PIC 2.0 SIEM

Umfassende Sicherheitsüberwachung auf einen Blick

Das Thema Informationssicherheit ist komplex und gewinnt immer mehr an Bedeutung. Ungewöhnliche Ereignisse ebenso wie aktuelle Bedrohungen bei allen verwendeten Systemen parallel zu identifizieren, um mögliche Sicherheitslücken aufzudecken und schnell reagieren zu können, erfordert ebenso viel Know-how wie Kapazitäten. Gleichzeitig führt kein Weg daran vorbei, da auch in der jüngsten Fassung der BAIT eine umfassende und regelbasierte Überwachung aller IT-Systeme gefordert und von Prüfungsverbänden sowie der BaFin verstärkt kontrolliert wird. Die gute Nachricht: Unsere neue SIEM-Lösung berücksichtigt alle bekannten regulatorischen Anforderungen, erhöht die Informationssicherheit deutlich und ist derart flexibel anpassbar, dass sie für jedes System kompatibel gestaltet werden kann.

Das Prinzip hinter SIEM (Security Information and Event Management)

Jedes IT-System speichert eine Vielzahl von sicherheitsrelevanten Informationen zu Vorfällen und Ereignissen in Log-Dateien. In komplexen IT-Umgebungen liegt die Kunst darin, alle diese Informationen einzusammeln und an einer zentralen Stelle automatisiert auszuwerten - genau das und noch einiges mehr leistet unsere SIEM-Lösung. Die PIC 2.0 SIEM-Lösung baut auf unserer Private Inhouse Cloud (PIC) auf, erfasst im gesamten Netzwerk die verschiedenen Log-Dateien und wertet diese basierend auf definierten Regeln aus. Ungewöhnliche Vorkommnisse, Abweichungen von üblichen Mustern oder versuchte Angriffe werden schnell identifiziert und die zuständige IT-Abteilung anschließend per Mail über jede auffällige Entdeckung informiert. So wird eine schnelle Reaktion ermöglicht, ohne selbst aktiv alle Systeme überwachen zu müssen.

