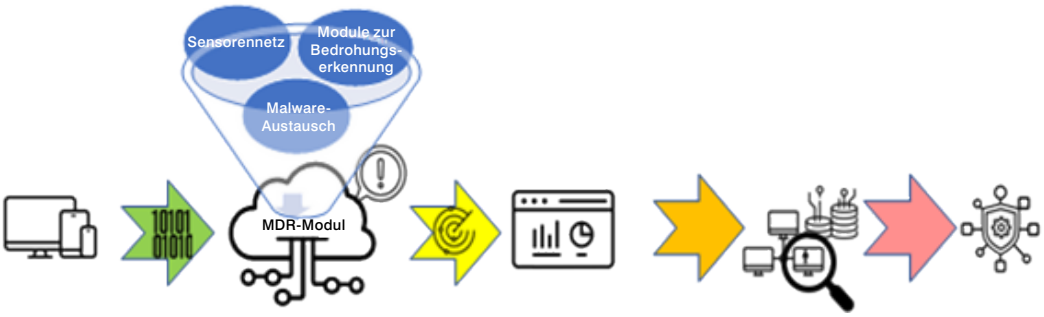

Abb. 1: Protokolle werden an das MDR-Modul (Managed Detection and Response) weitergeleitet, das mithilfe von Proofpoint-Bedrohungsdaten detaillierte Warnmeldungen erstellt. Unser Team triagiert, analysiert und priorisiert die Warnmeldungen. Anschließend führt es Korrelationsanalysen durch und sucht aktiv nach Bedrohungen, um diese einzudämmen und abzuwehren.

Anreicherung von Splunk-Protokollen mit Proofpoint-Bedrohungsdaten

Die Protokolle Ihres Netzwerks werden mit den Bedrohungsdaten von Proofpoint angereichert, um möglicherweise übersehene Bedrohungen zu identifizieren und neue Proofpoint-Warnmeldungen zu generieren. Wir unterziehen Warnmeldungen einer Triage-Prüfung und untersuchen sie anschließend. Details zu Bedrohungen (z. B. betroffene Anwender, wertvolle Ziele und Angriffsmuster) werden zum Zwecke der Priorisierung und Behebung identifiziert. Sofern eine erweiterte Bedrohungssuche erforderlich ist, werden die Bedrohungen entsprechend analysiert.

Zur schnellen Behebung aktiver Bedrohungen arbeitet das Proofpoint-Team mit einem vereinfachten Genehmigungs-Workflow, der zudem sicherstellt, dass die Sicherheitsressourcen des Unternehmens wieder für wichtigere oder strategische Sicherheitsaufgaben zur Verfügung stehen.

Erweiterte Bedrohungserkennung für Ihr Unternehmen

Der Proofpoint-Service verbessert die herkömmlichen SIEM-Funktionen mit erweiterten Erkennungsfunktionen, die auf branchenführenden Technologien und Services basieren und folgende Vorteile bieten:

- **Einzigartige Erfahrungswerte und proaktive Expertise:** Mit den Proofpoint-Bedrohungsdaten können wir Ihnen proaktiven Schutz bieten. Unser globales Sensornetzwerk und unser Bedrohungsanalysten- und Forscherteam bieten plattformübergreifende Bedrohungssuche und Korrelation. Dabei handeln unsere Experten vorausschauend, d. h. sie entwickeln Schutzmaßnahmen, die genau auf Ihre Bedürfnisse zugeschnitten sind, und greifen auf branchenweit bewährte Methoden und die neuesten Produkt-Updates von Proofpoint zurück.
- **Kontinuierliche, kostengünstige Sicherheitsabläufe:** Das Einstellen, Ausbilden und Halten von Sicherheitspersonal ist eine große Herausforderung. Dies gilt umso mehr, wenn es um spezielles Fachwissen wie die Identifizierung und Behebung von Zwischenfällen geht. Mit unseren Managed Services erhalten Sie Zugang zu unserem Expertenteam, das Ihnen rund um die Uhr zur Verfügung steht. Auf diese Weise können Sie die Zeit, das Geld und die Ressourcen für die Bewältigung lokaler Personalprobleme auf ein Minimum reduzieren.
- **Regelmäßige Berichte und Einblicke für Führungskräfte:** Wir liefern Ihnen Metriken, die wertvolle Einblicke in Sicherheitstrends geben, potenzielle neue Sicherheitsprioritäten aufzeigen und Ihnen helfen, fundierte Entscheidungen zu treffen.

Diese Informationen werden bei Proofpoint Managed SIEM in Ihre Systeme integriert, sodass Ihre Bedrohungsabwehr optimiert wird. Unser Team unterstützt Sie bei der Aufrechterhaltung der Sicherheit in Ihrer Umgebung und bei der Optimierung der Regelkonfiguration in Splunk, sodass Bedrohungen zuverlässig erkannt werden. Diese Unterstützung umfasst die Implementierung von System-Upgrades, Patches und notwendigen Optimierungen. Unsere Lösung kombiniert die erweiterte Erkennung, Priorisierung und Behebung schwerwiegender Bedrohungen mit schnellen Abwehrmaßnahmen. Kurz gesagt: Unser Team bietet Sicherheitstechnik vom Feinsten. Wir helfen Ihnen dabei, Sicherheitslücken zu schließen und Angriffsflächen zu reduzieren.

MEHR ERFAHREN

Weitere Informationen finden Sie unter **proofpoint.com/de**.