# Security Incident & Event Management (SIEM)

Unbefugter Zugriff auf Daten und Systeme wird meist viel zu spät oder gar nicht bemerkt. Mehrstufige Angriffe bedienen sich auf dem Weg in die Unternehmen unterschiedlichster Kanäle – über Notebooks, Smartphones, Tablet PCs, private Geräte der Mitarbeiter oder von Unternehmen gemieteter Cloud-Dienste.

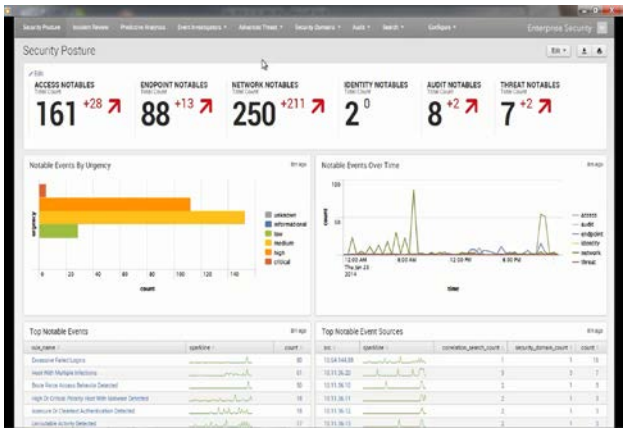
Wer SIEM-Lösungen richtig einsetzt, erschwert es Angreifern erheblich, sich unerlaubt Zugriff auf Unternehmensressourcen zu verschaffen und erhält sehr schnell die Möglichkeit, die Angriffsvektoren aufzudecken und zu schließen.

Security Incident & Event Management-Systeme (SIEM) sind in der Lage, sowohl unautorisierte Zugriffe schnell und effektiv zu erkennen als auch die Auswirkungen eines erfolgreichen Angriffs zu bewerten und Folgeschäden zu minimieren.

Eine SIEM-Lösung wertet Daten unterschiedlichster IT-Security-Systeme aus und stellt sicherheitsrelevante Log-Daten in einem einheitlichen, leicht zu interpretierenden Format bereit.

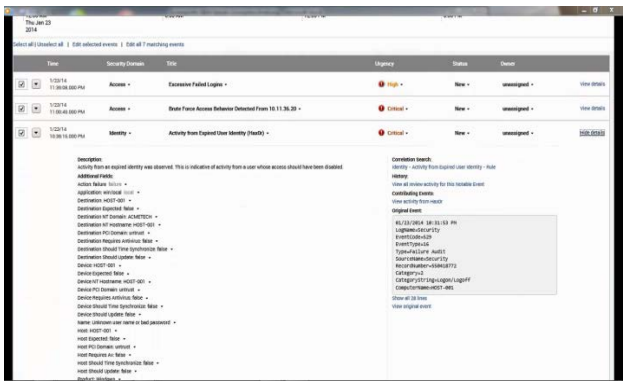
Mittels Data-Mining auf Korrelationsbasis rekonstruiert das SIEM aus der Vielzahl der Log-Daten reale Angriffsmuster, stellt diese in einer Übersicht dar und gibt Hinweise zur Risikobewertung.

Erst damit wird es überhaupt möglich, mehrstufige Angriffe als solche zu erkennen und einzelne Ereignisse, die jedes für sich betrachtet nur ein geringes Gefahrenpotential darstellen, in der Summe aber den unerlaubten Zugriff auf wichtige Systeme ermöglichen, aufzuschlüsseln und entsprechend zu bewerten.




*Übersichtliches Dashboard, Risikobewertung gemeldeter Vorfälle*

Damit entlastet ein SIEM-System die IT-Abteilung bei der Abarbeitung aufgetretener Sicherheitsvorfälle. So lässt sich beispielsweise die Gesamtanzahl dieser Ereignisse mittels intelligenter Verdichtung und Erkennung von Wechselbeziehungen signifikant reduzieren. Zudem liefert eine SIEM-Lösung der Führungsebene Statuszusammenfassungen mit grafischen Elementen und aussagekräftigen Berichten. Für spätere forensische Untersuchungen sollte eine SIEM-Lösung ebenfalls eine revisionssichere Archivierung der Daten ermöglichen.

