splunk>

SOLUTION GUIDE

SPLUNK® FÜR SICHERHEIT

Nutzen Sie analysegestützte Sicherheit.

- **Umfassende Sicherheitsanalysen** aus Sicherheits- und anderen Datenquellen
- **Optimierte Untersuchung komplexer Bedrohungen** durch die "Kill Chain"-Methodik
- **Schnelle Vorfallsanalyse** durch kurze Antwortzeiten und proaktive Bedrohungssuche
- **Auf Machine Learning basierende leistungsfähige Analysen** für die schnelle Anomalie- und Bedrohungserkennung und Minimierung interner und externer Angriffe
- **Adaptive Reaktion** für die bessere Abwehr komplexer Bedrohungen durch eine einheitliche Verteidigungsstrategie innerhalb des gesamten Sicherheitsökosystems

Moderne Cyber-Angriffe sind äußerst raffiniert, die Zahl der APT-Bedrohungen nimmt zu und es wird immer wichtiger, Unternehmensrisiken laufend zu behandeln. Unternehmen sind daher gezwungen, ihr gesamtes Sicherheitsökosystem neu zu bewerten. Es ist äußerst wichtig, dass Sicherheitsanalysen eine detaillierte Analyse von Informationen über Benutzer, Angriffe, Kontext, Uhrzeit und Standort enthalten, die aus Identitätssystemen, Endpunkten, Servern, Apps, Web- und E-Mail-Servern sowie speziellen Systemen stammen.

Die zunehmende Verbreitung von Cloud- und Hybridverteilungen sowie mobilen Arbeitslasten verstärkt die Notwendigkeit, Einblicke in Cloud-Services und -Anwendungen zu bekommen. Dazu sind eine dynamische Infrastruktur und eine anwendungsweite Sicht auf Aktivitäten erforderlich, um interne und externe Bedrohungen in Echtzeit erkennen, untersuchen und abwehren zu können.

Splunks analysegestützte Sicherheitslösungen bieten einen umfassenden Ansatz für Cyber-Sicherheit mit komplexen Verfahren wie Machine Learning und verhaltensbasierter Analyse. Mithilfe dieser Verfahren können Sicherheitsteams Bedrohungen schnell erkennen, untersuchen und abwehren, da sie auf einem breiteren Sicherheitskontext basieren als traditionelle Sicherheitsprodukte. Splunk-Lösungen können lokal, in der Cloud oder in einem Hybrid-Modell verteilt werden.

Splunk als Nervenzentrum

Bei der Adaptive Response Initiative von Splunk werden Maschinendaten aus dem gesamten Sicherheitsökosystem genutzt, um Informationen über Technologien hinweg zu kombinieren. Dies verbessert das Sicherheitsniveau eines Unternehmens, da Bedrohungen schnell geprüft werden und die Kill Chain systematisch unterbrochen wird. Dieses Modell vereint Benachrichtigungen und Bedrohungsinformationen aus verschiedenen Sicherheitsbereichen und -technologien. Durch die Summe der gewonnenen Erkenntnisse sind bessere Entscheidungen für die gesamte Kill Chain möglich. Dies gilt besonders beim Prüfen von Bedrohungen und der Anwendung analysegestützter Reaktionsanweisungen an Sicherheitsumgebungen.

Erkennung interner Bedrohungen

Profitieren Sie von der automatischen Erkennung von Insider-Bedrohungen mittels Machine Learning, Basiswerten für das Normalverhalten sowie Peer-Gruppen- und Verhaltensanalysen.

Erkennung komplexer Bedrohungen

Nutzen Sie die Kill Chain-Analyse, um die verschiedenen Phasen einer komplexen Bedrohung nachzuvollziehen, die Sequenz der Ereignisse festzustellen und gezielte Abwehrmaßnahmen zu definieren.

Betrugserkennung und -untersuchung

Erkennen, untersuchen und berichten Sie verschiedenste Betrugs-, Diebstahls- und Missbrauchsaktivitäten in Echtzeit. Splunk ergänzt vorhandene Betrugsbekämpfungs-Tools durch das Indizieren von Ereignisdaten, um eine unternehmensweite Sicht auf Betrugsaktivitäten sowie eine konsolidierte Betrugseinstufung für eine einzelne Transaktion zu erhalten.

SIEM

Verwenden Sie diese Lösung für SIEM-Anwendungsfälle in Unternehmen wie Vorfallsüberprüfung, Unterstützung für das Incident-Management, die Erstellung von Analysen und Verhaltensprofilen, Erheben von Bedrohungsinformationen und Ad-hoc-Suchen. Große Unternehmen nutzen Splunk für eine breite Palette von Informationssicherheitsvorgängen, wie Beurteilung des Sicherheitsniveaus, Monitoring, Benachrichtigungen und Bewältigung von Sicherheitsvorfällen, CSIRT, Analyse und Reaktion bei Sicherheitsverletzungen und Ereigniskorrelation. Splunk kann als SIEM eingesetzt werden, um SOCs (Security Operations Center) beliebiger Größe zu unterhalten.

Schnelle Untersuchung von Vorfällen

Durch die Zusammenarbeit können SOC-Analysten und Abwehrexperten innerhalb eines Unternehmens schnell Vorfälle untersuchen, indem sie Ad-hoc-Suchen mit bestehenden Korrelationen auf der Basis aller sicherheitsrelevanten Daten durchführen. Sie können Verlaufsdaten nutzen, um die grundlegende Ursache und die nächsten Schritte festzustellen.

Compliance-Reporting

Erstellen Sie Korrelationsregeln und Berichte, um Gefahren für sensible Daten oder Mitarbeiter an Schlüsselpositionen festzustellen und automatisch die Compliance zu belegen oder Bereiche aufzuzeigen, in denen keine ausreichenden technischen Kontrollen durchgeführt werden, wie etwa: PCI, HIPAA, FISMA, GLBA, NERC, SOX, EU-Datenschutzrichtlinie, ISO, COBIT und die CIS Top 20.

Log-Management

Sie können beliebige sicherheitsrelevanten Maschinendaten konsolidieren, erfassen, speichern, indizieren, durchsuchen, korrelieren, visualisieren, analysieren und in Berichten zusammenstellen, um sicherheitsrelevante Probleme schnell zu identifizieren und zu beheben. Ad-hoc-Abfragen und -Berichte auf der Basis historischer Daten sind ohne Reporting-Software von Drittanbietern möglich. Die Splunk-Software unterstützt die Log-Datenveredelung, indem sie flexibel Zugriff auf relationale Datenbanken, durch Feldtrennzeichen strukturierte Daten in CSV-Dateien (Comma Separated Value) oder andere Unternehmensdatenspeicher wie Hadoop oder NoSQL ermöglicht.

Testen Sie Splunk Enterprise Security Überzeugen Sie sich von der Leistungsfähigkeit von Splunk Enterprise Security, ganz ohne Downloads, Hardwareeinrichtung oder Konfiguration. Mit der Online-Sandbox für Splunk Enterprise Security erhalten Sie 7 Tage lang Zugriff auf eine Testumgebung mit bereits vorhandenen Daten in der Cloud, in der Sie Daten durchsuchen, visualisieren und analysieren sowie Vorfälle aus verschiedensten Sicherheitsbereichen eingehend untersuchen können. Sie können auch die schrittweise Anleitung durchgehen, um die mit der Splunk-Software möglichen leistungsfähigen Visualisierungen und Analysen kennen zu lernen. **Erfahren Sie mehr.**

SplunkCe@Splunk.com www.splunk.com