ArcSight Intelligence Verhaltensanalytik

Die Verhaltensanalyse von Micro Focus ArcSight Intelligence gibt Ihnen ein neues Tools an die Hand, mit dem Sie Bedrohungen, die sich in Ihrem Unternehmen verstecken könnten, erkennen, untersuchen und darauf reagieren können - bevor Ihre Daten etwas zustößt.

Warum ArcSight Intelligence

Mithilfe von maschinellem Lernen verarbeitet ArcSight Intelligence Milliarden von Ereignissen zu einer priorisierten Liste hochwertiger Sicherheitshinweise, um die Bemühungen Ihres Security Operations Center (SOC) zu konzentrieren und zu beschleunigen. Die maschinellen Lernmodelle von ArcSight Intelligence, kombiniert mit einer äußerst intuitiven Benutzeroberfläche, beschleunigen die Erkennung und Untersuchung von Bedrohungen von Wochen auf Minuten.

Viele Unternehmen haben wichtige Ressourcen zu schützen, seien es Kundendaten, geistiges Eigentum, kritische Infrastrukturkontrollen oder all diese genannten Faktoren. Leider sind die bestehenden Ansätze zum Schutz dieser Ressourcen immer wieder unzureichend, so dass die Sicherheitsteams mit starren, regelbasierten Analysen, fragmentierten Sicherheitsökosystemen und einer nicht enden wollenden Flut von Warnmeldungen zu kämpfen haben - von denen die meisten dann sogar auch meistens Fehlalarme sind. Gleichzeitig wird von diesen Teams erwartet, dass sie sich einwandfrei gegen kritische Bedrohungen wie Datenexfiltration und unbefugten Netzwerkzugriff schützen.

ArcSight Intelligence ist einzigartig positioniert, um die Bedrohungen zu finden, die für Unternehmen von Bedeutung sind, die wertvolle Daten zu schützen haben, deren Sicherheits- oder Finanzressourcen begrenzt sind und die eine große Fläche überwachen müssen. Im Gegensatz zu anderen Lösungen umgeht ArcSight Intelligence Regeln und Schwellenwerte und bewertet stattdessen das potenzielle Risiko eines Benutzers oder einer Entität in Ihrem Unternehmen auf der Grundlage mathematischer Wahrscheinlichkeiten und unüberwachter maschineller Lernmodelle. Dieser Ansatz, kombiniert mit der nativen Big-Data-Architektur von ArcSight Intelligence, ermöglicht es Ihrem Sicherheitsteam, Bedrohungen schnell und in großem Umfang zu erkennen.

Insider Thread

- Gefährdete Mitarbeiter
- Hochgefährdete Mitarbeiter
- Konto-Missbrauch
- Privilegierter Kontomissbrauch
- Entlassene Mitarbeiter Aktivität

Data Breach

- Daten-Staging
- Exfiltration von Daten
- E-Mail-Exfiltration
- Druck-Exfiltration
- USB-Exfiltration
- Ungewöhnlicher Datenzugriff
- Ungewöhnliche Uploads

Advanced Threat

- Kompromittierte Konten
- Interne Überwachung
- Ungewöhnlicher Traffic
- Ungewöhnliche Prozesse
- Ungewöhnliche Anwendungen
- Infizierte Hosts
- Bösartiges Tunneling
- Bot-Erkennung

IP Diebstahl

- Mooching
- Snooping
- Interaktionen mit ruhenden Ressourcen/Dateien
- IP-/Datenzugriff mit hohem Risiko
- Laterale Bewegung

ArcSight Intelligence verwendet fortschrittliche mathematische Algorithmen, um ständig Milliarden von Datenpunkten zu analysieren und Indikatoren für Insider-Bedrohungen, Datenschutzverletzungen, fortgeschrittene anhaltende Bedrohungen (APT), IP-Diebstahl und vieles mehr aufzudecken.

Lösung

IT-Security Management

Produkt

ArcSight Intelligence

Highlights

Bietet fortschrittliche Bedrohungserkennung zur Unterstützung von Insider-Bedrohungsprogrammen zum Schutz vor IP- und Datendiebstahl.

