SafeBreach

IT OT

Red - Teaming

CYBERANGRIFF B A S LÖSÜNG

FÜR IKS UND KRITISCHE VERSORGUNGSUNTERNEHMEN

"ANGRIFFE AUSNUTZEN"

Um Die Eigene Verteidigung Zu Verbessern

OTD BİLİŞİM

GLOBAL VAD

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

Moderne Unternehmenssicherheit wird nicht weniger komplex, sondern komplexer.

Im Durchschnitt, nutzen Unternehmen **75 %** Tools im Zusammenhang mit der Cybersicherheit in ihren Netzwerken

95% der erfolgreichen Eindringversuche sind das Ergebnis bekannter Angriffe

61% der Unternehmen haben Schwierigkeiten, Prioritäten bei der Minderung von Cyberrisiken zu setzen.

Stärkung der Verteidigungssysteme von IT- und OT-Teams

Prüfung der Wirksamkeit von Sicherheitskontrollen, Festlegung von Prioritäten künftiger Investitionen

Datengesteuerter Ansatz mit berichtspflichtigen Metriken

Suche nach mögliche Pfade zu hochsensiblen Bereichen, die Angreifer durch die Organisation verfolgen werden

Kontinuierliche Verbesserung der Erfahrungen von Verteidigern

OTD BİLİŞİM GLOBAL VAD

Kennen Sie diese...

94%

Prozentsatz der kürzlich befragten Organisationen, bei denen es in den letzten 12 Monaten zu einem OT/IoT-Sicherheitsvorfall kam

80%

Industrieorganisationen 80% haben nur einmal im Jahr oder seltener einen Rettungsdienst Durchführung einer Sicherheitsbewertung

3

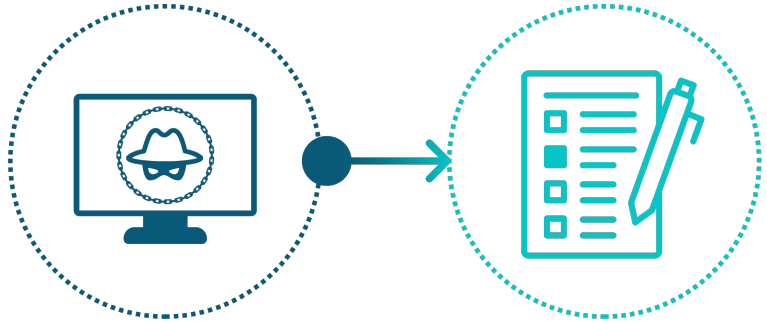
Engineering-Workstations, HMIs und Betriebsserver (alle laufen unter einem kommerziellen Betriebssystem wie Windows oder Linux) sind die drei Steuerungssystemkomponenten, die bei einem OT-Angriff am stärksten gefährdet sind

Viele OT-Angriffe beginnen als IT-Angriffe

Viele Angriffe beginnen mit dem Eindringen über das IT-Netzwerk.

Sobald sich die Angreifer im Inneren befinden, führen sie eine Erkundung durch, um Zugangsdaten zu erhalten und anfällige Pfade zum OT-Netzwerk zu identifizieren.

Der Angreifer nutzt dann zuvor kompromittierte Systeme, Anmeldeinformationen oder Anwendungen aus, um auf Systeme in Zonen mit höherer Sicherheit zuzugreifen, beispielsweise in der OT-DMZ.



Informationsressourcen	Zielinformationen
System- oder Prozessdokumentation	Diagramme der Netzwerkarchitektur auf hoher Ebene
Tastaturhören	Hostnamen und IP-Adressen
Bildschirmüberwachung	Kommunikationswege
Netzwerkverwaltungskonsolen	Benutzernamen und Anmeldeinformationen
Port-Scanning (aktiv und passiv)	

OTD BİLİŞİM GLOBAL VAD

Perfekter Sturm

Aufgrund seines Designs unsicheres IKS

- **Flache Netzwerke**
- **Schwache Authentifizierung**
- **Ohne Verschlüsselung**
- **Unsichere ICS-Protokolle**
- **Schwerer/seltener Patch**

Immer vernetzter

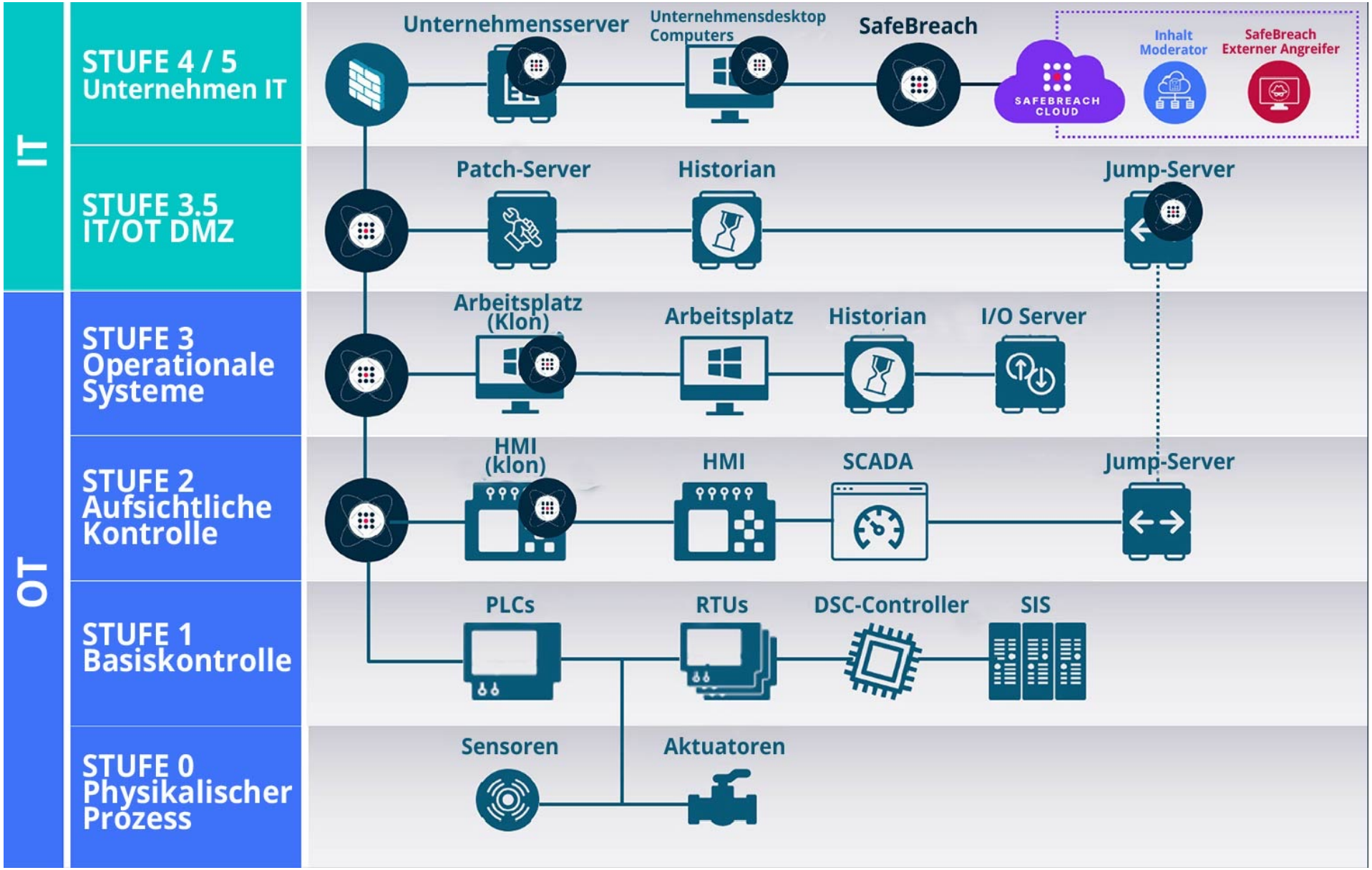
- **Integrierte IT/OT-Netzwerke**
- **KPIs von unten nach oben**
- **Datenanalyseprogramme**
- **Integration der Lieferkette**
- **Fernzugriff**

Aktive Bedrohung Sicht

- **Nationalstaatliche Angriffe richten sich gegen IKS**
- **Wiederholte Warnungen von DHS/FBI, GCHQ und anderen**
- **Kollateralschaden in Milliardenhöhe durch Ransomware-Angriffe**
- **Für den Zugriff auf anfällige Systeme sind keine fortgeschrittenen Hacking-Kenntnisse erforderlich**

SCHLECHTE SICHTBARKEIT IM IKS-NETZWERK

Purdue-Architektur



SafeBreach

BAS und IT/OT-Umgebung

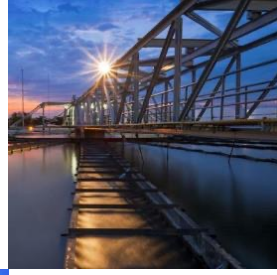
Wie passt das in Ihr Sicherheitsprogramm?

