Cyber Security Operation Center

Die zentrale Anlaufstelle für digitale Sicherheit

In einer zunehmend vernetzten Welt sind Cyberangriffe und digitale Bedrohungen allgegenwärtig. Unternehmen, Organisationen und öffentliche Einrichtungen müssen ihre kritischen Infrastrukturen, sensiblen Daten und Geschäftsprozesse rund um die Uhr schützen. Ein Cyber Security Operations Center (SOC) bietet dafür die notwendige Kompetenz, Technologie und organisatorische Struktur, um Bedrohungen frühzeitig zu erkennen und wirksam darauf zu reagieren. Es schafft Bewusstsein für sicherheitskritische Situationen und stärkt die digitale Widerstandsfähigkeit auf allen Ebenen.

So funktioniert es

Das Cyber Security Operations Center vereint organisatorische Prozesse, technologische Werkzeuge und fundiertes Fachwissen. Teilnehmer erhalten umfassende Schulungen zu Aufbau, Aufgaben und Organisation eines SOC, wobei insbesondere IT- und OT-Systeme in Unternehmen und kritischen Infrastrukturen berücksichtigt werden. Zentraler Bestandteil ist die Arbeit mit technischen Systemen wie Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) und Security Orchestration, Automation and Response (SOAR). Die Trainings beinhalten zudem praxisnahe Inhalte zu aktuellen Cyberbedrohungen, technischen Schwachstellen, Reaktionen auf Sicherheitsvorfälle, Playbook-Entwicklung und digitaler Forensik. Im AIT-eigenen Cyber Range - Training Center, einer besonderen Simulations- und Trainingsumgebung, können die erlernten Fähigkeiten in realitätsnahen Szenarien unter Anleitung erfahrener Trainer angewendet und vertieft werden. So lernen die Teilnehmer, Bedrohungen zu erkennen, Sicherheitsvorfälle zu analysieren, Präventionsmaßnahmen umzusetzen und die IT-Sicherheit kontinuierlich zu verbessern.

Das große Ganze

Mit einem Cyber Security Operations Center erhöhen Organisationen ihre digitale Resilienz, verbessern die Sicherheitsüberwachung und minimieren Risiken durch Cyberangriffe. Die strukturierte Kombination aus Wissenstransfer, technologischen Werkzeugen und praktischer Übung befähigt Mitarbeitende, Bedrohungen frühzeitig zu erkennen und effizient zu reagieren. Dies sichert den störungsfreien Betrieb kritischer Systeme, schützt sensible Daten und stärkt das Vertrauen von Kunden, Partnern und der Öffentlichkeit. Gleichzeitig unterstützt das SOC die Einhaltung gesetzlicher Anforderungen, interne Compliance-Standards und Best Practices im Bereich Informationssicherheit.

Fakten

- Lösungsbereich: **Organisationen, Prozesse, Qualitätssicherung und Zertifizierung, Soziale Teilhabe und Engagement, Technologische Innovation**
- Verwaltungsebene: **Bundesland, Bund**
- Lösungsprozess: **Digitalisierung und Technologie, Öffentlicher Dienst, Wissenschaft und Forschung**
- Technologie: **Automation und Robotics, Informationstechnologie, Künstliche Intelligenz, Netzwerke**

best practice austria.

aed – Agency for Economic Cooperation and Development
Ferdinandstraße 4,
1020 Wien, Österreich

+43 (1) 448 00 55 10
platform@bestpracticeaustria.at