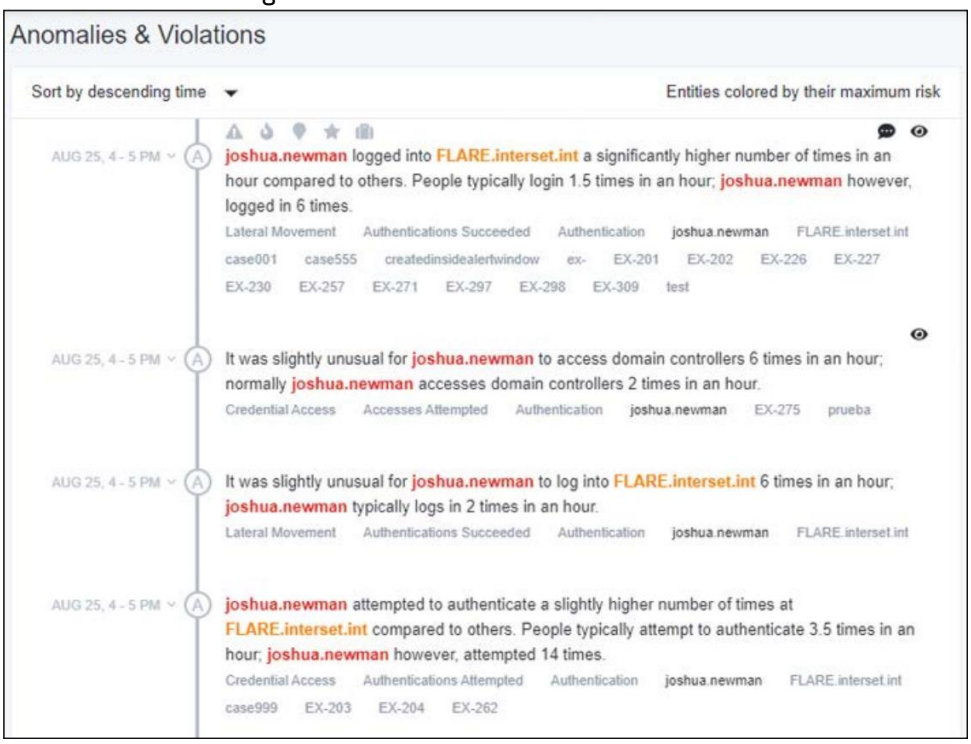
Flexible Bereitstellungen zur Bedrohungsjagd vor Ort, in der privaten Cloud, als SaaS und SaaS mit Integration von CrowdStrike Falcon.

Senkung der Sicherheitskosten durch Verbesserung der Effizienz von Analysten und Automatisierung manueller Aufgaben bei der Suche nach Bedrohungen durch Sicherheits-KI.

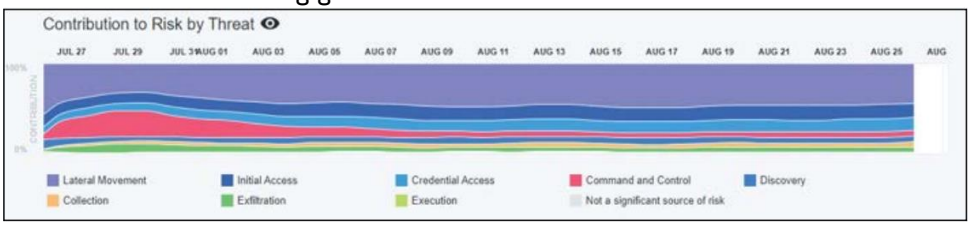
Ein kurzer Einblick in die Lösung

Mithilfe von unüberwachtem maschinellen Lernen - einer Art von künstlicher Intelligenz (KI), die keine Label benötigt - extrahieren die Algorithmen von ArcSight Intelligence verfügbare Entitäten (Benutzer, Maschinen, IP-Adressen, Server, Drucker usw.) aus den Protokolldateien und beobachten Ereignisse, die diese Entitäten betreffen, um das erwartete Verhalten zu bestimmen - eine Messung, die als "einzigartig normal" bezeichnet wird. Wenn neue Informationen in den Analyseprozess einfließen, werden die Ereignisse ausgewertet.

1. Zeigen Sie alle Entitäten innerhalb des Unternehmens an, deren Analysen angezeigt werden sollen, gruppiert nach Entitätstyp. Der Screenshot zeigt die Darstellung eines Benutzers und die aufgetretenen Anomalien und Verstöße



2. Bei der Betrachtung einer Entität wird ihr Risikowert im Zeitverlauf in einer Zeitleistenansicht angezeigt. Diese Perspektive zeigt nicht nur die Veränderung des Risikowertes, sondern auch eine umfassende Beschreibung der Verhaltensweisen, die zu dieser Veränderung geführt haben.



