ArcSight Logger

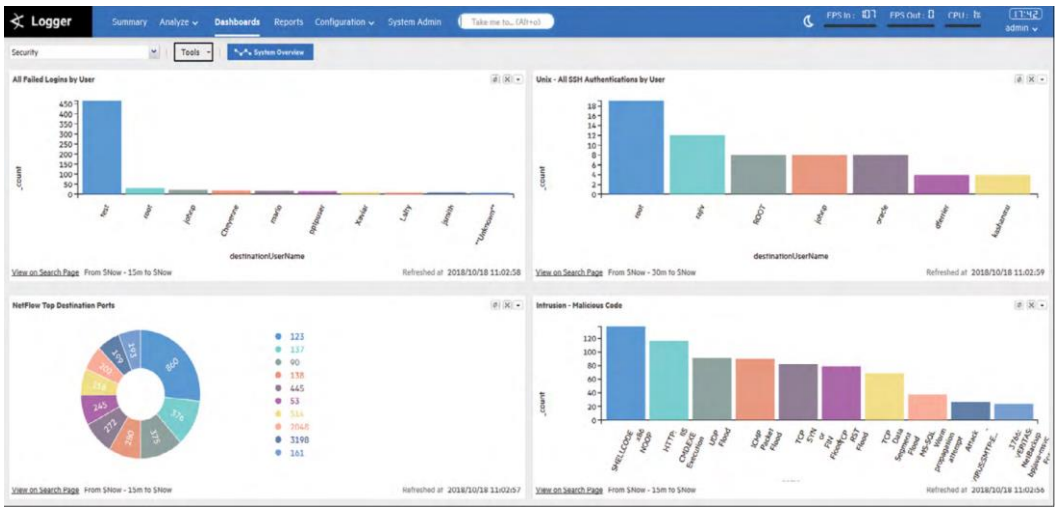
Vereinheitlichen Sie die Erfassung, Speicherung und Analyse von Maschinendaten für Security Intelligence. Micro Focus ArcSight Logger ist eine branchenführende Datenerfassungslösung, die gleichzeitig die Anforderungen an Cybersicherheit, Compliance und IT Operations Log Management erfüllen kann, während Ihr Unternehmen wächst.

Produkt Highlights

Mit der Zunahme von Bedrohungen der Cybersicherheit wurden zentralisierte Maschinendatenprotokolle schnell zu einer wichtigen Informationsquelle. Heute spielt eine effektive Protokollverwaltung eine wichtige Rolle bei der Durchführung aufschlussreicher Sicherheitsanalysen.

ArcSight Logger ist eine umfassende Log-Management-Lösung, die Sicherheitsexperten den Aufwand für die Einhaltung von Vorschriften erleichtert und eine schnellere forensische Untersuchung ermöglicht, indem sie Maschinendatenprotokolle aus dem gesamten Unternehmen vereinheitlicht speichert und eine schnelle Suche und Berichterstattung über diese Daten ermöglicht. ArcSight Logger spielt eine wichtige Rolle bei der Mission von ArcSight, leistungsstarke mehrschichtige Analysen zu liefern und grundlegende Sicherheitsoperationen zu etablieren.

Logger ermöglicht es Unternehmen, Datenprotokolle aus über 480 Quellen zu erfassen und dank seiner beeindruckenden, kosteneffizienten Komprimierungsrate über Jahre hinweg in einem sauberen, normalisierten Format zu speichern. Logger kann nicht nur Millionen (sogar Milliarden) von Ereignissen pro Tag aufnehmen und speichern, sondern auch Sicherheitsexperten dabei helfen, diese Daten effizient zu nutzen, um Anomalien aufzudecken und schnelle forensische Untersuchungen durch vereinfachte Suche und anpassbare Dashboards durchzuführen.



Logger wird mit integrierten Inhalten, Dashboards und Berichten geliefert, die die Einhaltung von Sicherheitsvorschriften ohne Unterbrechung erleichtern. Es sind auch Inhaltspakete erhältlich, die die Einhaltung von PCI, SOX, HIPAA und anderen Vorschriften erleichtern. Dies vereinfacht die Durchführung von Audits und verkürzt die Zeit, die Sie benötigen, um nachzuweisen, dass Sie die relevanten Vorschriften und Anforderungen einhalten.

