

## Warum CCS?

Cyberresilienz ist mehr als eine Frage der Technologie — es geht um Menschen, Prozesse und Entscheidungen unter Druck. CCS bietet eine sichere, realitätsnahe Umgebung, in der Sie die Reaktion auf Sicherheitsvorfälle üben, Verfahren überprüfen und die Handlungssicherheit Ihrer Organisation stärken können.

### Die wichtigsten Vorteile



#### REALISTISCHE SZENARIEN

Abgestimmt auf Ihre Infrastruktur, Risiken und Bedrohungslage.



#### EINBINDUNG DES GESAMTEN TEAMS

Von IT-Fachkräften bis zu Führungskräften — alle trainieren in ihrer tatsächlichen Rolle.



#### EFFIZIENTES TRAINING

Mehrtägige Vorfälle lassen sich in nur wenigen Stunden simulieren.



#### GESTÄRKTE KOMPETENZEN

Teams werden schneller, besser koordiniert und widerstandsfähiger.



#### LANGFRISTIGER MEHRWERT

Eine wiederverwendbare Cyber-Umgebung ermöglicht kontinuierliches Training mit vielfältigen Szenarien.



#### EINBLICKE IN ANGRIFFSMETHODEN

Verstehen Sie die Taktiken, Techniken und Vorgehensweisen (TTPs) von Angreifern.

## Werden Sie CCS-Partner

Wir bauen ein Netzwerk vertrauenswürdiger Partner auf — Beratungsunternehmen, Systemintegratoren und Schulungsanbieter, die mit CCS anspruchsvolle Cyberübungen durchführen möchten.

### UNSER ANGEBOT

- Partnerschulungen — Lernen Sie, Cyber-Umgebungen und Szenarien zu gestalten und Übungen durchzuführen.
- Kontinuierliche Unterstützung — Unterstützung bei der Anpassung von Übungen an die Bedürfnisse und Anforderungen der Endanwender.
- Skalierbare Zusammenarbeit — Nutzen Sie CCS für Projekte oder als Bestandteil Ihrer Dienstleistungen.

### IHRE VORTEILE ALS PARTNER

- Erweitern Sie Ihr Portfolio um hochwertige Dienstleistungen
- Heben Sie Ihr Angebot vom Wettbewerb ab
- Stärken Sie Ihre Kundenbeziehungen
- Erweitern Sie Ihre Kompetenzen
- Bieten Sie modernste Schulungen zur Reaktion auf Cybersicherheitsvorfälle an

+385 (1) 36 35 666

info@utilis.biz



Utilis Ltd. | [www.utilis.biz](http://www.utilis.biz) | [ccs.utilis.biz](http://ccs.utilis.biz)



Kofinanziert von der Europäischen Union

Für weitere Sprachen scannen



**CCS** Cyber Conflict Simulator

# Trainieren Sie Ihre Organisation für die Bewältigung von Cyberkrisen

Eine Plattform für Cyberplanspiele zur Stärkung der Cyberresilienz Ihrer Organisation.

# Cybersicherheit im Kontext

In der heutigen hochgradig vernetzten Welt ist Cybersicherheit zu einem zentralen Anliegen für Einzelpersonen, Unternehmen und Regierungen geworden. Staatlich unterstützte Angriffe, finanziell motivierte Kriminalität und hacktivistische Bewegungen entwickeln sich schneller als die Abwehrmaßnahmen.

EU-Regelwerke wie DORA und NIS2 verlangen eine höhere Cyberresilienz. Organisationen müssen nicht nur ihre Daten schützen, sondern auch die Kontinuität wesentlicher Dienste während und nach Sicherheitsvorfällen gewährleisten.



## CYBERSICHERHEITSVORFÄLLE

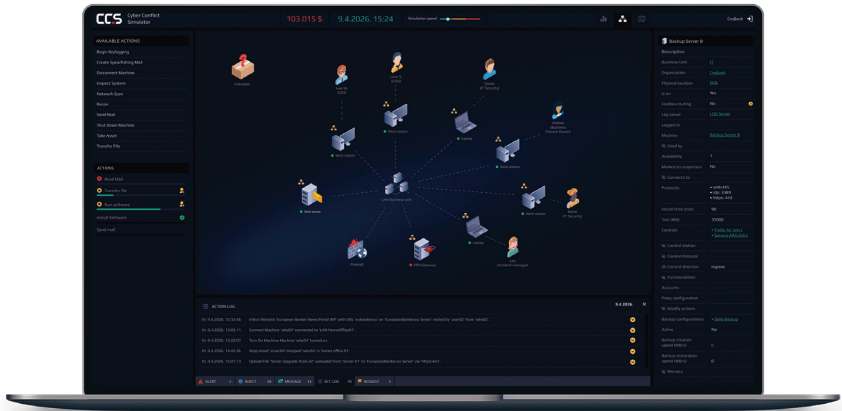
Cybersicherheitsvorfälle gelten seit mehreren Jahren in Folge weltweit als größtes Geschäftsrisiko. Organisationen investieren erhebliche Ressourcen in technische und organisatorische Präventionsmaßnahmen. Ebenso wichtig sind Investitionen in die Vorbereitung auf den Ernstfall.

