
CYOSS
CYBER
SIMULATION & TRAINING
Zu Ihrem Schutz
ermöglichen wir alles
Menschenmögliche

LIVE UND LEHRREICH

Bei allen technischen Schutzvorkehrungen bleibt der Mensch in der Schlüsselposition. Er trägt in der Vorbeugung und Erkennung von Cyberattacken große Verantwortung, er muss in der Abwehr und Behebung von Angriffen die richtigen Entscheidungen treffen. Die notwendigen Fähigkeiten trainieren wir in unserer realistischen Simulationsumgebung mit hocheffektiven Erlebnissen.

„Tolles Team vermittelt vielschichtige Erfahrungswerte!"

„Sehr gut vorbereitet und durchgeführt in einer tollen Umgebung"

– Zentrum für Cyber-Sicherheit der Bundeswehr

Profitieren Sie von unserer jahrzehntelangen Erfahrung im Einsatz von State-of-the-Art-Simulationstechnik für Training und Testing in der Automobil- und Luftfahrtindustrie. Das CYOSS Cyber Simulation & Training Center verfügt über modernste Cyber-Simulationstechnik, die sich bereits im internationalen Umfeld und in einer Vielzahl von Branchen bewährt hat. Wir bilden IT-Infrastrukturen mit gängigen Sicherheitstechnologien nach und fordern in intensiven Trainings Ihre IT-Profis mit vollautomatischen Angriffen unter realistischen Bedingungen. Hier sammeln Ihre Mitarbeiter wertvolle Praxiserfahrung, ohne Risiko für die eigene Infrastruktur. So machen und halten wir sie fit für den Einsatz im Ernstfall.

Maßgeschneidertes Training – wann und wo Sie es benötigen

Trainieren Sie in unserem Center im Herzen von München. Oder wir bringen unsere Simulation über Remote-Zugang zu Ihnen ins Haus. Auf Ihre individuellen Wünsche gehen wir ein – bis hin zur Nachbildung Ihres eigenen IT-Netzwerks.

CYBER DEFENCE TRAINING

Incident Detection & Response

Wir trainieren IT-Administratoren, (angehendes) SOC-/CERT-/CSIRT-Personal und IT-Sicherheitspersonal in der Angriffserkennung und Abwehr mit höchster Intensität in zwei Stufen.

BASIC (5 Tage)

Das Aufbautraining für folgende Fähigkeiten:

- Anomalien entdecken
- Cyber-Angriffe erkennen
- IT-Security-Werkzeuge effizient einsetzen
- Angriffsaktionen im Netzwerk nachverfolgen, isolieren und analysieren
- Maßnahmen zur Wiederherstellung des Normalbetriebs
- Incidents und Maßnahmen dokumentieren
- Effizientes Teamwork

ADVANCED (5 Tage)

Die Vertiefung für Fortgeschrittene:

- Kenntnis eines breiteren Angriffsspektrums in höherer Detailtiefe
- Komplexen Angriffen mit entsprechenden Gegenmaßnahmen begegnen
- Weiterentwicklung der Teamwork-Fähigkeiten in komplexen Angriffssituationen

Buchen Sie einen Termin bei uns in München oder auf Wunsch führen wir das Training bei Ihnen vor Ort.

Aktuelle Termine und mehr Infos:
cyoss.com/de/training

CYBER DEFENCE EXERCISES
Trainieren Sie im Team

Trainieren und optimieren Sie Ihre Kommunikations- und Entscheidungsprozesse in ein- oder mehrtägigen simulationsgestützten Übungen bei CYOSS in München oder bei Ihnen vor Ort.

Team Exercise

In dieser Cyber-Defence-Übung testet, trainiert und optimiert Ihr Team (IT-Administratoren, SOC-/CERT/CSIRT-Personal, IT-Sicherheitspersonal) die gemeinsamen Abläufe zur erfolgreichen Bewältigung von Cyber-Angriffen. Dies steigert das interdisziplinäre Arbeiten in zeitkritischen Momenten.

Enterprise Exercise

Trainieren Sie die Bewältigung von Cyber-Angriffen simultan auf der Responder-Ebene (IT-Abteilung/CERT/SOC) und der Management-Ebene (Krisenstab, Business Continuity Management, Notfallkoordinatoren). In dieser unternehmensübergreifenden Cyber-Defence-Übung werden Ihre IT-Sicherheitsexperten mit realistischen Cyber-Angriffen konfrontiert, während die Management-Ebene auf die Lageentwicklung reagieren und entsprechende Entscheidungen treffen muss. Vor allem die ebenenübergreifende Kommunikation wird hier effizient getestet und trainiert.

Hoher Lernerfolg bei geringem Zeit- und Kostenaufwand

Eine Vielzahl unterschiedlicher Szenarien und Angriffsverfahren stehen „auf Knopfdruck" zur Verfügung, so dass Trainings und Übungen mit sehr geringem Zeitaufwand durchgeführt werden können. Hochrealistische Simulationen machen es Ihnen leicht, auch komplexe Angriffsszenarien schnell zu verstehen und zu beherrschen. Für eine transparente Auswertung stehen umfangreiche Analysefunktionalitäten zur Verfügung.

Authentische Umgebung

Für eine optimale Trainings- und Testumgebung können kundenspezifische IT-Netzwerke in die Simulationsumgebung integriert werden.

Auch reale Komponenten, wie z. B. Industriesteuerungsanlagenkomponenten (SCADA) und IT-Security-Tools (SIEM, Firewall, etc.) können eingebunden werden. Anhand der Simulation aktueller Angriffsverfahren werden deren mögliche Konsequenzen für IT- und Geschäftsbetrieb sowie die Auswirkungen von Gegenmaßnahmen nachvollziehbar aufgezeigt.

IHRE ANFORDERUNGEN
Machen wir zu unserer Aufgabe

Testing
Unsere sichere Simulationsumgebung bietet ein optimales Testfeld, wo wir risikolos Netzwerkschwachstellen und die Auswirkungen von Cyber-Angriffen untersuchen. Auf Wunsch können Sie in Ihrem nachgebildeten Netzwerk die Performance von Security-Tools testen und Ihre IT-Sicherheitskonzepte verifizieren und weiterentwickeln.

Komplettsystem
Trainieren Sie Ihre IT-Sicherheitsexperten in Ihrem eigenen Cyber Simulation Center. Gerne richten wir Ihnen Ihre eigene Trainingsumgebung im Komplettpaket vor Ort ein. Mit Hilfe unserer Experten im Bereich Cybersimulationstechnologie können Sie die modernsten Schulungsmethoden auf dem Markt einsetzen.

Blue Team Challenge
Motivieren Sie Ihre IT-Spezialisten zu reaktiver Höchstleistung am Standort Ihrer Wahl. Für ein spielerisches Wettbewerbserlebnis rund um optimale Verteidigungsstrategien setzen wir gern unseren Demonstrator bei Ihnen ein.

CYOSS GmbH
Ganghoferstr. 66
80339 München
cyoss.com

Kontaktieren Sie uns:
training@cyoss.com
Tel. +49-89-92161-2080
cyoss.com/de/training