SAFELY ENABLING BUSINESS

Cyber Defense Training Made ~~Easy~~ Extra Tough!

Erleben Sie Cyber Defense aus einer neuen Perspektive.

Angriffsabwehr unter Realbedingungen ist der beste Weg, die Qualifikationen und das Expertenwissen zu erwerben, die im Ernstfall wirklich helfen. In der Cyber Simulation Range, unserer hyperrealistischen Trainingsumgebung, haben angehende Sicherheitsexperten die Möglichkeit, anhand einer Vielzahl von Angriffen gegen IT- und OT-Infrastrukturen ihre Abwehrfähigkeiten zu testen und unbezahlbare Praxiserfahrung zu sammeln, ohne dass die Sicherheit eines realen Unternehmens gefährdet wird.

Mehr als nur intensive Produktschulung: Komplett eintauchen

Ein Cyber Simulation Training ist mehr als nur eine intensive Produktschulung. Ein Cyber Defender muss im Team zusammen mit anderen Spezialisten unter Druck schnelle und richtige Entscheidungen treffen. Angriffsparameter müssen mit einer Palette von Tools aufgespürt, analysiert, interpretiert und dokumentiert werden.

Dazu bedarf es einer Trainingsumgebung, die der Realität so nah wie möglich kommt. Das macht unser Schulungsangebot aus:

- Voll ausgestattetes Cyber Defense Center (CDC) zum trainieren mit allen Tools
- Realistische simulierte Firmeninfrastruktur: Server, Clients, Applikationen, Datenbanken...
- Simulierte OT-Komponenten: Segmentierte Produktionsnetze, Steuerkomponenten...
- Crash-Kurse in modernen Security Tools: SIEM, Proxies, Sandboxes, NextGen Firewalls, Intrusion Detection, Ticketing
- Erfahrene Analysten als Ausbilder
- Realistische Angriffsszenarien, orientiert an echten Vorfällen aus der täglichen Praxis unserer CDCs
- Immersive Trainingsumgebung: Simulation von Stromausfällen, Sicherheitsalarmen, etc.

Fit für den Ernstfall

Die Kursteilnehmer trainieren mit Komponenten führender Anbieter von Sicherheitslösungen:

- Security Orchestration & Automation (SOA)
- NextGen SIEM & Log Management
- KI-basierte Flow Analytics und Intrusion Detection
- KI-unterstützte User Behaviour Analytics
- Malware Detection & Analytics Platforms
- External Threat Intelligence
- Denial & Deception Technologie
- Incident Response Systems

Die **Cyber Simulation Range** ist Teil des **Information Security Hub** (ISH) unter Federführung des Flughafens München.

Mehr dazu unter ***www.infosec-hub.de***

ISH
Information Security Hub

SecureLink Germany GmbH • Paul-Gerhardt-Allee 24 • 81245 München • info@de.securelink.net • +49(0) 89 2000148 00
www.securelink.de

SecureLink is the market leading provider of cyber security in Europe.

Erfahren Sie mehr unter:
info.securelink.de/ish

»Theoretisches Wissen reicht nicht! Wer im CDC kritische Firmendaten verteidigt, muss Angriffe unter Realbedingungen erkennen, korrekt einschätzen und richtig reagieren können.

Das kann man nur in der Praxis lernen – oder in der Cyber Simulation Range.«

Andreas Günther // Managing Analyst Cyber Security & ISH-Trainer, SecureLink Germany GmbH

CSR101 - SECURITY INCIDENT HANDLING FOR SOC-ANALYSTS - LEVEL 1

In diesem Kurs wird das Zusammenspiel der Komponenten eines State of the Art CDC erklärt und in der Praxis erlebt. Dabei werden auch die Grundlagen der wichtigsten Tools erläutert und praktisch trainiert.

Was Sie bekommen:

- Verstehen Sie die Funktionsweise und Arbeitsprozesse eines State of the Art CDC.
- Nutzen Sie die integrierten Tools eines kompletten CDC Technology Stack.
- Lernen Sie Incidents zu erkennen, zu analysieren und korrekt einzuordnen.
- Holen Sie sich erweiterte Informationen durch die Nutzung von externer Threat Intelligence.
- Übernehmen Sie verschiedene Rollen im CDC Team unter realistischen Bedingungen.

Fit für das CDC: Absolventen des Trainings sind vorbereitet auf die praktische Arbeit im Sicherheitszentrum und können Angriffe erkennen, analysieren und abwehren.