OTD BİLİŞİM GLOBAL VAD

ICT OTD PREFER EXPERIENCE ONLINE Since 2011









Besserer Schutz und Sichtbarkeit in der gesamten Anlage

Halten Sie die Produktionsverfügbarkeit aufrecht

Konsolidieren, optimieren und melden Sie IT-/OT-Sicherheitstests

Unterstützen Sie die digitale OT-Transformation mit Zuversicht

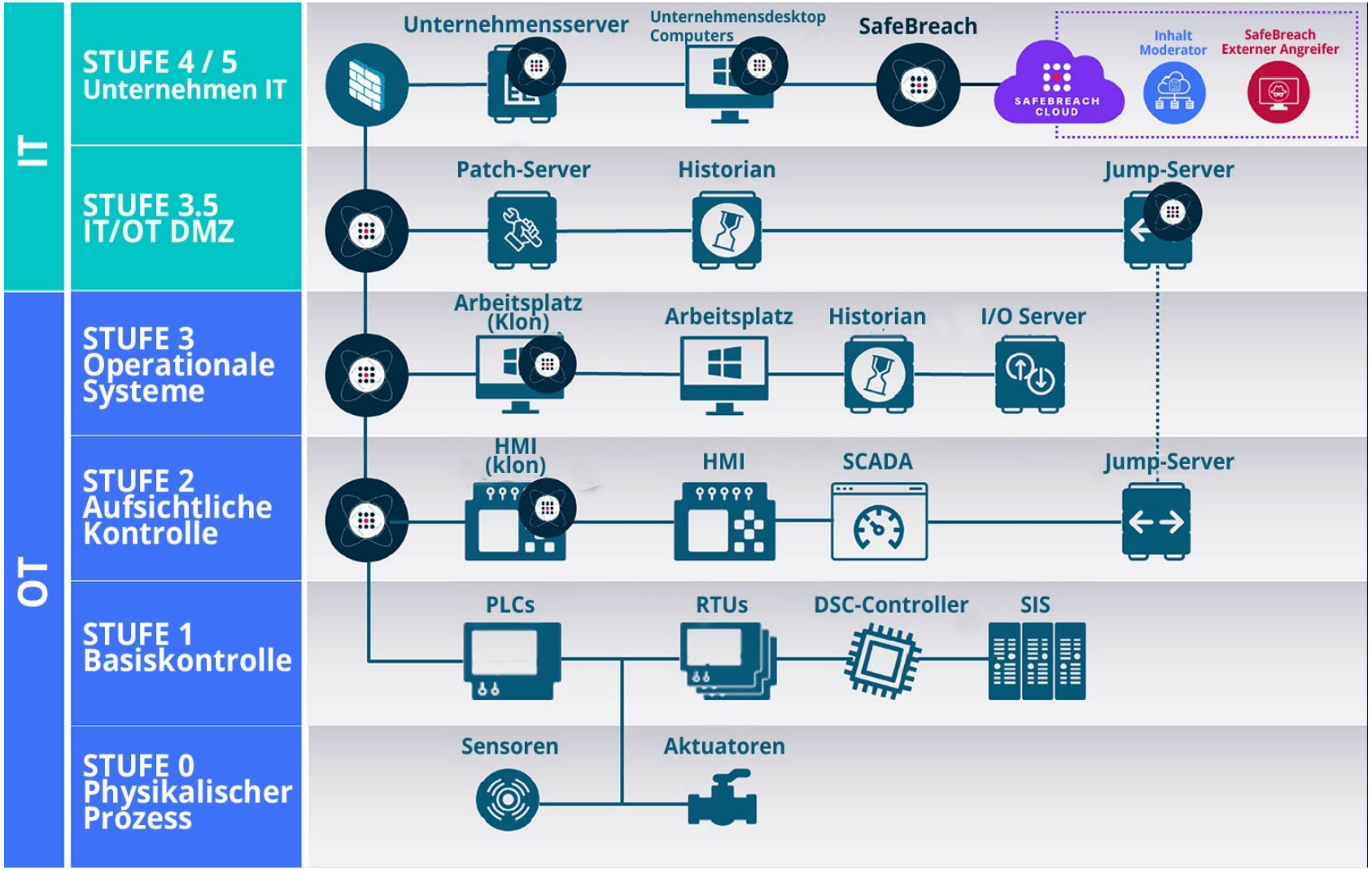
Kontrollieren Sie Sicherheitsrisiken in der Lieferkette

Verbessern Sie die Zusammenarbeit zwischen IT- und OT-Stakeholdern

"Dadurch konnte das SafeBreach-Team Lücken identifizieren, die das OT-Netzwerk gefährden, und gemeinsam mit dem Team vor Ort an einem Behebungsplan arbeiten."

SoC-Direktor
Strom- und Energieversorger

SafeBreach in IT/OT-Umgebung



SafeBreach führt Angriffssimulationen sowohl auf Netzwerk- als auch auf Host-Ebene auf Ebene 4 und 3.5 durch

- Überprüfung der Sicherheitskontrolle auf Host-Ebene (Dsktp, Srvr, Remote)
- Überprüfen der Firewall-Erkennungsregeln
- Überprüfen der EKL-Regeln der Firewall
- Validierung der Protokollierung auf SIEM- und Sicherheitskontrollebene

SafeBreach führt Angriffssimulationen auf Ebene 3.5 bis 2 und geklonte Ebene-3-Hosts im Netz durch

- Überprüfen der Firewall-Erkennungsregeln (Arbeitsplatz-Klon)
- Überprüfen der Firewall-Erkennungsregeln
- Überprüfen der EKL-Regeln der Firewall
- Validierung der Protokollierung auf SIEM- und Sicherheitskontrollebene

SafeBreach simuliert Angriffe auf Ebene 2 bis 3+ und geklonte Ebene-3-Hosts im Netzwerk

- Überprüfung der Sicherheitskontrolle auf Host-Ebene (HMI-Klon)
- Überprüfen der Firewall-Erkennungsregeln
- Überprüfen der EKL-Regeln der Firewall
- Validierung der Protokollierung auf SIEM- und Sicherheitskontrollebene

Anmerkung: Alle Simulationen finden zwischen SafeBreach-Simulatoren statt. Zwischen Nicht-SafeBreach-Systemen findet keine Simulation statt. Anmerkung: Alle Proxys in der Umgebung werden für die Tests verwendet.

SafeBreach beleuchtet 99 % Ihres OT-Risikos

99 % der kompromittierten Systeme werden Computerarbeitsplätze und Server (HMIs) sein.

99 % der Verweildauer des Einbruchs erfolgt auf handelsüblicher Computerausrüstung, bevor Geräte der Purdue-Stufe 0–1 betroffen sind.

99 % der Malware wird für diese Computer-Workstations und Server entwickelt.

99 % der Erkennungsmöglichkeiten ergeben sich aus Aktivitäten im Zusammenhang mit diesen Computerarbeitsplätzen und Servern.

99 % der forensischen Untersuchungen werden auf diesen Computerarbeitsplätzen und Servern durchgeführt.