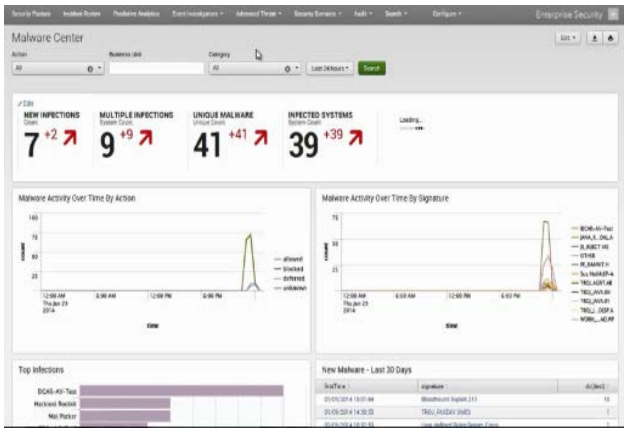


*Aktivitäten auf stillgelegten Accounts weisen auf Missbrauch hin*

## SIEM – Der Mehrwert für Ihr Unternehmen

SIEM-Lösungen sollten Ihr Unternehmen auch hinsichtlich der unterschiedlichen Compliance-Vorschriften wie ISO 2700x, PCI DSS, HIPAA, SOX, NERC und GLBA unterstützen. Die Anforderungen reichen aber wesentlich weiter. Neben dem zentralen Sammeln von Log-Daten mit mehreren 10.000 Events pro Sekunde müssen sich die Informationen dieser Ereignisse über Korrelationen in sinnvolle Aussagen überführen lassen, die einen konkreten Überblick hinsichtlich der aktuellen Sicherheitslage ermöglichen.

Die Einbettung konkreter Use Cases, wie beispielsweise die Überwachung privilegierter Accounts, das Monitoring temporärer oder stillgelegter Zugänge, sollte möglichst einfach in einer SIEM- Lösung implementiert werden können.




*Dashboard des zentralen Malware Centers zur Erfassung aller Angriffsvektoren*

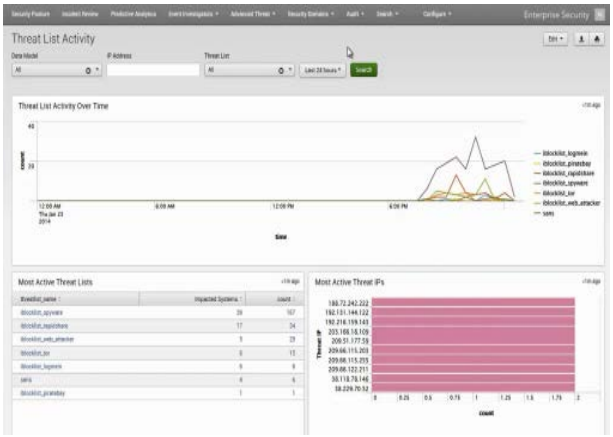
SIEM-Lösungen unterstützen Sie auch bei der Einführung eines Information Security Management Systems (ISMS), indem durch spezifische Dashboards viele IT-Security relevanten Prozesse und Arbeitsabläufe protokolliert und visualisiert werden.

So wird Ihr Unternehmen auch bei anstehenden Audits und der Umsetzung spezifischer Compliance-Anforderungen unterstützt.

Als Systemintegrator und Managed Service Provider steht Ihnen Controlware als Partner bei der Einführung einer SIEM-Lösung zur Seite.

Dies umfasst die Durchführung von Workshops in den zuständigen Fach-abteilungen, die Begleitung eines PoC, Installation, Konfiguration sowie Anpassung der Lösung an Ihre spezifischen Gegebenheiten.

Die Umsetzung von Use Cases, die nicht über Standard-Reports einer gängigen SIEM-Lösung erfasst werden, können individuell von unseren Experten implementiert werden.




*Übersicht von welchen IP-Adressen die meisten Malware-Aktivitäten ausgehen*

Haben wir Ihr Interesse geweckt?
Möchten Sie wissen, welche Rahmenparameter die erfolgreiche Einführung einer SIEM-Lösung unterstützen?
Dann sprechen Sie mit uns. Wir stellen Ihnen gerne weitere Informationen zur Verfügung.

**Zentrale**

**Controlware GmbH**
Waldstraße 92
63128 Dietzenbach

Tel. +49 6074 858-00
Fax +49 6074 858-108

info@controlware.de
www.controlware.de