FIREMON

PROACTIVE SECURITY INTELLIGENCE

www.firemon.de

IMMEDIATE INSIGHT

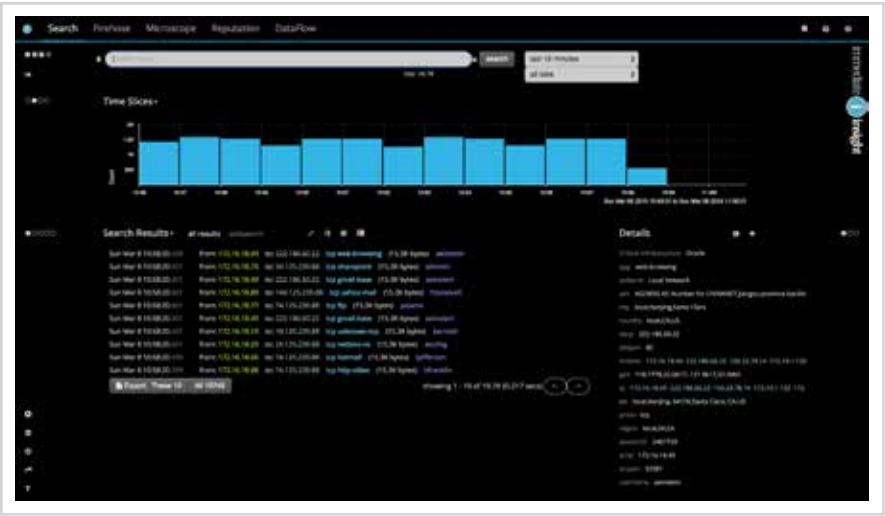
IT-Datenanalysen in Echtzeit

Die Antworten auf viele der heutigen Sicherheitsvorfälle und Betriebsstörungen liegen in Ihren Daten. Die Erfassung und Analyse von Daten von Geräten, Systemen und Anwendungen in einem Unternehmensnetzwerk ist jedoch ein zeitintensives und kostspieliges Unterfangen – besonders für kleine IT-Teams mit wenigen Mitarbeitern. Ohne ein gutes Verständnis dieser Daten können Netzwerkbedrohungen und Serviceprobleme unerkannt und ungelöst bleiben.

Immediate Insight von FireMon sammelt und korreliert alle IT-Daten, damit Analysten und Betriebsteams die Datentransparenz steigern und den Zeit- und Arbeitsaufwand für die Priorisierung von Vorfällen reduzieren können.

WAS IST IMMEDIATE INSIGHT?

Mit Immediate Insight lassen sich Daten so schnell und einfach wie mit Google analysieren und erfassen. Es vereint Maschinenlernen, Korrelation und eine natürliche Sprache in einer einfachen Workflow-basierten Oberfläche und macht Zusammenhänge zwischen Daten sichtbar, von denen die Benutzer noch nicht einmal wussten, dass sie überhaupt existieren. Es bringt Unternehmen dazu, sich von der Denkweise „Daten als letzte Rettung" zu verabschieden und eine „Daten zuerst"-Vorgehensweise zu verfolgen, die zur Verbesserung von Sicherheit, Performance und Betrieb erforderlich ist.



Die Datensilo-übergreifende Echtzeitanalyse von Immediate Insight bietet eine zeitnahe und umfassende Transparenz, die erforderlich ist, um:

- verdächtige Vorkommnisse zu identifizieren und zu untersuchen
- nach Anzeichen für eine Sicherheitsverletzung und nach betrieblichen Ineffizienzen zu suchen
- eine Echtzeitanalyse der Sicherheitsdaten durchzuführen
- die Behebung von Vorfällen zu beschleunigen und Eskalationen einzudämmen
- Datensilos automatisch zu verbinden und zueinander in Beziehung zu setzen
- Daten für die Analyse durch die Eskalationsteams bereitzustellen

VORTEILE VON IMMEDIATE INSIGHT

Erkennen Sie rasch Probleme, die Sicherheit und Leistung beeinträchtigen, indem Sie Daten aus mehreren Quellen analysieren.