SafeBreach hilft Ihnen, Ihre IT-/OT-Sicherheitsintegration voranzutreiben

OTD BİLİŞİM GLOBAL VAD

Basis

BEWERTEN, PLANEN UND ORGANISIEREN

ZIEL:

Identifizieren Sie wichtige OT-Assets, bewerten Sie die Architektur und bereiten Sie Reaktionspläne für Vorfälle vor

Hauptaufgaben und Meilensteine:

- Führen Sie eine Architekturüberprüfung mit Kronjuwelenanalyse durch [Angriffssimulation und -analyse]
- Vervollständigen Sie einen Vorfallreaktionsplan [kontinuierliche Sicherheitsüberprüfung und BAS-Plan

Machen Sie es betriebsbereit

KONTROLLE DES UNKRAUTRISIKOS

ZIEL:

OT-Sicherheitsprogramm mit Ressourcen und Fähigkeiten zur Erkennung und Reaktion auf Vorfälle

Hauptaufgaben und Meilensteine:

- Implementieren Sie die Asset-/Netzwerküberwachung für Standorte mit erstklassigen OT-Assets
- Operationalisieren Sie Verwaltung, Asset-Überprüfung, Bedrohungserkennung und -untersuchung
- Implementieren Sie Abhilfeprozesse für kritische OT-Schwachstellen

Optimieren

ERWEITERTES PROGRAMM ZUR REDUZIERUNG DES UNKRAUTRISIKOS

ZIEL:

Proaktive Risikominderung und Programmverbesserung

Hauptaufgaben und Meilensteine:

- Erweitern Sie die Anlagen-/Netzwerküberwachung in OT-Einrichtungen mit hohem und mittlerem Risiko
- Überprüfen Sie defensive Kontrollen – Inventar, Topologie, Verkehrsüberwachung, Schwachstellen
- Aktives Schwachstellenmanagement und Bedrohungsjagdprogramme
- Integrieren Sie OT-Bedrohungsinformationen in Sicherheitsbetriebsprozesse

1–3 IS → 3–12 IS → 12–24 IS (+FORTSETZUNG)

Angriff. Lösung. Berichterstattung. Wiederholung.

Kontinuierlicher Angriff

Validiert Ihre Sicherheitskontrollen automatisch und sicher

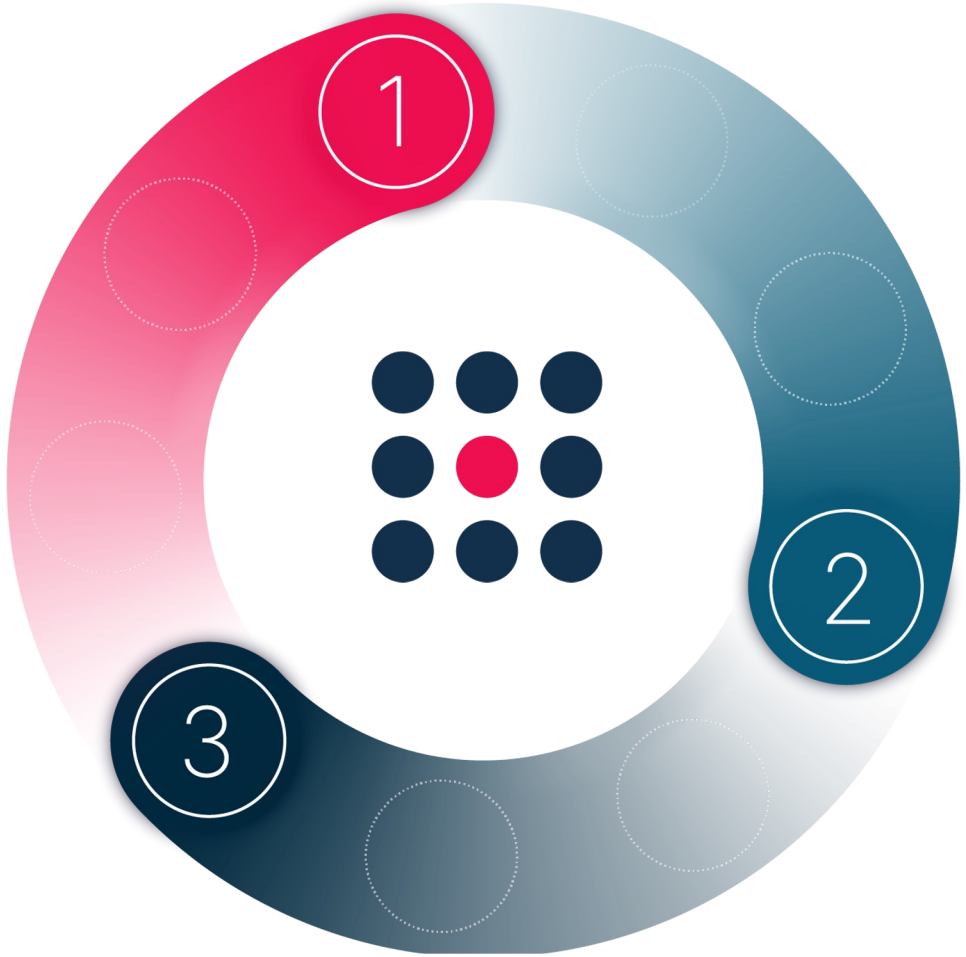
Mehr als **30K** Angriffsmethoden

SLA - Alle US-CERT-Warnungen werden innerhalb von **24** Stunden hinzugefügt

Reduzieren Sie das Risiko

Einzigartige Analysen und Integrationen zur Automatisierung der Schadensbegrenzung in großem Maßstab

CISO-Dashboard zur Überwachung des Fortschritts und Präsentation von KPIs auf Dashboard-Ebene



Priorisierung der Ergebnisse

Visualisiert den Sicherheitszustand

Integration mit Plattformen zur Verwaltung von Schwachstellen

Bezieht sich auf die Sicherheitskontrollen, um sich auf die kritischsten Lücken zu konzentrieren

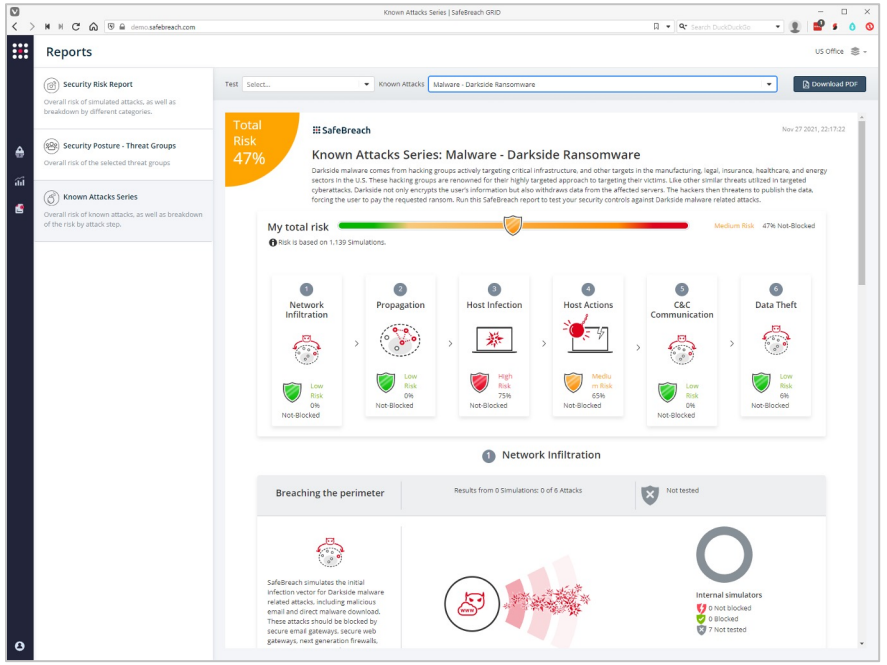
Gezielter Angriff

Das branchenweit größte Verzeichnis von Angriffstaktiken (Playbook) mit mehr als **30.000** Angriffsmethoden

Ein engagiertes Forschungsteam aktualisiert das Playbook innerhalb von **24** Stunden nach neuen Zertifizierungen und kritischen Angriffen

Erzeugt und/oder passt Angriffe an

Integriert mit Bedrohungsaufklärung



Bedrohungsaufklärung

Simuliert Angriffe, die aus IOCs der neuesten Bedrohung generiert werden

Alien Vault OTX	ThreatConnect	ThreatQ	Unit42

Kontinuierliche Validierung und Optimierung der Wirksamkeit von Cloud- und Onsite-Sicherheitskontrollen

Simuliert Angriffe auf Ihre Sicherheitskontrollen, um deren Wirksamkeit zu überprüfen

Integriert mit SIEM und Sicherheitskontrollen, um Ergebnisse zu korrelieren und Schwachstellen effizient zu identifizieren

Testet das gesamte Sicherheitsökosystem:

Cloud, Träger, Netzwerk, Web, Endpunkt, E-Mail, DLP

Sicherheitskontrollen

Korreliert automatisch simulierte Angriffe mit Sicherheitsereignissen, die von bestimmten Endpunkten und Netzwerkkontrollen empfangen werden

Tanium Threat Response
SentinelOne
Palo Alto Panorama
Crownstrike Falcon
FireEye HX
Microsoft Defender for Office 365
Microsoft Defender for Endpoint
Carbon Black Defense
Cisco AMP
Cybereason
Cisco Secure Email
Cortex XDR
BigQuery
McAfee ePD
Cisco Umbrella
CylancePROTECT & CylanceOPTICS
Amazon Web Services
Microsoft Azure

SIEM

Korreliert automatisch simulierte Angriffe mit Sicherheitsereignissen aus mehreren Quellen

QRadar
NetWitness Platform
LogRhythm REST
LogRhythm
Google Chronicle
Splunk
Splunk v2 (REST)
ArcSight Logger

SIEM

Korrelieren Sie simulierte Angriffe automatisch mit Sicherheitsereignissen aus verschiedenen Quellen.