PIC 2.0 SIEM

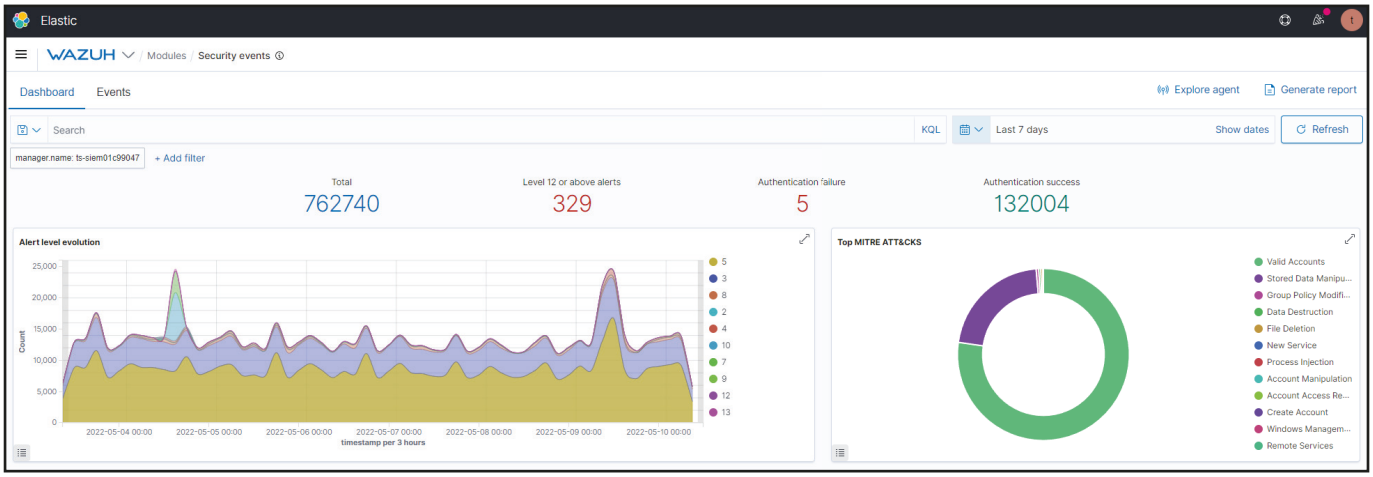
banking & network it solutions GmbH

Kompatibel und individuell anpassbar bis ins letzte Detail

Die PIC 2.0 SIEM-Lösung basiert auf der OpenSource Plattform Wazuh und bietet dadurch nicht nur ein unschlagbares Preis-Leistungs-Verhältnis, sondern ist auch sehr flexibel erweiter- und anpassbar. Die in der PIC 2.0 eingesetzten Systeme haben wir bereits in Wazuh integriert. Auch spezifische eigene Systeme können problemlos in die PIC 2.0 SIEM-Lösung aufgenommen werden. Während der umfassenden Konfiguration erfassen wir alle intern verwendeten Systeme und entwickeln eine für Sie maßgeschneiderte Lösung. So entsteht eine Datenbank, in der alle sicherheitsrelevanten Informationen zusammenlaufen, regelbasiert und automatisch ausgewertet und überwacht werden. Über unseren Software-Service erhalten Sie Zugang zu regelmäßigen Updates der Konfigurationsdateien zur Analyse und Auswertung, so dass diese stets auf dem aktuellen Stand sind.

Aktuell unterstützen wir folgende Komponenten:

- Windows Server und Clients
- Linux Server
- Sophos Firewalls (XG und SG)
- LANCOM (Firewall, WLC, APs)
- VMware
- Aruba Switche
- Windows Defender
- McAfee WebGateway
- Überwachung von Konfigurationsänderungen, Windows PowerShell sowie bekannter Angriffsbefehle
- Sysmon



Drei Beispiele für Ereignisse, bei denen unser SIEM Alarm schlägt:

- **Jemand versucht, sich 50-mal mit einem falschen Passwort anzumelden, danach erfolgt eine erfolgreiche Anmeldung**
- **In einem System startet ein verdächtiger Dienst**
- **Per PowerShell werden verdächtige Befehle ausgeführt**

banking & network it solutions GmbH · Klosterdorf 38 · 91443 Scheinfeld · Tel. +49 9162 5279990 · info@bn-its.de · www.bn-its.de

PIC 2.0 SIEM

banking & network it solutions GmbH

Ihre Vorteile auf einen Blick

- Umfassender Überblick über die Sicherheitslage Ihrer IT-Infrastruktur unter **Berücksichtigung aller bekannten regulatorischer Anforderungen** mit einem einzigen System.
- **Deutliche Erhöhung der Informationssicherheit** durch die zentrale und regelbasierte Auswertung möglicher Sicherheitsvorfälle inkl. regelmäßiger Updates.
- **Erfassung aller internen Systeme** durch die individuelle Anpassbarkeit der PIC 2.0 SIEM-Lösung zur lückenlosen Sicherheitsüberwachung.
- **Alarmbenachrichtigungen per Mail** ermöglichen das schnelle Reagieren auf Anomalien und mögliche Sicherheitsrisiken.
- **Umfassende individuelle Konfiguration durch unsere IT-Spezialisten**, die alle derzeit bekannten regulatorischen Anforderungen ebenso kennen wie gängige bankenspezifischen Systeme und Programme.
- **Unschlagbares Preis-Leistungs-Verhältnis** durch die Verwendung einer OpenSource Plattform.

Über uns

Die bn-its banking & network it solutions GmbH bietet Hard- und Softwarelösungen vorrangig für Genossenschaftsbanken und mittelständische Unternehmen in Deutschland.
Mit ganzheitlichen Lösungen, die Eigenentwicklungen mit Standardprodukten kombinieren, trägt bn-its nachhaltig zur Reduzierung von IT-Kosten bei. Die besondere Expertise liegt im Bereich der regulatorischen Anforderungen im IT-Bankenumfeld.

banking & network it solutions GmbH · Klosterdorf 38 · 91443 Scheinfeld · Tel. +49 9162 5279990 · info@bn-its.de · www.bn-its.de