ArcSight

Lösung

IT-Security Management

Produkt

ArcSight Intelligence

Highlights

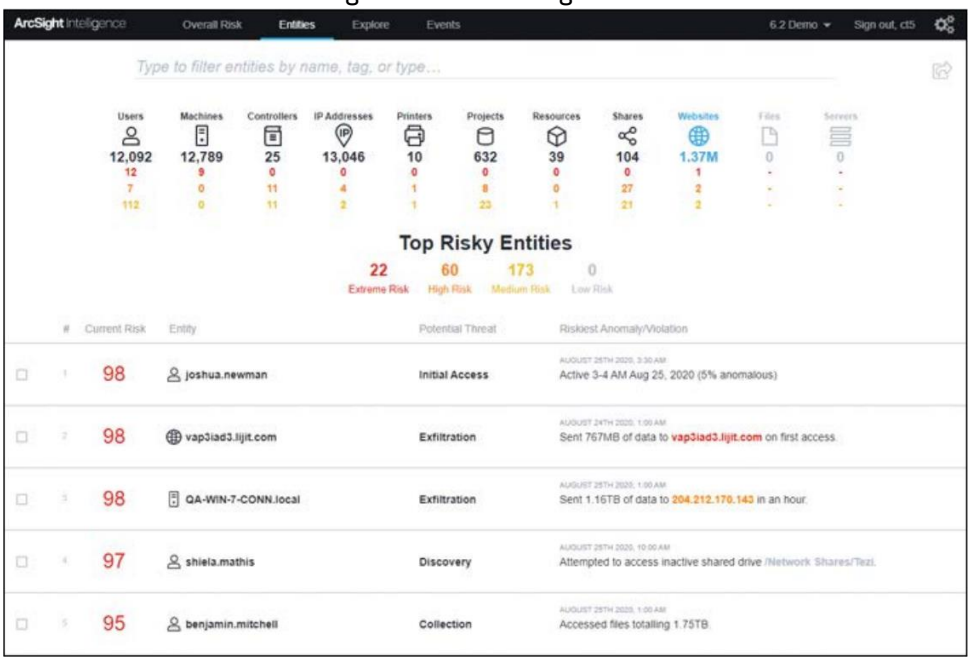
Bietet fortschrittliche Bedrohungserkennung zur Unterstützung von Insider-Bedrohungsprogrammen zum Schutz vor IP- und Datendiebstahl.

Flexible Bereitstellungen zur Bedrohungsjagd vor Ort, in der privaten Cloud, als SaaS und SaaS mit Integration von CrowdStrike Falcon.

Senkung der Sicherheitskosten durch Verbesserung der Effizienz von Analysten und Automatisierung manueller Aufgaben bei der Suche nach Bedrohungen durch Sicherheits-KI.

Ein kurzer Einblick in die Lösung

3. Bei der Anzeige einer Entität werden die mit der Entität verbundenen Warnungen unterhalb der Zeitleistenansicht angezeigt. Sie können nach zugehörigen Entitäten und Risikotypen gefiltert werden, und da sie in chronologischer Reihenfolge in Verbindung mit der Zeitleiste angezeigt werden, ist es einfach, die Entwicklung des Verhaltens im Zusammenhang mit anderen Ereignissen zu sehen.



4. Ein Klick auf einen der Alarme ermöglicht eine Untersuchung, die das Ereignis im Kontext der Baseline des Benutzers und anderer relevanter Entitäten im Unternehmen zeigt. Das mit der Warnung verbundene Risiko wird angezeigt, und das Modell, das die Warnung ausgelöst hat, wird detailliert beschrieben. Beachten Sie, dass die Baseline des Benutzers sowohl mit sich selbst als auch mit anderen ähnlichen Entitäten verglichen wird. Diese ähnlichen Unternehmen werden durch statistische Peer-Gruppen ermittelt.

Lösung

IT-Security Management

Produkt

ArcSight Intelligence

Highlights

Bietet fortschrittliche Bedrohungserkennung zur Unterstützung von Insider-Bedrohungsprogrammen zum Schutz vor IP- und Datendiebstahl.

Flexible Bereitstellungen zur Bedrohungsjagd vor Ort, in der privaten Cloud, als SaaS und SaaS mit Integration von CrowdStrike Falcon.

Senkung der Sicherheitskosten durch Verbesserung der Effizienz von Analysten und Automatisierung manueller Aufgaben bei der Suche nach Bedrohungen durch Sicherheits-KI.