HANDLUNGSEMPFEHLUNG

Durch Security Operations stetig sicherer werden

Unsere 6 Handlungsempfehlungen für ein effektives SOC

… kurzfristig

1 Anbindung der wichtigsten Logquellen an ein SOC:

Starten Sie mit zentralen Systemen wie Active Directory, Firewalls, Mailservern und geschäftskritischen Anwendungen. Priorisieren Sie die Anbindung nach Risikolage, Relevanz und technischer Verfügbarkeit.

2 SOC-Use-Cases definieren:

Erarbeiten Sie individuelle Anwendungsfälle, abgestimmt auf Ihre Bedrohungslage – zum Beispiel Ransomware-Erkennung, auffällige VPN-Nutzung oder User Behavior Analytics (UBA). Damit sorgen Sie dafür, dass Ihr SOC relevante Sicherheitsereignisse erkennt.

3 Regelmäßige SOC-Review-Meetings:

Führen Sie strukturierte Abstimmungen mit Ihrem SOC-Dienstleister durch. Optimieren Sie gemeinsam Schwellenwerte, Alarme und Eskalationswege, um echte Vorfälle zuverlässig zu erkennen und zügig zu behandeln.

… mittelfristig

4 Ausbau der Überwachung auf die gesamte Infrastruktur:

Erweitern Sie die Überwachung auf alle relevanten IT-Komponenten Ihres Unternehmens – schrittweise, in Phasen nach Systemkritikalität und Gefährdungspotenzial.

5 Use Case Tuning und False-Positive-Analyse:

Passen Sie bestehende Use Cases regelmäßig an – auf Basis realer Vorfälle und Feedback aus dem Betrieb. Durch die gezielte Analyse von Fehlalarmen (False Positives) erhöhen Sie die Effizienz Ihres SOC erheblich.

6 Security als kontinuierlichen Prozess verstehen:

Verankern Sie das Bewusstsein, dass Informationssicherheit ein dynamischer, fortlaufender Prozess ist. Nutzen Sie aussagekräftige Kennzahlen (KPIs), um die Wirksamkeit Ihres SOC zu überprüfen.

ORBIT Gesellschaft für Applikations- und Informationssysteme mbH | mailing@orbit.de | www.orbit.de