IMMEDIATE INSIGHT:

- Liefert Ihnen Informationen zu Ihren Daten, über die Sie sich zuvor nicht bewusst waren
- Läuft in Echtzeit – ermöglicht die Suche und Anzeige von aktuellen Daten
- Ist einfach zu bedienen – Suchanfragen in natürlicher Sprache und mit „Point-and-Click"-Funktionalität
- Reichert Daten automatisch an, um nicht offensichtliche Beziehungen kenntlich zu machen
- Vereinfacht die Datenerfassung erheblich – ganz ohne Parsing

FUNKTIONEN:

- Datenerfassung und -analyse in Echtzeit
- Datenassoziation, Clustering und Vergleichsanalysen
- Interne Reputations-Engine
- Daten-Tags für zusätzlichen individuellen Kontext
- Pinnwand für gespeicherte Suchanfragen

MEHR INFORMATIONEN ZU IMMEDIATE INSIGHT: WWW.FIREMON.DE

LÖSUNGSÜBERSICHT

DATENERFASSUNG

Immediate Insight sorgt für eine einfache und flexible Datenerfassung, damit sich Analysten auf die Identifizierung und Behebung von Problemen konzentrieren können, anstatt die Daten erst erfassen und vorbereiten zu müssen.

- Automatische Ausgabe von strukturierten und unstrukturierten Datenströmen
- Datenimport nach Bedarf über eine Drag-and-drop-Schnittstelle
- Eliminierung der Notwendigkeit des Parsing durch natürliche Sprachtechnologien

ANALYSE DER DATEN

Daten werden mithilfe sofort einsatzbereiter Analyse- und Korrelationsverfahren automatisch für die Echtzeitanalyse angereichert und optimiert. Anwender können Anomalien und nicht offensichtliche Beziehungen innerhalb großer Datensätze erkennen und einfach durch große Datenmengen navigieren. Zu den wichtigsten Merkmalen gehören:

- Übersicht der gemeinsamen Entitäten (d. h. Benutzer, Anwendungen, Netzwerke usw.)
- Automatische Gruppierung von gleichartigen Daten
- Trenderstellung für willkürliche Datengruppierungen über einen gewissen Zeitraum (neu, fehlend, aufsteigend/absteigend)
- Automatische Anwendung von lokalen, erlernten Kontexten und Reputationen als Metadaten

UNTERSUCHUNG DER DATEN

Gezielte Suchanfragen helfen den Anwendern beim Auffinden von relevanten Situationen, beim Hinzufügen von Kontext und der Reaktion auf Sicherheitsvorfälle sowie bei der Suche nach ungewöhnlichen Aktivitäten oder nach Möglichkeiten zur Verbesserung der Sicherheit und der Geschäftsabläufe – und das alles, ohne eine Abfragesprache lernen zu müssen. Es gibt fünf Standardansichten für die Suchergebnisse: detaillierte Vorfälle, Entitätszugehörigkeiten, Ereignis-Cluster, Vergleiche und Anmerkungen, Tags und Warnhinweise.

Anwender können Suchanfragen auf einer Pinnwand speichern. Für jede gespeicherte Suchanfrage können Sie:

- Volumina und Trends ansehen
- Ansichten nach beliebigen Kriterien filtern
- die Durchklickfunktion nutzen, um detaillierte Daten anzuzeigen
- auf leistungsstarke Datenanalysen in natürlicher Sprache zugreifen