ArcSight Logger


Microsoft Sentinel

Devo


ElasticSearch


Exabeam v1 (user-password authentication)


FortiSIEM


Google Chronicle

GuardDuty (SDK)


LogRhythm SOAP (deprecated)


LogRhythm

NetWitness Platform

QRadar


InsightIDR


Securonix


Splunk SDK (deprecated)


Splunk


Splunk SOAR

Sumo Logic

Sicherheitsprüfungen

Korrelieren Sie simulierte Angriffe automatisch mit Sicherheitsereignissen, die von bestimmten Endpunkt- und Netzwerkkontrollen abgerufen werden.

OTD BİLİŞİM GLOBAL VAD

- Carbon Black Defense
- CheckPoint NGFW
- Cisco AMP
- Cisco Secure Email
- Cisco Umbrella
- Cortex™ XDR
- CrowdStrike Falcon
- Cybereason
- CylancePROTECT & OPTICS
- FireEye HX
- Firepower
- FortiGate NGFW
- BigQuery
- Trellix ePO
- Microsoft Defender for Endpoint
- Netskope SASE
- Microsoft Defender for Office 365
- Palo Alto Panorama
- SentinelOne
- Tanium Threat Response
- Trend Micro XDR
- Windows Events

OTD BİLİŞİM GLOBAL VAD

Setzt Prioritäten und automatisiert Verbesserungen, um Risiken effizient zu reduzieren

Umsetzbare Verbesserungsschritte zur Erleichterung der Schadensbegrenzung

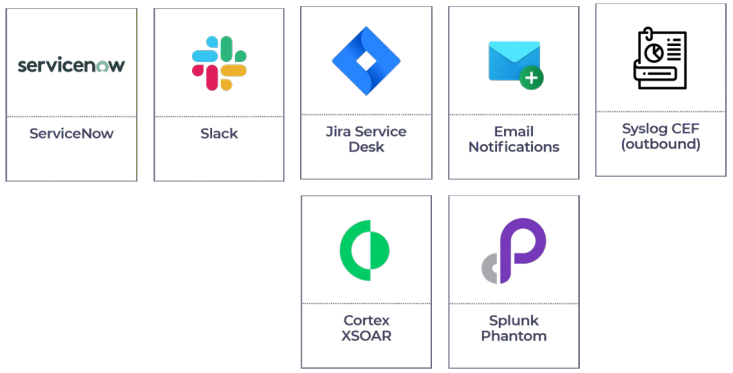
Priorisierung von Verbesserungsmaßnahmen je nach Geschäftsrisiko

Integriert mit SIEM, SOAR und Workflow-Management zur Automatisierung von Abhilfemaßnahmen

Integration mit Plattformen zur Schwachstellen-Management, um ausnutzbare Schwachstellen zu identifizieren und zu priorisieren

Arbeitsablauf und Automatisierung

Empfängt Benachrichtigungen über Systemereignisse und erzeugt Ereignisse für automatische Abhilfemaßnahmen



Schwachstellen-Management

Priorisierung der Schwachstellen nach Ausnutzbarkeit und Auswirkungen auf der Grundlage von SafeBreach-Simulationen

Management von Sicherheitslücken

Priorisieren Sie Sicherheitslücken auf der Grundlage von SafeBreach-Simulationen nach Ausnutzbarkeit und Auswirkungen.

Tenable Nessus

Qualys

Rapid7 Nexpose

Tenable.io

Tenable.sc

Bedrohungsaufklärung

Simulieren Sie Angriffe, die aus IOCs der neuesten Bedrohungen generiert werden.

AlienVault OTX

Anomali

Falcon Intelligence

Recorded Future

ThreatConnect

ThreatQ

Unit42

Diversifizierung: Bereiten Sie Ihr Unternehmen auf die Zukunft vor

OTD BİLİŞİM GLOBAL VAD

Automatische Schadensbegrenzung

Liefert umsetzbare Daten für die automatisierte Schadensbegrenzung mit Ihrer Orchestrierung in großem Maßstab.

CORTEX XSOAR BY PALO ALTO NETWORKS

splunk> phantom

Unternehmenstauglich

Skalierbar & Sicher

Leichter Einsatz

Automatisch und berührungsarm

Maximale Deckung

Verfolgen Sie die gesamte Angriffskette mit Cloud-basiertem, Onsite- oder Air-Gapped-Einsatz.

Das größte Playbook auf dem Markt mit >20K Angriffen.

SLA - Neue Bedrohungen werden innerhalb von 24 Stunden hinzugefügt.

Windows

aws

docker

macOS

Azure

Google Cloud

Offene Plattform

IBM Radar

CROWDSTRIKE

ThreatConnect

Microsoft

tenable

RSA

RAPID7

CYLANCE

paloalto NETWORKS

SafeBreach

SentinelOne

CISCO

now

CARBON BLACK

Qualys.

McAfee

splunk> phantom

OTD BİLİŞİM GLOBAL VAD

OTD ICT PREFER EXPERIENCE ONLINE Since 2011

SafeBreach-Paneele

Sichere Berichterstattung

Plant Messungen der Sicherheitslage und andere Berichte

Umsetzbares MITRE-Rahmenwerk und NIST-Mapping

Einfache Verfolgung von Trends im Zeitverlauf

Berichte zur Sicherheitstransparenz an das Management

Einsatz von SafeBreach

Simulatoren

Unkomplizierter Software-Agent, der auf internen und externen Vertretersystemen eingesetzt wird

Bei Angriffen in die Rolle des Angreifers und des Ziels schlüpfen, um die Sicherheit zu gewährleisten

Windows, Linux, Mac, AWS, Azure, GCP usw.

Administration

SaaS-, Onsite- oder Standalone-Optionen

Meldet Ergebnisdaten, plant, organisiert und stellt sie zu Visualisierungen und Analysen zusammen

Integriert sich in Sicherheitskontrollen, SIEM, SOAR, VM, TI und Workflow-Plattformen

Angriffs-Playbook

Cloud-Dienst mit Tausenden von aktualisierten Angriffsmethoden

Kein Software-Update für neue Angriffe erforderlich, Angriffe werden automatisch aktualisiert

Manuelle Aktualisierung bei offline Administration

Nutzen Sie die Macht des BAS

Überprüfung der Sicherheitskontrolle

SC1	Unternehmensweite Sicherheitslage
SC2	Lagebeurteilung pro OE/Einheit
SC3	Erkennung von Umgebungsabweichungen
SC4	ITRE ATT&CK Bewertung
SC5	Bewertung der Endpunkttechniken
SC6	Bewertung der E-Mail-Sicherheit
SC7	Überprüfung der Umgebung
SC8	Bewertung von Datenlecks
SC9	Überprüfung der Segmentierungskontrolle
SC10	Vergleich von Sicherheitskontrollen
SC11	SOC/IR-Überprüfung
SC12	M&A-Risikobewertung

Beurteilung der Bedrohung

TA1	Beurteilung der unmittelbaren Bedrohung
TA2	Bewertung von MITRE-Bedrohungsakteuren
TA3	TI - Integrierte Bewertung

Beurteilung der Cloud-Sicherheit

CS1	Bewertung von Cloud-Bedrohungen
CS2	CWPP Kontrollüberprüfung
CS3	Überprüfung der Konfigurationskontrolle

Risikobasierte VM

VM1	Priorisierung von Sicherheitslücken
VM2	Bedrohungsbasierte Priorisierung von Sicherheitslücken

Unternehmen, die uns vertrauen...

