# Concat SIEM-Lösung

## GANZHEITLICHE SICHT AUF DIE IT-SICHERHEIT

splunk>

Sie suchen eine Lösung, mit der Sie Sicherheitsvorfälle oder Warnhinweise zu IT-Komponenten schnell und gezielt identifizieren, in Echtzeit analysieren und effizient lösen, bevor sie zu Problemen werden?

**... dann ist Security Information und Event Management (SIEM) kombiniert mit dem Tool Splunk das Richtige für Sie. Sie können die SIEM-Dienstleistung im eigenen Rechenzentrum realisieren oder als Service aus dem Concat-Rechenzentrum beziehen.**

In IT-Infrastrukturen von Unternehmen fallen täglich große Mengen an Statusmeldungen an. Im Regelfall stammen diese aus diversen Quellen, zum Beispiel Netzwerk- oder Sicherheitskomponenten, Anwendungen, Webserver oder Maschinen aller Art. Das Problem: Diese Daten fallen jeweils lokal an und sind nicht miteinander verknüpft, erlauben also auch keine Aussagen über den Gesamtzustand.
Eine regelmäßige Analyse dieser Daten findet nicht statt und aus Platzgründen werden sie nur kurze Zeit vorgehalten. Erschwerend kommt dazu, dass jedes Gerät, jedes Programm, jedes System jeweils eigene Zugangsdaten benötigt. Tritt ein Fehler auf, ist die Suche nach der Ursache mühsam und zeitaufwendig.


**Hier einige Beispiele von Ereignissen und Mustern, die auftreten können:**

- Auffälliges Verhalten, das typisch ist für Schadprogramme (z. B. erhöhter Netzverkehr, Abnahme der Performance, Fehler in Anwendungen und Integritätsverletzungen)
- Ungewöhnlicher Anstieg von CPU-Last und Speicherverbrauch
- Hardware-Defekte wie fehlerhafte Sektoren bei Datenspeichern (z. B. Festplatte) oder ausfallende Komponenten aufgrund von Hardware-Fehlern
- Verlust von Netzverbindungen

Lösen lässt sich dieses Dilemma mit einem SIEM-Konzept, das nach BSI-Vorgaben konzipiert und implementiert wurde. Der SIEM-Server empfängt alle Statusmeldungen eines Unternehmens und speichert diese zentral und ausfallsicher. Jegliche über das Internet übertragenen Daten werden mithilfe eines VPN-Tunnels verschlüsselt.

concat AG
IT SOLUTIONS


Für die Analyse, Archivierung und Forensik der Daten verwenden wir die Software Splunk. Das Programm speichert alle Statusmeldungen von IT-Geräten oder Anwendungen an einer zentralen Stelle und liefert so eine ganzheitliche Sicht auf die Sicherheit der Infrastruktur in Ihrem Unternehmen. Sollte Ihr Unternehmen angegriffen werden oder ein Fehler in der Infrastruktur auftreten, durchsucht Splunk zügig den gesamten Datenbestand, um wichtige Erkenntnisse für die forensische Untersuchung zu liefern.

Bei bestimmten Ereignissen sendet das Tool automatisch Berichte oder Benachrichtigungen. Mithilfe von Forensik-Funktionen lassen sich auch Fehler analysieren, die bereits länger zurückliegen. Die redundante Datenhaltung trägt dazu bei, den Verlust von Statusmeldungen durch z. B. Festplattenausfall deutlich zu minimieren.
Mithilfe von SIEM und Splunk können Unternehmen die Produktivität erhöhen und den Unternehmenserfolg sichern.

### Vorteile für Ihre IT-Organisation:

- Zentrale Speicherung von Meldungen und Ereignissen ermöglicht schnelle Durchsuchung großer Datenbestände – egal welcher Art und von welchem Speicherort
- Redundante Datenhaltung (180 Tage) steigert Ausfallsicherheit
- Logische Gruppierung von Logmeldungen für Fehleranalyse, Erkennen von Angriffen und Anomalien, Forensik, Ermittlung von Trends
- Automatisierte Berichte der Ereignisse täglich, wöchentlich, monatlich je nach Wunsch
- Sofortige Benachrichtigung im Fehler- oder Angriffsfall

### Um ein hohes Maß an IT-Sicherheit für Ihr Unternehmen zu erreichen, beraten und unterstützen wir Sie mit folgenden Dienstleistungen:

- Assessment IT-Sicherheitsmanagement
- Security-Workshop
- Risikoanalyse von Geschäftsprozessen
- Beratung zur Einführung eines Informations-Sicherheits-Management-Systems (ISMS) nach ISO27001
- Mehrstufige Perimeter-Sicherheitsarchitektur
- Secure Client VPN (2FA, Compliance Check etc.)
- Zonierung im Trusted Network (TN) mit starker Verschlüsselung
- HUB / Site Schleusentechnik
- Endpoint Security inkl. Anti-Ransomware
- Security Incident und Event Management System (SIEM)
- Sandbox-Verfahren
- Analyse mit Forensik-Reports
- Managed Antiviren-Lösungen
- Security Scans: Schwachstellenanalyse der Unternehmens-IT
- Social-Engineering-Kampagnen

**Concat AG** IT Solutions
Seit 1990 realisieren wir maßgeschneiderte IT-Infrastrukturen. Unsere Managed-Service-Organisation erbringt dafür die Support- und Betriebsleistungen (24×7).
Mit mehr als 1.000 technischen Zertifikaten der führenden IT-Hersteller sind wir für den Dienstleistungsbereich optimal aufgestellt.

Haben wir Ihr Interesse geweckt?
Wir helfen Ihnen gerne weiter:
Telefon: **+49 (0)89 89080-500**
E-Mail: **security@concat.de**

Weitere Informationen: **www.concat.de**

concat AG
IT SOLUTIONS
A Meridian Group International Company

Concat AG
Berliner Ring 127–129
64625 Bensheim
Tel: +49 (0)6251 7026-0
Mail: info@concat.de