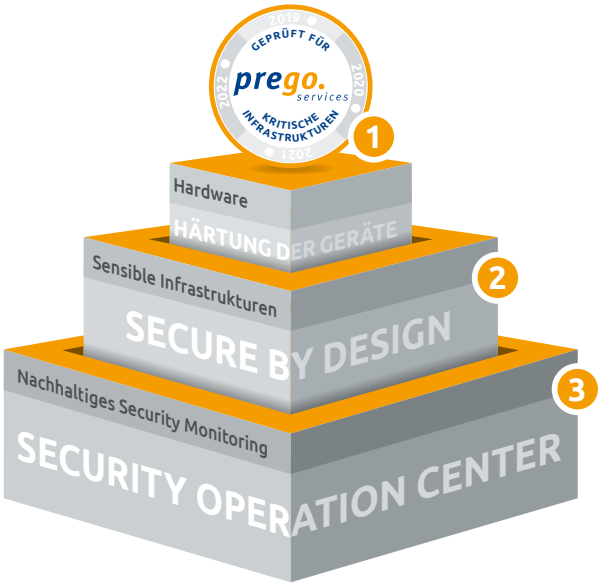
prego. SECaaS

Security Information und Event Management im Security Operation Center

Modulare Use Cases für die Überwachung der Sicherheitsmeldungen im Netzwerk

Für heutige Netzwerk-Infrastrukturen, speziell für kritische Infrastrukturen, ist die Überwachung von Sicherheitsmeldungen im Netzwerk gesetzlich vorgeschrieben (laut BDSG §9 Absatz 1.5). „Neben den Gesetzen und Vorschriften ist es im Interesse jeder Organisation, neben personenbezogenen Daten auch geistiges Eigentum und Finanzinformationen zu schützen. Darüber hinaus fordert die ISO Zertifizierung DIN ISO-27001 ein aktives Monitoring mit dem Ziel, unautorisierte Aktivitäten aufzudecken.

Die **SIEM**-Lösung speichert alle Informationen von Ereignissen und ermöglicht über die Analysefunktion, aus der Menge der unstrukturierten Daten, die Auswertung nach geforderten Suchkriterien.“[1]



Modulsystem schafft Cybersicherheit

Dreistufiger skalierbarer Qualifizierungsprozess zum nachhaltigen Schutz Ihrer Infrastruktur

- **Stufe 1 – Hardware**
  - Prüfung und Härtung der IP-basierten Geräte in Ihrem System
- **Stufe 2 – Sensible Infrastrukturen**
  - Sicherung des Netzwerks durch bspw. Segmentierung der Infrastruktur in Zonen und DMZ
  - Beraten, planen, bauen, betreiben von Secure by Design-Infrastrukturen
- **Stufe 3 – Nachhaltiges Security Monitoring**
  Monitoring/Betreuung und kontinuierliche Anpassung an die Bedrohungslage mit:
  - Security Information & Event Management (SIEM)
  - Malware-Erkennung
  - Sicherheitsbetrachtung, Forensik, Penetrationstests

[1] Vgl. (Secupedia, 2018)

prego. services

Security Information und Event Management im Security Operation Center

Modulare Use Cases für die Überwachung der Sicherheitsmeldungen im Netzwerk

Kurzbeschreibung

Wir stellen Ihnen mit unseren Experten in unserem 2-stündigen Workshop unsere SIEM Lösung mit den Modularen Use Cases vor. Die verschiedenen Use Cases befassen sich mit unterschiedlichen Security-/Angriffs-Szenarien.

Weitere Use Cases werden gerne in einem persönlichen Termin vorgestellt und erläutert.

Leistungsbeschreibung

Die verschiedenen Sicherheitsmeldungen sowie Angriffsszenarien werden mittels einer IST Analyse bewertet und eine Empfehlung an Use Cases geben, welche individuell an das Kunden-Netzwerk abgestimmt sind.

Die Ergebnisse der Use Cases können in 3 verschiedenen Modulen an den Kunden weitergegeben werden. In Form einer zeitnahen Alarmierung bei einem Vorfall, einem regelmäßigen Reporting mit allen wichtigen Informationen zusammengefasst und/oder eine Übersicht des Netzwerks in Form von Kennzahlen.

Use Cases

Alarmierung	Reporting	KPI
Incident/Event	Zyklische Reports für Kunden	Kennzahlen zum Kundennetzwerk
Event ist relevant (kein False-Positive)	Manuelle Auswertung der Auffälligkeiten	Übersicht relevanter Faktoren zur schnellen Erkennung von Abweichungen
Analyse mit Kunden/ Handlungsempfehlungen	KI-gestützte Auswertung (Machine Learning)	

prego. services

Security Information und Event Management im Security Operation Center

Modulare Use Cases für die Überwachung der Sicherheitsmeldungen im Netzwerk

Ihr Mehrwert:

- Individuelle, Herstellerunabhängige Use Cases
- Monatliches Reporting
- Aktive Überwachung der Alarme
- Kennzahlen (KPI) zu Kundennetzen

Haben Sie Fragen zu unserem Qualifizierungsprozess zur Sicherung kritischer Netze?

Wir helfen Ihnen gerne weiter.

Kontakt

prego services GmbH
Neugrabenweg 4 · 66123 Saarbrücken
Franz-Zang-Straße 2 · 67059 Ludwigshafen
0681 95943-1265
vertrieb@prego-services.de
www.prego-services.de
info@prego-services.de

prego. services

Stand: 11/2018 v2