FINANZDIENSTLEISTUNGE

WELLS FARGO
BARCLAYS
INDEPENDENT FINANCIAL
AIG
MERCHANTRADE
Wafra
BREWIN DOLPHIN
L&T Finance
BANK OF CANADA BANQUE DU CANADA
jack henry & ASSOCIATES INC.
Goldman Sachs
PayPal
MAX FINANCIAL SERVICES
greendot bank
Morgan Stanley
BRINKS
GRUPO FINANCIERO BANORTE
TIAA
UBS
FAB First Abu Dhabi Bank
SCB ไทยพาณิชย์
experian
Jefferies
Allica Bank
ENVESTNET
shva The payments arena
DAVIVIENDA
ISRAEL DISCOUNT BANK
BanCERT Comunidad Bancaria de Ciberseguridad
Cboe
KB Kookmin Bank
BANCO INDUSTRIAL
bank hapoalim
AXIS BANK
RAYMOND JAMES

GESUNDHEITSWESEN

Cleveland Clinic
MARKEN
SHARP
CVSHealth
teva
children's health
CovenantHealth
GEHA

PRODUKTION

MARS
BOSCH
Cipla
MASCO
Titan.
Olin
Wabtec CORPORATION
GE
MODINE Always Innovating. Always Improving.
ACME BRICK
IAI
TESLA
ArcelorMittal

PHARMA UND BIOTECHNOLOGIE

Hovione
Johnson & Johnson
GILEAD
McKESSON
REGENERON
insmed
ICON
HilltopHoldings

VERSICHERUNG

JACKSON
TRAVELERS
PRUDENTIAL
BlueCross BlueShield
CNA
AON
SOMPO Digital Lab
GENERALI
cigna healthcare
MarshMcLennan

OTD BİLİŞİM GLOBAL VAD

Unternehmen, die uns vertrauen...

TECHNOLOGIE

Microsoft
ByteDance
paloalto NETWORKS
Trustwave
CRYPSIS
mimecast
IBM
TREND MICRO
WIZ
FORTIVE
virsec
IAS Integral Ad Science
netskope
VARONIS
JUNIPER NETWORKS
PEGA

LEBENSMITTEL UND GETRÄNKE

PEPSICO
Carlsberg Group
Kellogg's
OTD BİLİŞİM GLOBAL VAD
OTD

BERATUNG

Deloitte.
CYNERGISTEK A Clearwater Company
softserve
HCL
seek
PARAGON CONSULTING GROUP
SP6

RECHT

HUSCH BLACKWELL
FOLEY FOLEY & LARDNER LLP
pillsbury
BakerHostetler

DIENSTLEISTUNGEN

Service Corporation International
ADT

BILDUNG

CARIBBEAN EXAMINATIONS COUNCIL
Singapore Institute of Management

KRAFTFAHRZEUGE

Marathon Petroleum Corporation
ICEPCO
PG&E
NORTHLAND POWER
Ameren
Southern Company

TRANSPORT

UNION PACIFIC
SINGAPORE AIRLINES
American Airlines

KOMMUNIKATION

TIM
iZZI telecom
at&t
Ministry of the Interior and Safety National Information Resources Service
ECHOSTAR
NOS
orange