Lösung

IT-Security Management

Produkt

ArcSight Logger

Highlights

- Kostengünstige Speicherung und Suche in Terabytes von Daten mit schneller, verteilter Peer-Suche
- Umfassende Datenerfassung
- Flexible Einsatzarchitektur
- Sicher und zuverlässig
- Ultraschnelle Suche und Untersuchung
- Non-stop compliance
- Einfache Bereitstellung und Verwaltung
- Dateninhaltsanalyse mit maschinellem Lernen

Die wichtigsten Vorteile

Umfassende Datenerfassung: ArcSight Logger sammelt Maschinendaten mit Aufnahmeraten von Terabytes an Daten pro Tag aus beliebigen Quellen (einschließlich Logs, Clickstreams, Sensoren, Stream-Netzwerkverkehr, Sicherheitsgeräte, Webserver, benutzerdefinierte Anwendungen, sozialen Medien und Cloud-Dienste). Sie können die Daten durchsuchen, überwachen und analysieren, um wertvolle Sicherheitsinformationen über Ihr gesamtes Unternehmen zu erhalten.

Flexible Bereitstellungsarchitektur: ArcSight Logger kann als Cluster konfiguriert werden, der eine lastverteilte Sammlung bietet, wobei die Suchanfragen über die Plattform verteilt werden. Er kann auf einem Linux-System, einer VMware Virtual Machine (VM), als Appliance und in der Cloud (AWS und Azure) installiert werden. ArcSight Logger kann lokale Laufwerke oder eine bestehende SAN-Investition als primären Datenspeicher nutzen. Unabhängig davon, ob der Speicher on- oder off-board ist, werden die Daten effizient komprimiert, um die Speicher- und Wartungskosten zu reduzieren.

ArcSight nutzt das Common Event Format (CEF), ein erweiterbares, textbasiertes, leistungsstarkes Format, so dass Daten leicht gesammelt und für die Analyse durch ein Unternehmensmanagementsystem wie ArcSight ESM, ArcSight Investigate, Interset UEBA oder eine Anwendung eines Drittanbieters aggregiert werden können, die Ereignisorchestrierung, Automatisierung, Korrelation, Priorisierung, Analyse von Sicherheitsereignissen oder alle der oben genannten Punkte bietet.

Ultraschnelle Ermittlungen und Forensik: Wenn Sekunden den Unterschied zwischen einem erfolgreichen oder vereitelten Angriff bedeuten, ist es entscheidend, die richtigen Informationen zur richtigen Zeit zu erhalten. ArcSight Logger ermöglicht eine ultraschnelle Untersuchung indizierter Daten über eine einfache Suchoberfläche. Interessante Suchmuster können leicht in Echtzeit-Warnungen umgewandelt werden. Logger beschleunigt außerdem Ihre Untersuchung mit maschinell lernenden Data-Science-Inhalten. Verwenden Sie vorgefertigte Inhalte oder entwickeln Sie Ihre eigenen Data-Science-Algorithmen mit Python-Skripten. ArcSight Logger bietet eine Ad-hoc-Suche von Milliarden von Ereignissen in weniger als 10 Sekunden über Jahre von Daten, was Ihnen die Identifizierung von Sicherheitsverletzungen und die Durchführung detaillierter Analysen von Sicherheitsverletzungen ermöglicht.

Non-Stop-Compliance: ArcSight Logger verfügt über integrierte Inhalte, die für Cybersicherheit, Compliance, Anwendungssicherheit und IT-Betriebsüberwachung verwendet werden können. Zusätzliche Compliance-Inhaltspakete für PCI, ITGOV, HIPAA, NERC und Sarbanes-Oxley (SOX) sind als Zusatzoptionen erhältlich und werden auf bekannte Standards abgebildet, darunter National Institute of Standards and Technology (NIST) 800-53, ISO-17799, und SANS.

Warum ArcSight?

Die ArcSight SIEM-Plattform der nächsten Generation ist skalierbar und leistungsstark. Es handelt sich um eine umfassende Lösung, die von Sicherheitsexperten für Sicherheitsexperten entwickelt wurde. Sie verfolgt einen ganzheitlichen Ansatz für Security Intelligence und vereint auf einzigartige Weise Big Data-Erfassung, Netzwerk-, Benutzer- und Endpunktüberwachung sowie Forensik mit fortschrittlichen Sicherheitsanalysetechnologien, einschließlich Hunt-, Untersuchungs- und UEBA-Lösungen. Die Lösung bietet Echtzeit-Bedrohungserkennung und -Reaktion, Compliance-Automatisierung und -Gewährleistung sowie IT-Betriebsintelligenz.

ArcSight

Lösung

IT-Security Management

Produkt

ArcSight Logger

Highlights

- Kostengünstige Speicherung und Suche in Terabytes von Daten mit schneller, verteilter Peer-Suche
- Umfassende Datenerfassung
- Flexible Einsatzarchitektur
- Sicher und zuverlässig
- Ultraschnelle Suche und Untersuchung
- Non-stop compliance
- Einfache Bereitstellung und Verwaltung
- Dateninhaltsanalyse mit maschinellem Lernen