

SafeBreach



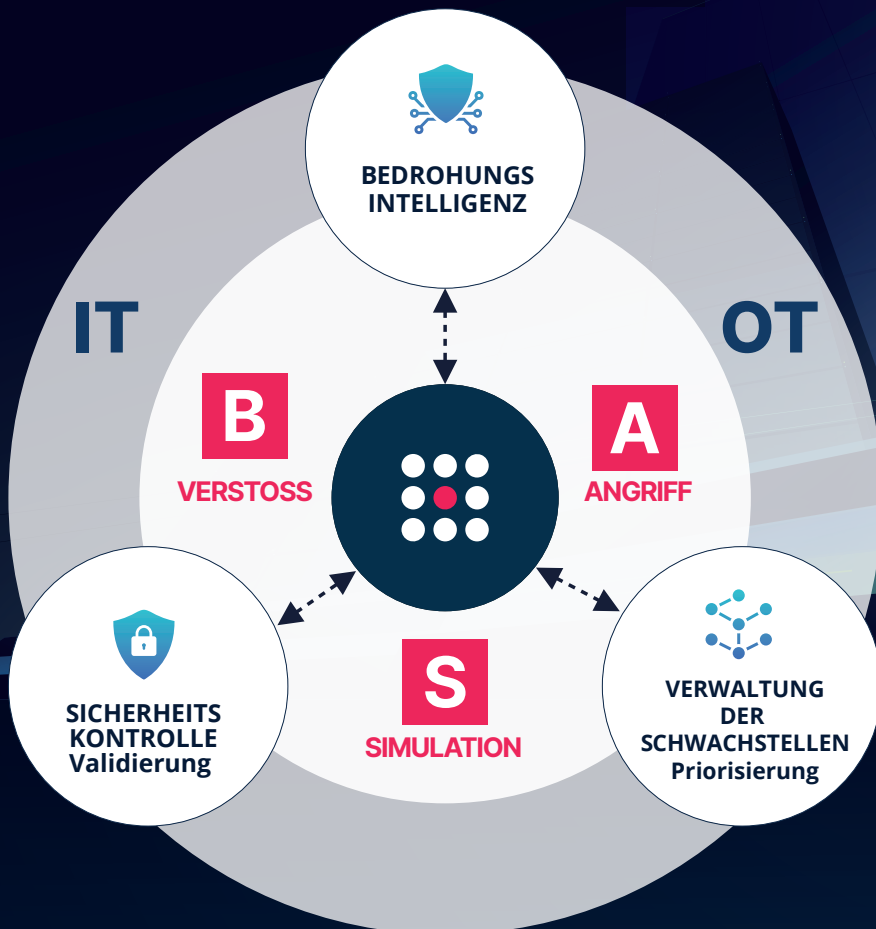
Red - Teaming

CYBERANGRIFF B A S LÖSUNG

FÜR IKS UND KRITISCHE VERSORGUNGSUNTERNEHMEN

“ANGRIFFE AUSNUTZEN”

Um Die Eigene Verteidigung Zu Verbessern



**SaaS,
On-Prem
Automatische
Red Teaming
Tests vor Ort**

SafeBreach



Überprüfen und optimieren
Sie ständig Ihre
Sicherheitskontrollen

RISIKEN EFFIZIENT ZU REDUZIEREN



IT & OT Cybersicherheitsstufe

"Testen" - "Berichten" - "Verbessern" - "Erneut testen"