UNTERHALTUNG

NETFLIX

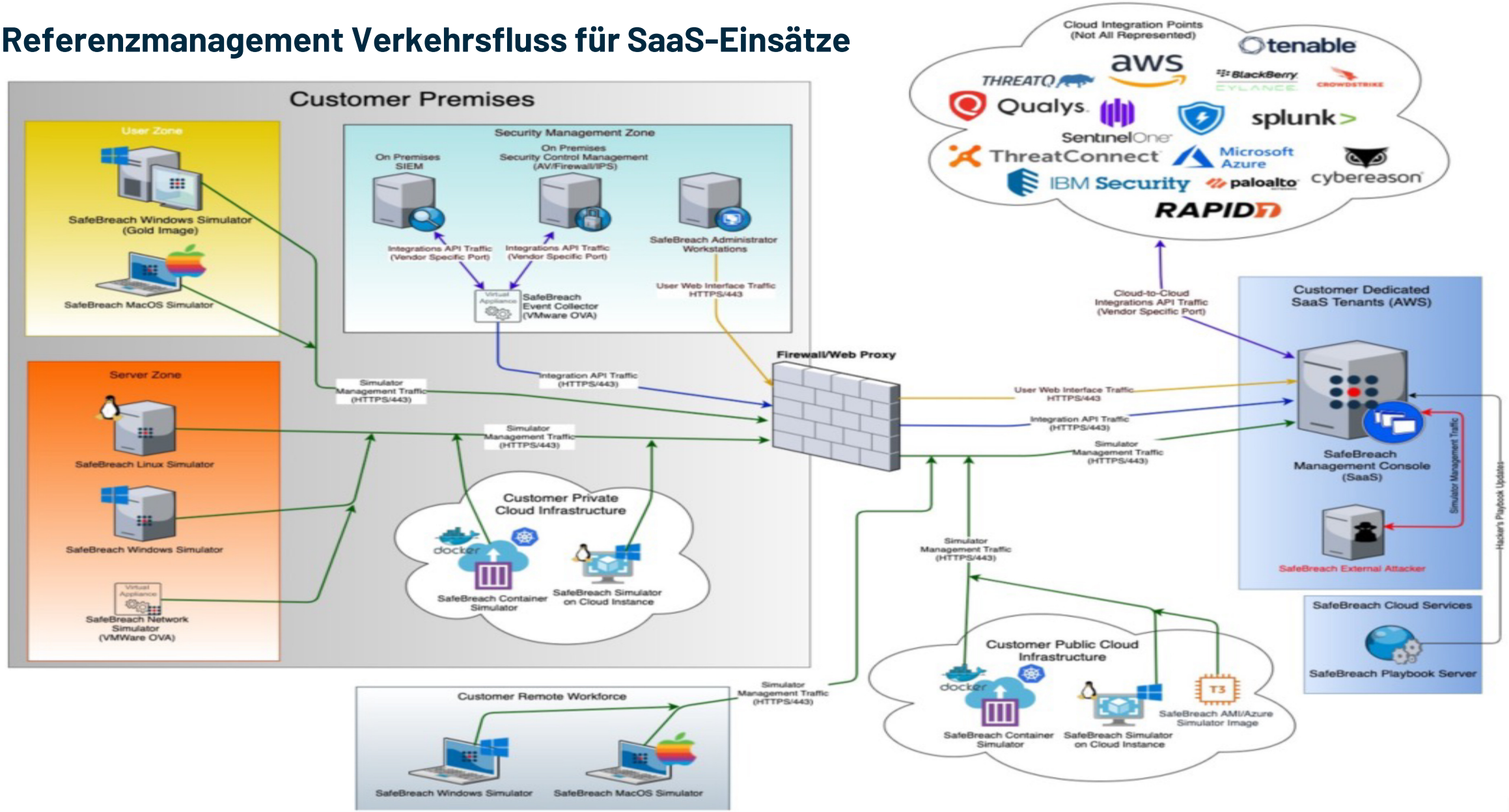
EINZELHANDEL

ABC Supply Co. inc.
7 ELEVEN
SPAR
ASBURY AUTOMOTIVE GROUP

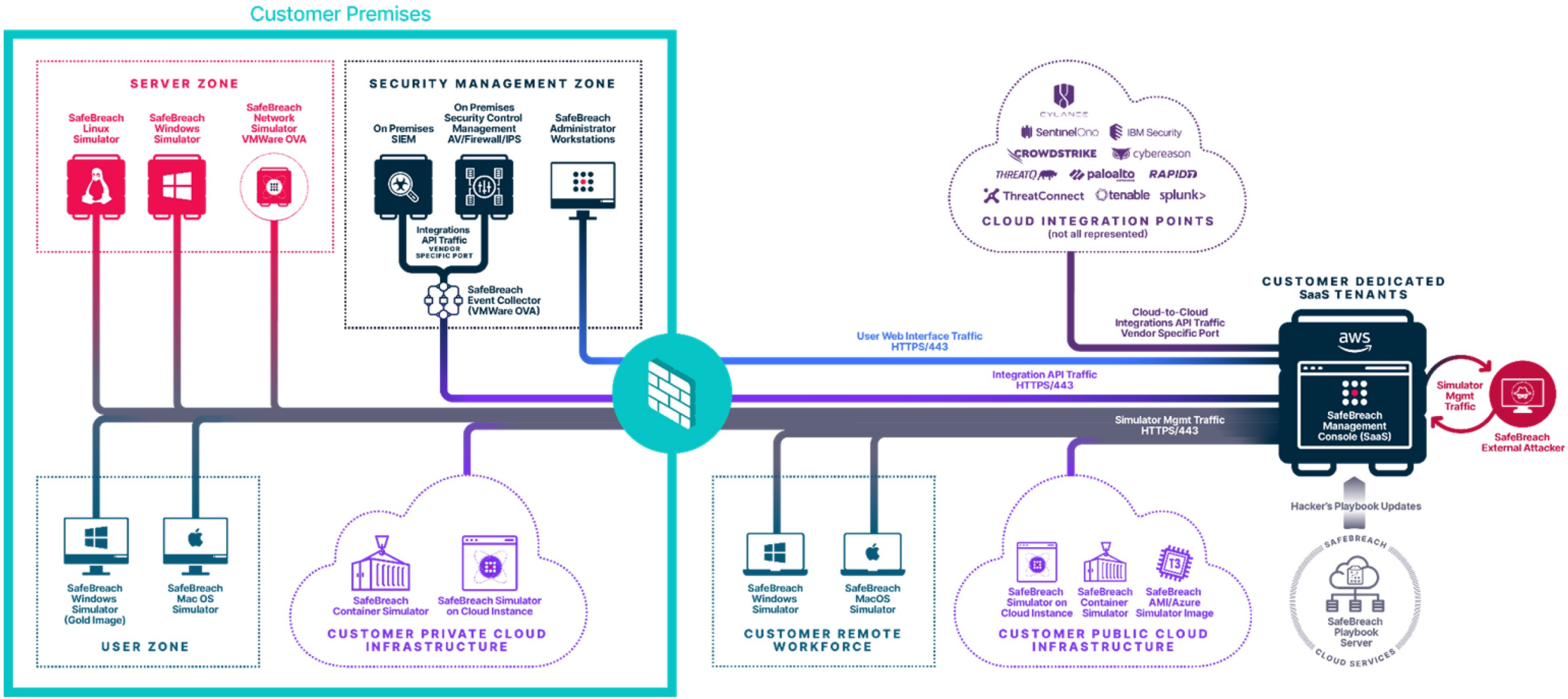
REGIERUNG

New Jersey Courts
Independence • Integrity • Fairness • Quality Service
ROWAN COUNTY NORTH CAROLINA Be an original.
RivCoNOW COMMUNITY NOW. SERVICES NOW.

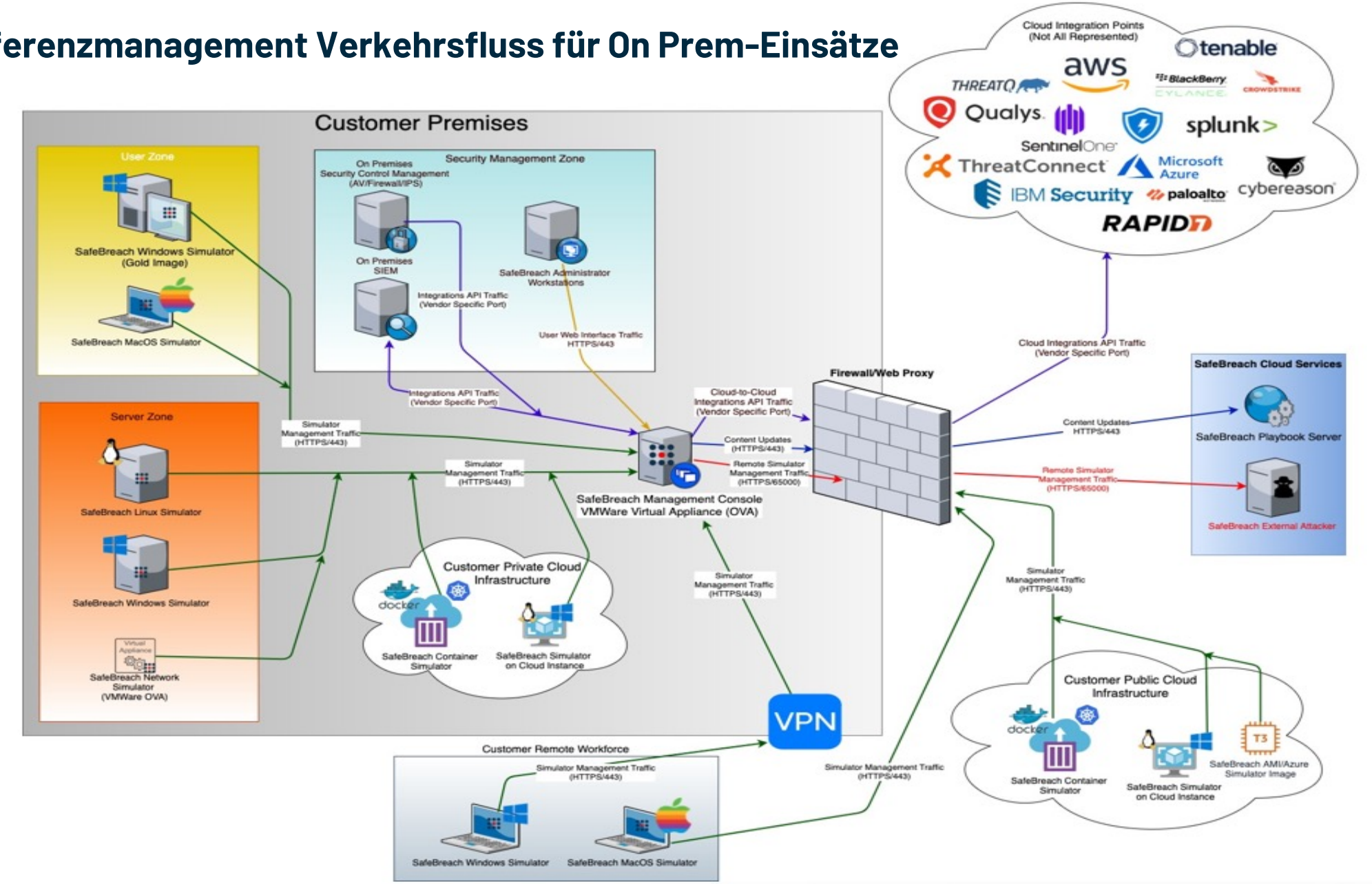
Referenzmanagement Verkehrsfluss für SaaS-Einsätze



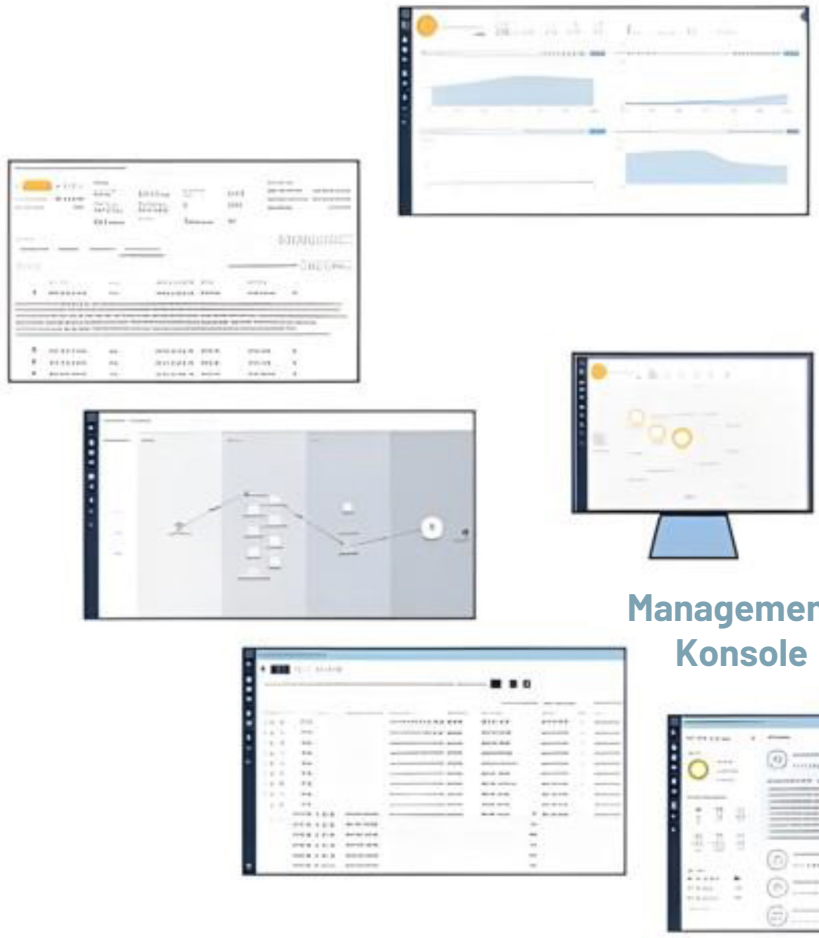
Referenzmanagement Verkehrsfluss für SaaS-Einsätze