## WARUM VORBEREITUNG WICHTIG IST

Laut einer IBM-Studie können erprobte Reaktionspläne und ein gut geschultes Incident-Response-Team die Kosten von Datenschutzverletzungen erheblich senken.

Gute Vorbereitung bedeutet:

- Ein solider Plan – Maßgeschneiderte Pläne zur Reaktion auf Sicherheitsvorfälle (Incident Response, IR), die in realistischen Szenarien getestet werden, decken Lücken auf und legen Rollen fest.
- Ein geschultes Team – Training unter Druck stärkt die Koordination.



# CCS Cyber Conflict Simulator

CCS ist eine Plattform für Cyberplanspiele, die realistische Angriffs- und Abwehrszenarien simuliert. Sie ermöglicht die Modellierung eines digitalen Zwillings von IT/OT-Systemen, Geschäftsprozessen und Menschen. So hilft sie Organisationen, ihre Bereitschaft zur Reaktion auf Sicherheitsvorfälle und ihre Entscheidungsfähigkeit unter Druck zu stärken

## So funktioniert CCS

### CYBER LANDSCAPE

CCS Cyber Landscape (CL) ist ein digitaler Zwilling, der Ihre IT/OT-Systeme und Geschäftsprozesse so abbildet, wie sie in der realen Welt bestehen. Geschäftsprozesse hängen von den zugrunde liegenden IT/OT-Systemen ab. Technische Ereignisse können daher den Betrieb beeinträchtigen und zu finanziellen Verlusten, Reputationsschäden oder sogar zur Gefährdung von Menschenleben führen.

Auch Menschen sind Teil des Modells — Administratoren, Analysten, Techniker und weitere Rollen, jeweils abgebildet mit ihren Fähigkeiten, ihrem Sicherheitsbewusstsein und ihren Gewohnheiten. Realitätsnahe Angreifer und Angriffsverhaltensweisen lassen sich simulieren. Dabei wird ein breites Spektrum an Bedrohungsquellen abgedeckt — von staatlich unterstützten Akteuren und cyberkriminellen Gruppen bis hin zu einzelnen Angreifern. Ihre Handlungen beruhen auf Taktiken, Techniken und Vorgehensweisen (TTPs), die aus Erkenntnissen über Bedrohungen abgeleitet werden. Sobald Cyber Landscape eingerichtet ist, können Sie beliebig viele Übungen mit unterschiedlichen Angriffsszenarien durchführen.

### SCENARIO

Jedes Übungsszenario wird auf die jeweiligen Ziele zugeschnitten und kann auf Bedrohungsinformationen oder Risikobewertungen basieren. CCS unterstützt ein breites Spektrum an Angriffen und kann Schwachstellen in Hardware und Software simulieren. Szenarien lassen sich aufzeichnen und erneut abspielen oder als Ausgangspunkt für künftige Übungen speichern. Den Teilnehmenden werden realistische Rollen zugewiesen — Einsatzleitung, technische Leitung, Verantwortliche für den IT-Betrieb und die Netzwerkadministration, Unternehmensleitung, Geschäftsverantwortliche, CISO, Fachleute, Leitung der Öffentlichkeitsarbeit, Rechtsberatung und Personalwesen. So werden reale Verantwortlichkeiten und die bereichsübergreifende Koordination abgebildet.

### SIMULATION

CCS simuliert sowohl technische Ereignisse als auch deren geschäftliche Auswirkungen. Übungen können vordefinierten Angriffsabläufen folgen oder Live-Aktivitäten eines Red Teams einbeziehen. Sie können in einer frühen Erkennungsphase oder in einer späteren Eskalationsphase beginnen. Die Teilnehmenden interagieren mit virtuellen Teammitgliedern, deren Handlungen ihre Fähigkeiten und Kompetenzen widerspiegeln. Die Zeitskalierung verdichtet mehrtägige Abläufe auf wenige Stunden und ermöglicht so realitätsnahe, zeiteffiziente Übungen.

### AFTER-ACTION REVIEW

Jede Handlung, Entscheidung und Nachricht wird detailliert protokolliert. Nach der Übung erstellt CCS ausführliche Berichte zur Bewertung der Wirksamkeit, der Koordination und der IR-Verfahren. So können Teams lernen, sich anpassen und ihre IR-Prozesse kontinuierlich verbessern.

## Erkenntnisse aus der Auswertung

- Wirksamkeit der Maßnahmen zur Erkennung, Verifizierung und Priorisierung von Vorfällen, zur Bestimmung ihres Ausmaßes, zur Eindämmung, zur Beseitigung von Bedrohungen und zur Wiederherstellung des Betriebs
- Kommunikation und Zusammenarbeit zwischen Rollen und Beteiligten unter Druck
- Stärken und Lücken in bestehenden IR-Verfahren und Playbooks
- Wirksamkeit von Firewalls, EPP, EDR, DLP und weiteren Sicherheitsmaßnahmen
- Beobachtete Taktiken, Techniken und Vorgehensweisen (TTPs) der Angreifer
- Vorrangige Bereiche für die Verbesserung technischer Abwehrmaßnahmen und organisatorischer Verfahren.