Advanced Reporting Tool

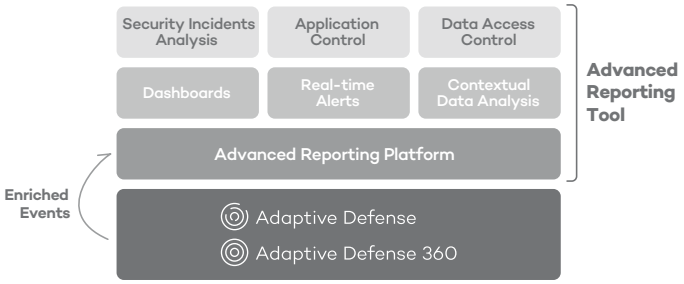
Interne und externe Sicherheitslücken gezielt erkennen und bekämpfen

In zunehmendem Maße werden in Unternehmen täglich große Mengen an – teilweise hochsensiblen – Daten generiert und verarbeitet. Ohne einen umfassenden Überblick über die IT-Infrastruktur und die dort laufenden Prozesse droht den IT-Abteilungen schnell die Gefahr, wichtige Einzelheiten zu übersehen und dabei die Sicherheit des gesamten IT-Systems zu gefährden.

Gezielt aufbereitet und analysiert können Informationen zu laufenden Prozessen genutzt werden, um Sicherheitsvorfälle in Firmen-Netzwerken zu entdecken und zu verfolgen, egal, ob sie von außen kommen oder von Insidern verursacht werden.

Die Lösung: Adaptive Defense mit integriertem Advanced Reporting Tool

Die Advanced Reporting Plattform automatisiert die Speicherung und den Abgleich der von Adaptive Defense gewonnenen Prozessdaten. Mit Hilfe dieser Daten können IT-Administratoren mit nur einem Klick detaillierte Sicherheitsinformationen generieren. So werden Angriffe und ungewöhnliche Verhaltensmuster festgestellt sowie der interne Missbrauch der Firmennetzwerke und -systeme erkannt.



Mit nur einem Klick ziehen Sie mit dem Advanced Reporting Tool detaillierte Rückschlüsse aus dem IT- und Sicherheitsmanagement des Unternehmens. Auf dieser Grundlage kann dann ein Aktionsplan mit nachfolgenden Punkten definiert werden:

- Bestimmung des Ursprungs von Sicherheitsbedrohungen, um zukünftige Angriffe zu verhindern
- Implementierung von restriktiven Richtlinien für den Zugriff auf wichtige Firmendaten
- Überwachung und Kontrolle des Missbrauchs von Unternehmensressourcen
- Korrektur des Mitarbeiterverhaltens, sofern diese sich nicht an die festgelegten Nutzungsrichtlinien halten

Hauptvorteile

1. Finden Sie relevante Informationen

Maximieren Sie Ihren Einblick in alle auf den Endpoints und Servern laufenden Prozesse und erhöhen Sie die Effizienz und Produktivität der IT-Abteilung.

Greifen Sie auf Protokolldaten zu, um die Sicherheit der Firmenressourcen und Nutzungsindikatoren zu analysieren.

Erhalten Sie detaillierte Informationen, um Sicherheitsrisiken sowie den Missbrauch der IT-Infrastruktur durch Insider zu identifizieren.

2. Diagnostizieren Sie Netzwerkprobleme

Reduzieren Sie die Anzahl der benötigten Tools und Datenquellen, um zu verstehen, was auf den Netzwerkgeräten passiert und welche Bedeutung dies für die Sicherheit und die Nutzung der Vermögenswerte Ihres Unternehmens hat.

Gewinnen Sie Informationen über die Ressourcennutzung und die Verhaltensmuster von Anwendern, um ihren potenziellen Einfluss auf das Unternehmen zu demonstrieren.

3. Seien Sie wachsam

Wandeln Sie entdeckte Anomalien in Echtzeit-Warnungen und Reports um.

Identifizieren Sie Sicherheitsabweichungen sowie den Missbrauch von IT-Ressourcen durch Mitarbeiter.

4. Horizontale und vertikale Informationen

Generieren Sie individuell konfigurierbare Reports, um methodische Analysen des Sicherheitsstatus Ihres Unternehmens durchzuführen und den Missbrauch von Vermögenswerten sowie Verhaltensanomalien festzustellen.

Analysieren Sie den Status wichtiger Sicherheitsindikatoren und verfolgen Sie deren Entwicklung zur Evaluierung der eingeführten Korrekturmaßnahmen.

Advanced Reporting Tool

FLEXIBLE, INDIVIDUELL ANGEPASSTE ANALYSEN

Das Advanced Reporting Tool enthält Dashboards mit Schlüsselindikatoren, Suchoptionen und Standardwarnmeldungen für drei zentrale Bereiche:

- Sicherheitsvorfälle
- Zugriff auf wichtige Informationen
- Nutzung von Anwendungen und Netzwerkressourcen

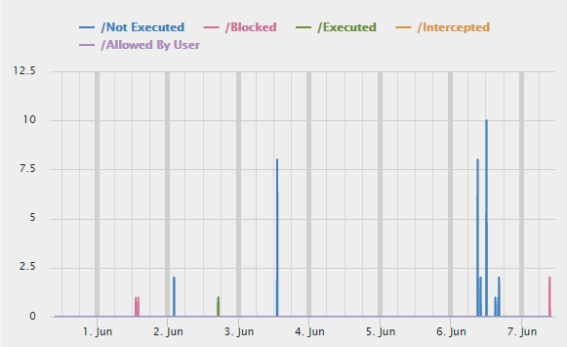
Suchvorgänge und Warnmeldungen können dabei an die individuellen Gegebenheiten Ihres Unternehmens angepasst werden.