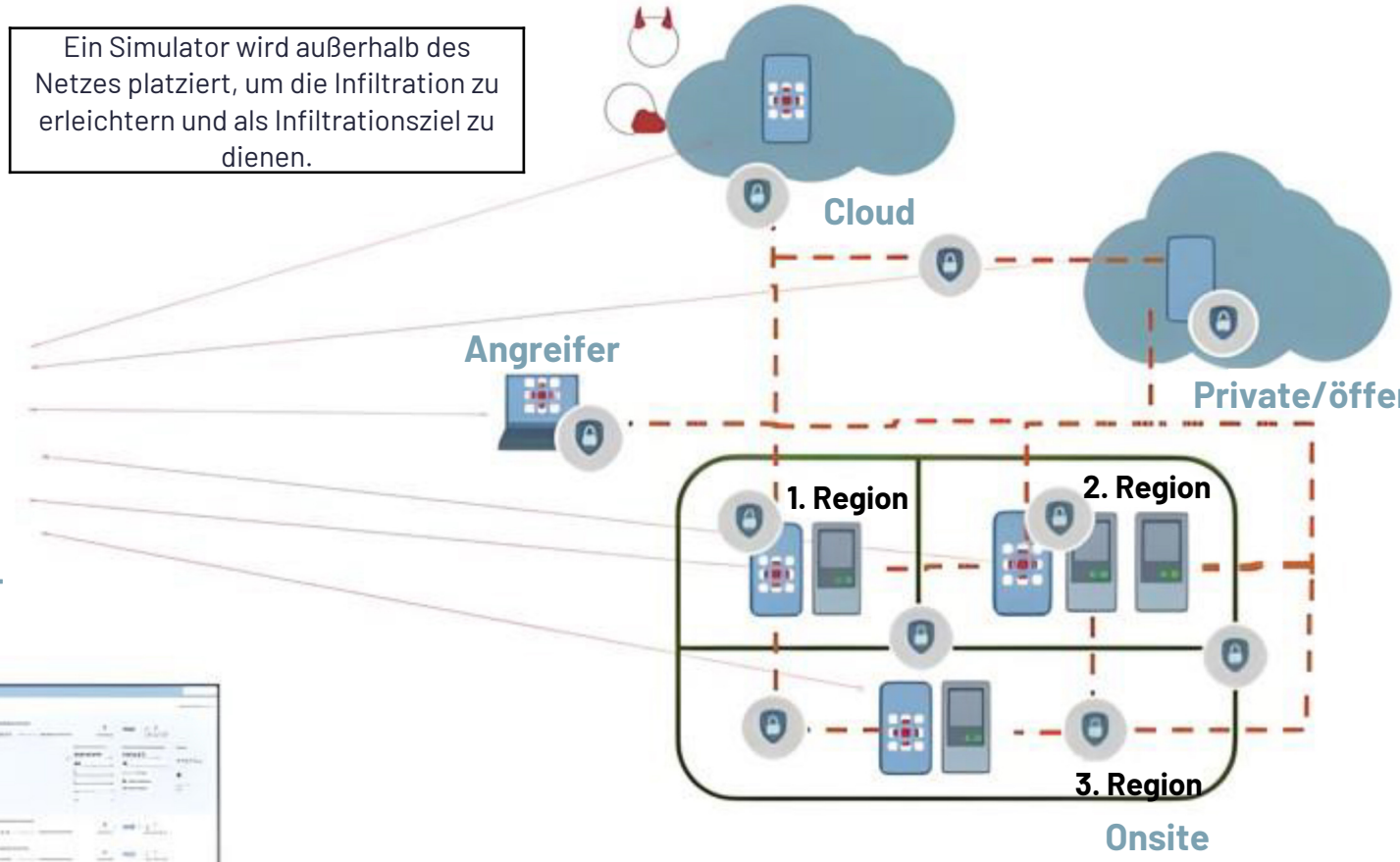
Referenzmanagement Verkehrsfluss für On Prem-Einsätze



OTD BİLİŞİM GLOBAL VAD



Ein Simulator wird außerhalb des Netzes platziert, um die Infiltration zu erleichtern und als Infiltrationsziel zu dienen.



Management-Konsole

Die Management-Konsole (MC) kommuniziert unabhängig und sicher mit jedem Simulator (Port 443) und weist ihn an, Simulationen durchzuführen. Die Simulatoren übermitteln ihre Ergebnisse an die MC, die diese dann analysiert und verschiedene Dashboards, mögliche Kill-Chain-Ansichten, Empfehlungen und Berichte erstellt.

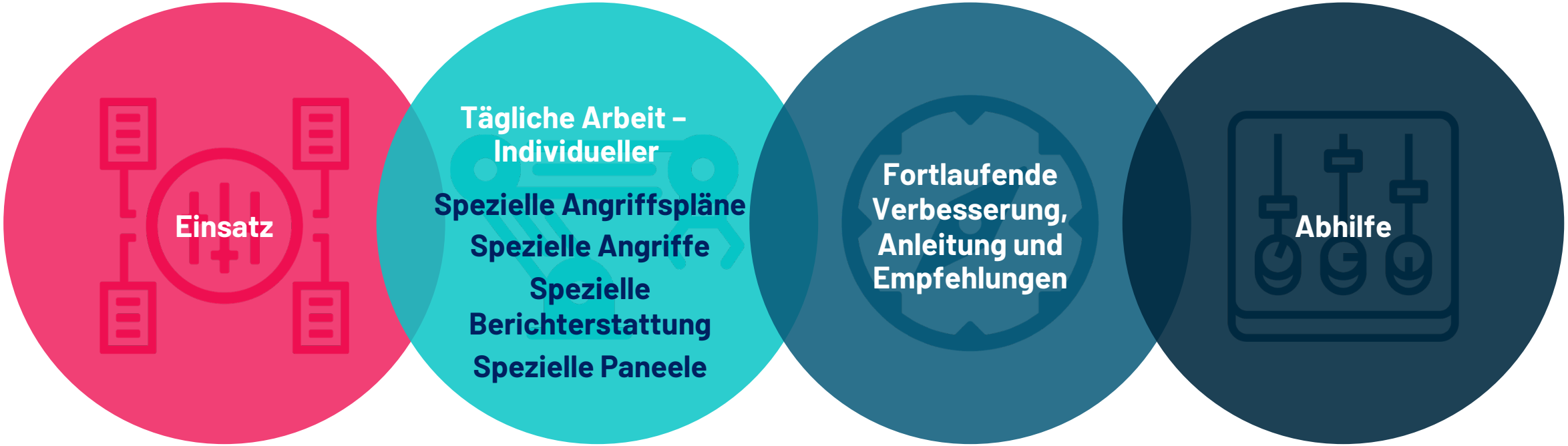
Diese Umgebung besteht aus 3 segmentierten Zonen mit verschiedenen Sicherheitskontrollen wie AV, EDR, Proxy, Secure Web Gateway, NexGen Firewall, IPS Sandbox usw.

Beschreibung

SafeBreach-Simulator
Sicherheitskntrolle
Vertretersysteme
Remote-Benutzer mit Simulator
Kommunikationspfad von der MC zu den Simulatoren
Mögliche Simulationspfade
Netzwerk-Segmentierung
Definiertes Infiltrationsziel
Definiertes Infiltrationsziel

Gehen Sie mit SafeBreach-as-a-Service von der Defensive in die Offensive: Die umfassendste BAS-Lösung

Alle Vorteile von SafeBreach bei der Verwaltung der Plattform



Ermöglicht Ihnen, sich auf Strategie, Verbesserung, Schadensbegrenzung und Festlegung von Standards zu konzentrieren und Ihre Sicherheitslage zu verbessern

Entriegeln Sie die Full-Kill-Chain durch agentenlose Sicherheitsauthentifizierung von Webanwendungen

SafeBreach für die Sicherheit von Webanwendungen

- Überprüfung der Full-Kill-Chain
- Der Umfang umfasst die zehn größten Sicherheitsrisiken der OWASP® Foundation
- Eine kontextualisierte Ansicht der Sicherheitslage von Webanwendungen
- Schneller und einfacher Einsatz
- Umsetzbare ROI-Berichte für Ihre WAF

OTD BİLİŞİM GLOBAL VAD

Anwendungsbeispiele

Wie passt das in Ihr Sicherheitsprogramm?