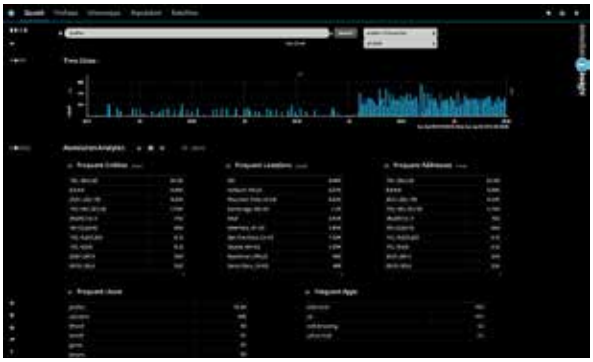
GEMEINSAME NUTZUNG DER DATEN

Dank den Funktionen und dem Workflow für die Zusammenarbeit, die die Immediate Insight-Lösung bieten, muss man nicht zu einem anderen System wechseln, um Erkenntnisse mit anderen Personen zu teilen – es wird ein virtuelles „Tiger Team“ zusammengestellt, wobei jedoch die üblichen Kosten für die physische Teambildung entfallen. Zu den wichtigsten Merkmalen gehören:

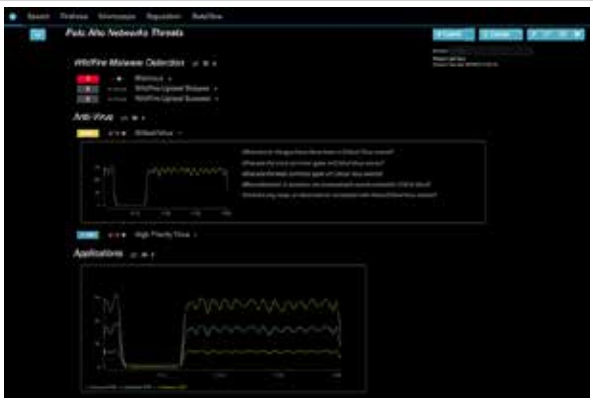
- Benutzerdefinierten Kontext (Tag) hinzufügen
- Benutzern im Stil sozialer Netzwerke folgen – lernen und beitragen

AUTOMATISIERUNG DER ANALYSE

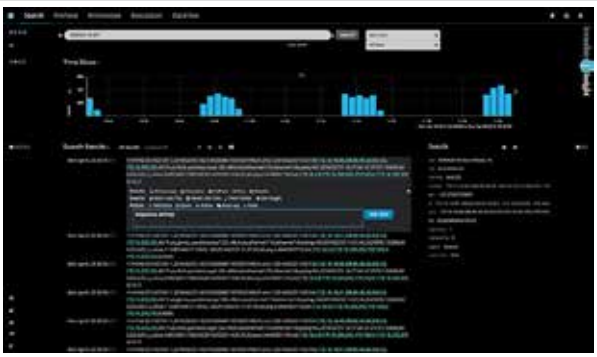
Das Workflow-System und der Datenrouter automatisieren die mehrschichtige Sicherheit oder die IT-Prozessanalyse und erstellen intelligente Aktionsrichtlinien für jeden Prozessschritt. Workflows werden über eine Drag-and-drop-Schnittstelle konfiguriert und für jeden Vorfall werden Einträge im Klartext angelegt. Diese Ereignisse werden vom Datenrouter in Echtzeit bearbeitet. Alle Workflow-Schritte werden zum Zwecke der Prozessverbesserung aufgezeichnet.



Finden von Unregelmäßigkeiten und nicht offensichtlichen Beziehungen zwischen den Daten in Echtzeit



Für jede Suche ist Folgendes möglich: Anzeige von Volumina und Trends, Filterung der Ansicht nach beliebigen Kriterien und Nutzung der Durchklickfunktion, um detailliertere Daten anzuzeigen



Die in die Software integrierten Kollaborations-Tools ermöglichen die Markierung von Daten, das Folgen von Nutzern, das Teilen von Suchanfragen und vieles mehr.

FIREMON

Erfahren Sie mehr über unsere Lösungen:
www.firemon.de

8400 W. 110th Street, Suite 500
Overland Park, KS 66210 USA
Tel.: +1 913 948 9570 E-Mail: info@firemon.com

©Copyright FireMon, LLC 2015

REV 052715