INFORMATIONEN ÜBER SICHERHEITSVORFÄLLE

Generieren Sie detaillierte Sicherheitsinformationen, indem Sie die während der Angriffsversuche aufgetretenen Ereignisse zeitnah verarbeiten und abgleichen.

Die Zeitleisten im Advanced Reporting Tool zeigen Ihnen

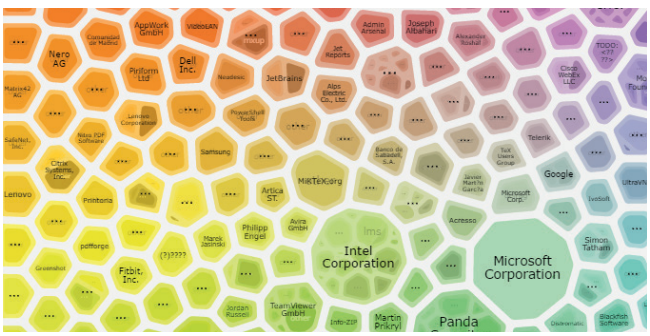
- Malware und PUPs, die in den vergangenen Jahren entdeckt wurden.
- Computer mit den meisten Infektionsversuchen und entdeckten Malware-Exemplaren.
- Malware-Ausführungsstatus auf Netzwerkcomputern.
- Computer mit gefährdeten Anwendungen.



KOSTENSENKUNG

Analysieren Sie die Nutzungsmuster Ihrer IT-Ressourcen, um Kostensenkungspotentiale zu definieren und durchzusetzen:

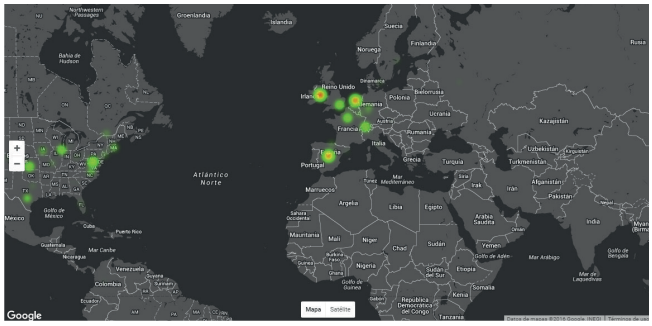
- Identifikation von Unternehmens- und Nicht-Unternehmensanwendungen in Ihrem Netzwerk
- Überblick über genutzte versus erworbene Lizenzen
- Anwendungen mit der höchsten Bandbreitennutzung
- Übersicht über Anwendungen, die im Netzwerk installiert wurden und möglicherweise zu Infektionen führen und somit Auswirkungen auf die Unternehmensleistung haben bzw. Wiederherstellungskosten verursachen



ZUGRIFFSKONTROLLE AUF GESCHÄFTSDATEN

Das Advanced Reporting Tool zeigt den Zugriff auf vertrauliche Dateien sowie Datenlecks im Netzwerk. Folgende Informationen können dabei abgerufen werden:

- Länder, zu denen die meisten Verbindungen von Ihrem Netzwerk hergestellt werden
- Dateien, die am häufigsten abgerufen und ausgeführt werden
- Zugriff auf bestimmte Netzwerkcomputer
- Detaillierte Informationen zum Datenversand (Aufbereitung in einer Timeline)



ECHTZEIT-WARNUNGEN

Konfigurieren Sie Warnmeldungen für mögliche Sicherheitsverletzungen oder Verstöße gegen die Richtlinien für das Daten-Management:

- Standardwarnmeldungen zur Anzeige von Risikosituationen
- Unternehmensspezifische Warnmeldungen, die auf gestellten Anfragen basieren
- Direkte Informationsdarstellung mittels Bildschirmanzeige oder per E-Mail, JSON, Service Desk, Jira, Pushovery und PagerDuty

FLEXIBLER, CLOUD-BASIERTER BIG DATA SERVICE

- An die Bedürfnisse von Netzwerkadministratoren angepasst, sowohl hinsichtlich des Speicherplatzes als auch der Möglichkeit, Protokolldaten zu durchsuchen.
- Sofort einsatzbereit, da weder Änderungen am Netzwerk des Kunden noch die Installation zusätzlicher Infrastrukturen erforderlich ist.
- Konfigurierbare Umgebung, die an die individuellen Bedürfnisse Ihrer IT-Abteilung angepasst ist.

TECHNISCHE ANFORDERUNGEN

Empfohlene Browser:

- Mozilla Firefox.
- Google Chrome.

Internetverbindung und sichere Kommunikation über Port 443

Minimale Bildschirmauflösung: 1280 x 1024 (empfohlen: 1920 x 1080)

Nur in Kombination mit Adaptive Defense (360) verwendbar