Nutzen Sie die BAS

Lösung zur

Simulation von

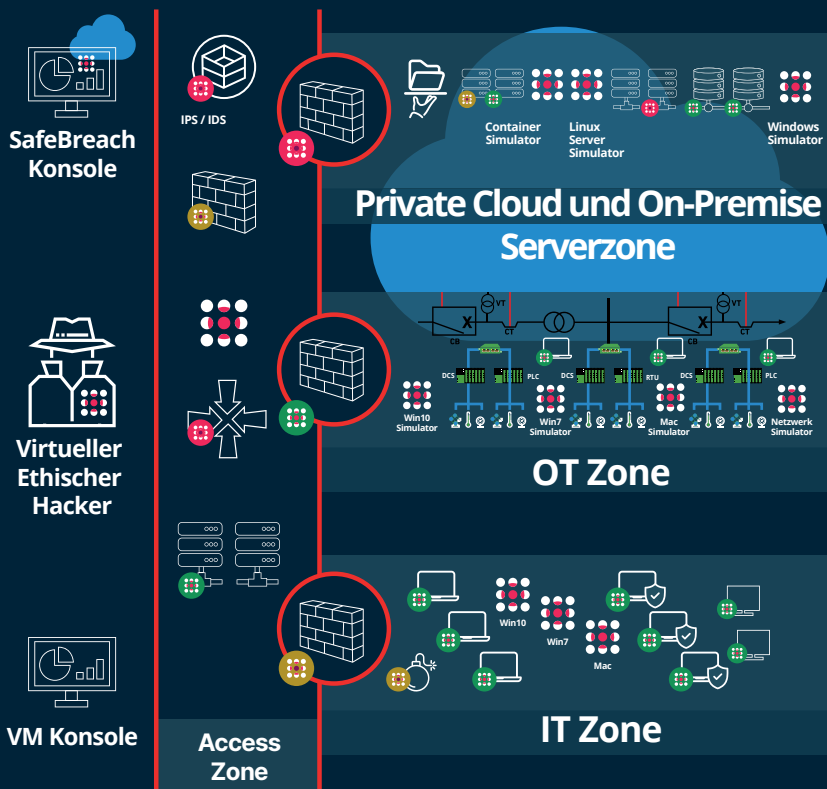
Cyber-Angriffen

zur Stärkung Ihrer

Verteidigungssysteme

i Risikominderung hört nicht auf, sondern geht kontinuierlich weiter. Erkennen und mindern Sie kritische Lücken vor dem eigentlichen Angriff- Verbesserungen automatisieren und priorisieren.

