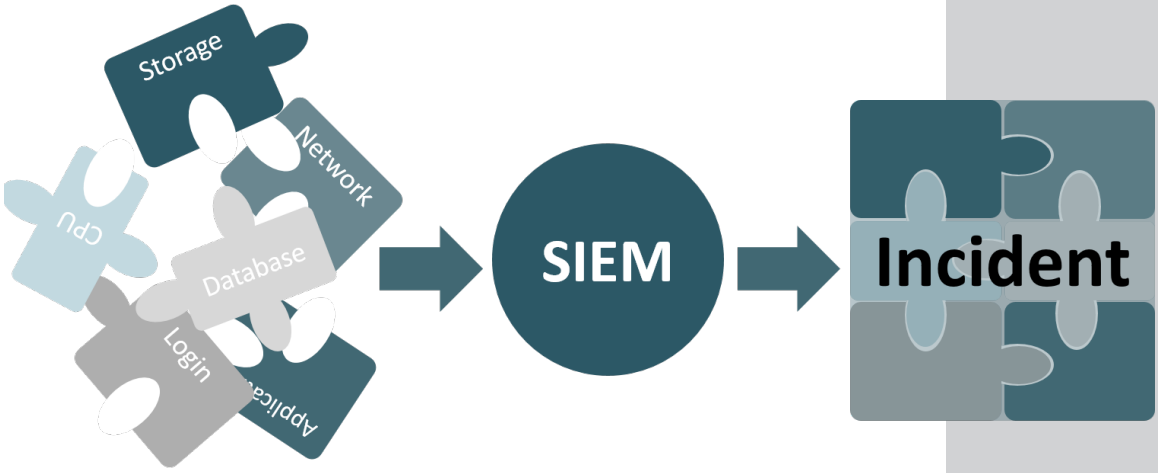
noris SIEM

Ihre Security and Event Management Plattform as a Service von noris



Gewinnen Sie den Überblick über Ihre Logs zurück und erfassen Sie die Zusammenhänge in Echtzeit.
Compliance wie Sie es sich wünschen - SIEM as a Service von noris

Vorteile

- Erfassen von Zusammenhängen zwischen Log-Events in Echtzeit
- Übersichtliche Darstellung in anpassbaren Dashboards
- Ermöglichen von nachträglichen Nachweisen über die Entstehung von Incindents
- Reduktion von Aufwänden für die Bearbeitung von Events
- Ermöglichung der Einhaltung von Complinace-Richtlinien

Highlights

- Freie Skalierbarkeit hinsichtlich Devices und Events pro Sekunden
- Einbindung von Devices in einem Rechenzentrum der noris network oder optional aus dem Netz des Kunden
- Auswertung und Bewertung von Reports auf Wunsch
- Standorte in eigenen, zertifizierten deutschen Hochsicherheitsrechenzentren

noris network

Details

Ihre System melden Ihnen zwar jede nur erdenkliche Information, die Flut an Meldungen ist jedoch selbst für ein ganzes Team von Security-Profis nicht zu bewältigen. Auch Compliance-Anforderungen können mit herkömmlichen Tools kaum noch erfüllt werden. Unser Angebot für Sie - SIEM as a Service!

Das noris SIEM (Security Information and Event Management) - System empfängt Syslog-Events von Ihren Devices, analysiert diese und bereitet die Informationen zur Darstellung korreliert auf. Aus der Analyse generieren Sie dann in Echtzeit Alarme/Events und erhalten Hinweise auf Security-Issues und Verbesserungspotentiale im Sicherheitskontext Ihrer Umgebung. Die Daten können auch über einen längeren Zeitraum gespeichert werden um nachträglich Nachweise über die Entstehung von Security-Issues zu liefern. Dadurch werden Daten bereitgestellt, die die forensische Analyse unterstützen und damit zur Einhaltung von Compliance-Vorgaben beitragen können.

Ihr SIEM-System verarbeitet Log-Daten und vergleichbare Informationen von einer Vielzahl unterschiedlicher Systeme - Devices genannt. Kollektoren erhalten Meldungen von Systemen wie Datenbanken, Servern oder Netzwerkkomponenten und normalisieren diese. Mit Hilfe von Korrelationstechniken werden dann die Logs automatisch in verwertbare und übersichtliche Informationen z. B. in Form Diagrammen auf Dashboards umgewandelt. Wenn man z.B. an einem Switch mehrfache erfolglose Login-Versuche sieht und dann im Anschluss weitere erfolglose Login-Versuche an nachgelagerten Servern könnte dies ein Hinweis auf eine Brute Force Attacke sein, bei der aktuell die erste Hürde (der Switch) bereits überwunden wurde und jeden Moment mit der Kompromittierung des angegriffenen Systems zu rechnen ist. Wurden einmal wichtige Zusammenhänge gefunden, so informiert das SIEM-System, die verantwortlichen Mitarbeiter über die potentiellen Probleme. Sie können sich sicherlich vorstellen, welchen Aufwand Sie ohne die Unterstützung durch ein SIEM-System hätten, wenn Sie solche Angriffe erkennen wollen.

Zur Visualisierung von Entwicklungen über einen längeren Zeitraum, werden in dem SIEM-System Daten vorgehalten und die Zusammenhänge aufzeigbar. So können Sie z. B. die Ursachen für immer länger werdende Antwortzeiten einer Datenbank finden und beseitigen.

Über eine leistungsfähige Suchfunktion sind Sie außerdem in der Lage nachträglich Logs zu erfassen und zu bewerten. Dies ist ganz besonders bei forensischen Nachweisen von großer Bedeutung.

Sie können bei noris ein SIEM als Managed oder Self-Managed Service nutzen. Bei der Managed-Variante erhalten Sie ein monatliches Reporting von sicherheitsrelevanten Meldungen. Die Übersicht über die aktuellen Ereignisse und die Bewertung der Bedrohungslage erfolgt dabei durch noris. Bei der Self-Managed-Variante erhalten Sie das voll funktionsfähige SIEM-System als Service. Die Alarmierung geht dann aber an Sie. Die Bewertung der aktuellen Bedrohungslage erfolgt ebenso durch den Kunden. Die Abrechnung über die Bereitstellung des Basissystems hinaus erfolgt abhängig von der Anzahl der zu überwachenden Devices und der Menge an Events pro Sekunde.

Gehen Sie auf Nummer Sicher mit SIEM as a Service von noris!

Interessiert?

Wir freuen uns auf Ihre Anfrage!

noris network AG
Thomas-Mann-Straße 16 - 20
D-90471 Nürnberg

T +49 911 9352-160
F +49 911 9352-100

produktanfrage@noris.de
www.noris.cloud

v0.1 20190314

noris network