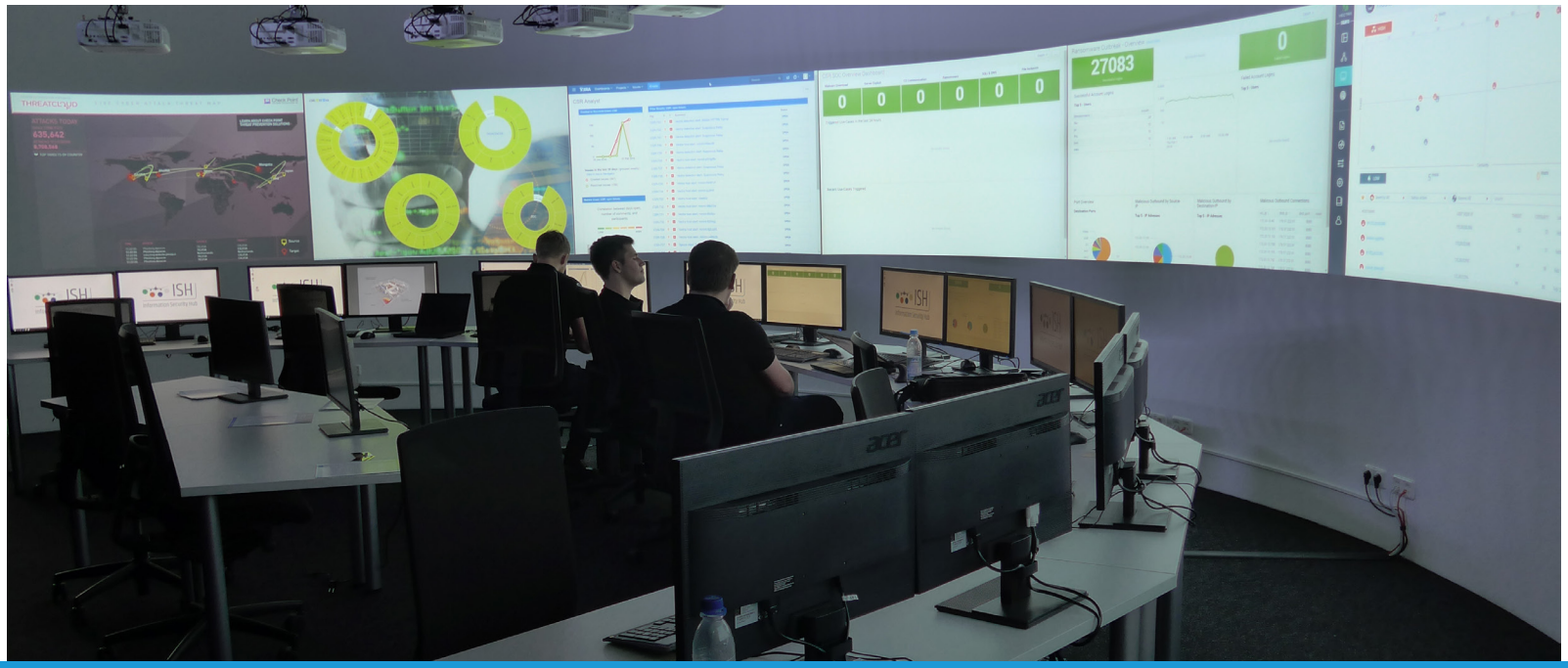
CSR102 - SECURITY INCIDENT HANDLING FOR SOC-ANALYSTS - LEVEL 2

Hier liegt der Schwerpunkt neben der Erkennung und Abwehr vertrackter Angriffe besonders auf der Operational Technology (OT). Denn besonders Produktionsnetze rücken immer mehr in den Fokus von Angreifern.

Was Sie bekommen:

- Stellen Sie sich den neuen Herausforderungen im Bereich der IT & OT Security.
- Nutzen Sie die Profi-Tools im CDC um die relevanten Ereignisse aus dem Datenstrom zu filtern.
- Erkennen, analysieren und bewerten Sie komplexe, mehrstufige und gezielte Attacken effizient.
- Reagieren Sie auch unter Druck richtig auf kritische Incidents.
- Arbeiten Sie effektiv im Team mit Security Analysten, IT-Forensikern und Abwehrspezialisten.

Vorbereitet auf IT&OT: Wer diesen Kurs abgeschlossen hat, kann vom CDC aus auch Steuerungssysteme und Produktions-OT gegen Cyberangriffe verteidigen.



SecureLink Germany GmbH • Paul-Gerhardt-Allee 24 • 81245 München • info@de.securelink.net • +49(0) 89 2000148 00

www.securelink.de

SecureLink is the market leading provider of cyber security in Europe.