ÜBUNGSUMGEBUNG VON DER DEFENSIVE ZUR OFFENSIVE

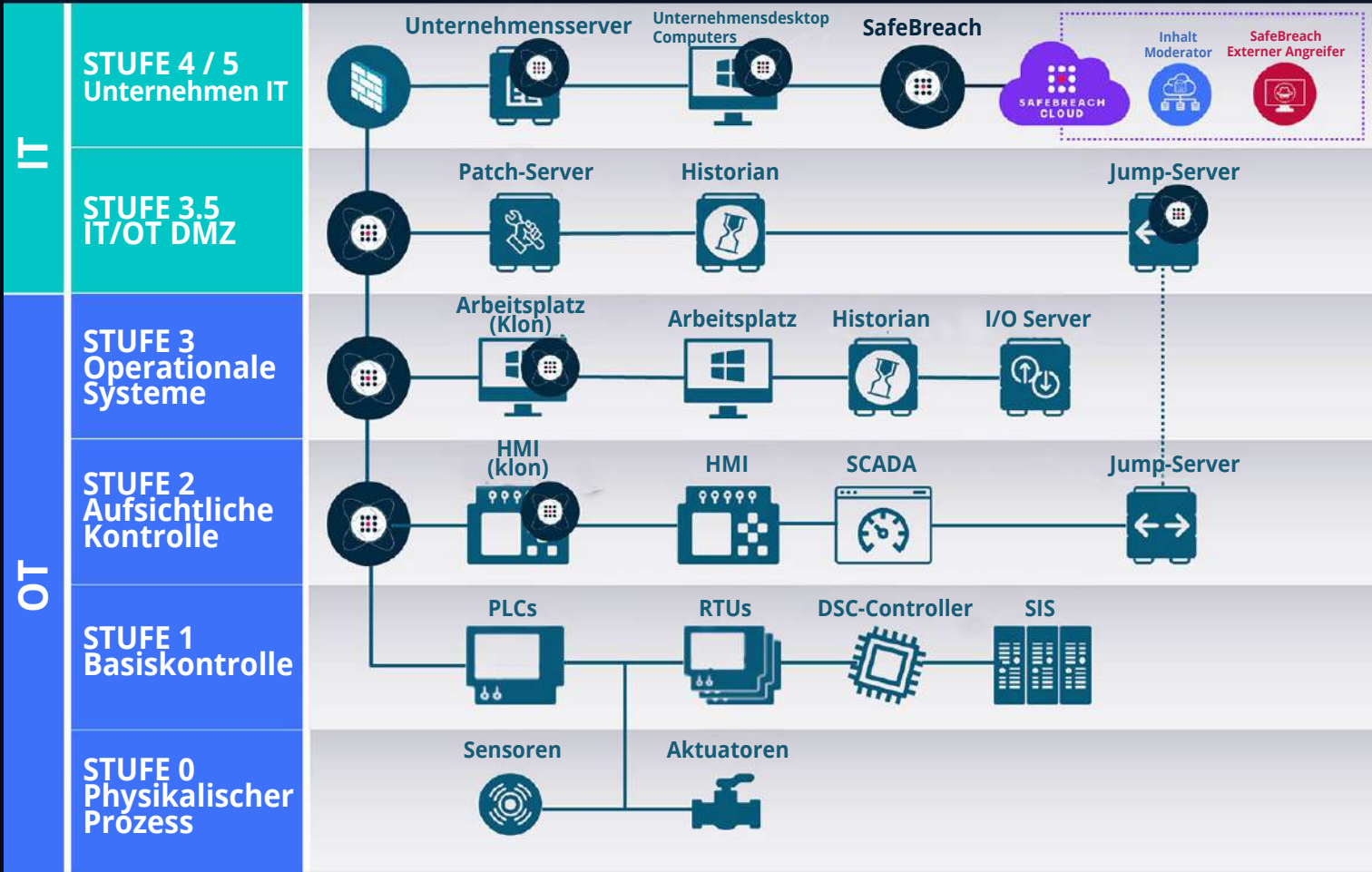


Kontinuierliche **"Kriegsspiele"** um Ihre Schwachstellen in Ihren Cloud und lokalen Netzwerksystemen zu erkennen.

Um Angriffe proaktiv zu erkennen und Ihre Sicherheitslage durch ständiges **Messen und Validieren** zu verbessern, verwenden Sie die Übungsplattform für **Cyber Angriffssimulationen** und erhöhen Sie Ihren Widerstand.

Um Ihre Verteidigungssysteme zu stärken, führen Sie szenariobasierte sichere **IT und BT Cyberangriffssimulationen** durch.

IT & OT ROTES TEAM CYBER SECURITY PLATTFORM "SAFEBREACH"



“Gewinnen Sie Einblick in den gesamten Cyberangriff”



SafeBreach

Sicherheitskontrolle- Arbeitsfluß

Reduzieren

- Probleme beheben
- Verfolgung der Fortschritte
- Feedback

Ergebnisse priorisieren

- Beziehen sich auf das Gesamtrisiko
- Visualisieren Sie den Angriffspfad
- Filtern und zielen Sie auf kritische Probleme ab, um umsetzbare Ergebnisse zu erzielen



Angriffe simulieren

- Cloud, Netzwerk, Endpunkt, E-Mail
- Infiltration, Seitliche Bewegung, Benutzerebene
- Mit 24-Stunden-SLA jedes US-CERT, jede aufkommende Bedrohung

Überprüfung der Sicherheitskontrolle

SC1	Haltung auf Sicherheitsniveau in der gesamten Organisation
SC2	Bewertung der OU/BU-basierte Sicherheitsniveau
SC3	Erkennung der Umgebungsdrift
SC4	Bewertung der Mitre Attack
SC5	Bewertung von Endpunkttechniken
SC6	Bewertung der E-Mail-Sicherheit
SC7	Umweltverträglichkeitsbewertung
SC8	Bewertung von Datenlecks
SC9	Überprüfung der IT/OT-Segmentierungskontrolle
SC10	Vergleich von Sicherheitskontrollen
SC11	SOC/IR-Überprüfung
SC12	M&A-Risikobewertung

Bewertung der Bedrohung

TA1	Bewertung der potentiellen Bedrohung
TA2	MITRE-Bewertung der Bedrohungsakteure
TA3	TI Integrierte Bewertung

Bewertung der Cloud-Sicherheit

CS1	Cloud-Bedrohungsanalyse
CS2	CWPP Kontrollüberprüfung
CS3	Überprüfung der Konfigurationskontrolle

Risikobasierte VM

VM1	Priorisierung von Sicherheitsschwachstellen
VM2	Priorisierung von Schwachstellen nach Bedrohung



VIDEOS ANSEHEN



OTD KATALOG

OTD BiLiSiM

GLOBAL VAD



www.onlineteknikdestek.com