Kunden-Fallstudie

Top 3 US-Versicherer

Herausforderung

Beurteilung von Cyber-Risiken und Verbesserung der Sicherheitslage in OUs und nicht integrierten Organisationen

Lösung

SafeBreach wird in OUs und NIEs eingesetzt und testet kontinuierlich auf Infiltration, Host-Ebene, laterale Bewegung und Eindringen

SafeBreach Panels werden vierteljährlich an die C-Ebene und den Vorstand berichtet

Nutzen / ROI (Investitionsrentabilität)

Fähigkeit zur Verfolgung des Programmfortschritts auf der Grundlage einheitlicher KPIs

Fähigkeit, eine Verbesserung der Lage im Laufe der Zeit zu zeigen

Fähigkeit, Tausende von Lücken zu erkennen und zu beheben

Kunden-Fallstudie

Top 3 US-Finanzdienstleister

Herausforderung

Beurteilung der Segmentierungskontrollen für die wertvollsten Segmente

Beurteilung der Widerstandsfähigkeit gegen unmittelbare Bedrohungen in kurzer Zeit

Lösung

SafeBreach wird in allen wichtigen Segmenten eingesetzt, in SIEM integriert und überprüft kontinuierlich die Segmentierung.

Wird für SafeBreach SLA verwendet, um die US-CERT Sicherheitslage zu testen

Nutzen / ROI (Investitionsrentabilität)

Verringerung der Angriffsfläche von >80% auf <5% bei Netzkontrollen

Widerstandsfähigkeit bei unmittelbarer Bedrohung und die Fähigkeit, den Plan zur Schadensbegrenzung innerhalb von Tagen zu kommunizieren

Kunden-Fallstudie

PayPal

Herausforderung

Frühzeitige Bewertung des Cyber-Risikos bei Fusionen und Übernahmen, um Lücken zu erkennen und die Fusion zu planen

Lösung

Das M&A-Team führt den SafeBreach-Basistest bei jedem DD-Prozess durch und beurteilt die Cyber-Sicherheitslage innerhalb weniger Tage.

Nutzen / ROI (Investitionsrentabilität)

Beurteilt erworbene Risiken rechtzeitig auf ihre Auswirkungen

Bewertet das damit verbundene Fusionsbudget und die Auswirkungen

Effizienter und schneller Beurteilungsprozess

FALLSTUDIE

OTD BİLİŞİM GLOBAL VAD

Spear-Phishing- und „Living-off-the-Land“-Tools (LOTL) initiieren die Erkennung von OT-Angriffen

Überprüfung der E-Mail-, Endpunkt- und Netzwerkkontrolle

Angreifer zielten mit einer Phishing-Kampagne auf Produktionsmitarbeiter. Ein eingebetteter Link veranlasste die Malware, einen nicht zuordenbaren Kommunikationspfad zu einem C&C-Server zu erstellen. Mithilfe von LOTL-Tools haben Angreifer Anmeldeinformationen kompromittiert und Berechtigungen erweitert, um mit der Kartierung der erweiterten Netzwerkarchitektur zu beginnen und interessante OT-Ziele zu entdecken.

Ziel	Validierung von Endpunkt- und Netzwerkkontrollen, Sichtbarkeit und Verhinderung böswilliger Hostaktionen als Teil von Malware-Aktivitäten.
Prüfen	Wir haben Angriffssimulationen in verschiedenen Phasen der Malware-Kill-Chain durchgeführt, um Host-Kontrollen zu testen, einschließlich der Erkennung anomalem Verhalten, der Whitelist von Anwendungen und Richtlinien zur Systemsperrung. Wir führten Netzwerk-Exfiltration/Exfiltrationssimulationen durch, um zu überprüfen, ob Filterregeln, Sperrrichtlinien und Netzwerkperimeter-Sicherheitskontrollen wirksam gegen Indicators of Compromise (IOC) waren.
Ergebnisse	Die festgelegten Netzwerksegmentierungs- und Filterregeln waren unzureichend und bergen das potenzielle Risiko, öffentlich bekannte Schwachstellen auszunutzen und mehrere Open-Source-Tools zu nutzen, um Zugang zu sensiblen Netzwerken zu erhalten. Die Wirksamkeit der EDR-Richtlinie bei der Erkennung und Verhinderung böswilligen Verhaltens muss verbessert werden. Genehmigte Sicherheitskontrollen können durch die Anwendung des Prinzips der geringsten Rechte gestärkt werden. Es wird außerdem empfohlen, Befehlszeilen-Scripting-Aktivitäten und -Berechtigungen zu deaktivieren, da Bedrohungsakteure Schwierigkeiten haben werden, Berechtigungen zu erweitern und/oder sich seitlich zu bewegen. Verstärkte Webfilterkontrollen gegen böswillige C2-Kommunikation.

FALLSTUDIE

Schadsoftware, die kritische Infrastruktur lahmlegt und funktionsunfähig macht

Endpunkt- und Netzwerkkontrollauthentifizierung

Angreifer zielten mithilfe der Malware WhisperGate und Hermetic auf Windows-basierte HMIs im IKS-Netzwerk. Sie versuchten, den Master-Boot-Record zu manipulieren, die Geräte funktionsunfähig zu machen und die Stromerzeugung abzuschalten.

Ziel	Überprüfen Sie die Netzwerkkonfiguration und die Wirksamkeit von Netzwerksicherheitskontrollen, Endpunktkontrollen und Abhilfemaßnahmen.
Prüfen	Wir haben die SPAN-Port-Konfiguration überprüft. Wir haben eine Netzwerkangriffssimulation gegen Level-2- und Level-3-HMIs und Engineering-Workstations durchgeführt, um zu überprüfen, ob die OT-Sicherheitstools ordnungsgemäß funktionieren. Wir haben die Sicherheitskontrollen des OT-Netzwerks mit SafeBreach ICS-Angriffen (Netzwerkübertragungen) getestet.
Ergebnisse	Wir haben Lateral-Movement-Angriffe, Fehlkonfigurationen netzwerkbasierter Zugriffskontrolllisten (ACLs) und Systemschwachstellen identifiziert, die die Verbreitung von Malware ermöglichen. Die Ergebnisse zeigten, dass Netzwerksegmentierungs- und Filterregeln im Hinblick auf die potenziellen Risiken des Entfernens/Änderns von Konfigurationsattributen oder der Zerstörung von Firmware oder Systembinärdateien nicht ausreichen; Diese können die Verfügbarkeit kritischer Netzwerkressourcen isolieren oder verringern.

FALLSTUDIE

Speziell entwickelte OT-Ransomware

IT/OT-Sicherheitsauthentifizierung

Die Ransomware-Angriffe WannaCry und SNAKE zwangen zwei der zehn größten Autohersteller dazu, Produktionslinien zu schließen. Es wird angenommen, dass beide Angriffe durch Phishing und erfolgreich kompromittierte Windows-basierte IKS-Endpunkte verursacht werden.

Ziel

Überprüfen Sie die Netzwerkkonfiguration und die Wirksamkeit von Netzwerksicherheitskontrollen, Endpunktkontrollen und Abhilfemaßnahmen.

Prüfen

Wir führten simulierte Angriffe durch, um die Sicherheitskontrollen des Systems zu überprüfen und festzustellen, wo der Zugriff auf Daten, die Produktionsprozesse enthalten, eingeschränkt werden sollte, und um Schwachstellen in den Sicherheitskontrollen zu identifizieren, die das System mit Malware infizieren könnten.

Mit unserem EDR-Integrationstool (Endpoint Detection and Response) wurden spezifische Bedrohungsverhalten simuliert, um die Wirksamkeit der Endpunktkontrollen zu überprüfen und sicherzustellen, dass diese EDR-generierten Warnungen korrekt priorisiert wurden.

Ergebnisse

Simulationen seitlicher Bewegungen validierten Sicherheitskontrollen, und die minimale Wirksamkeit der Netzwerksegmentierungs- und Filterregeln führte zur Implementierung und Implementierung einer mehrschichtigen Netzwerksegmentierung, wobei sich die kritischsten Kommunikationen und Daten auf der sichersten und zuverlässigsten Schicht, dem Whisper Gate, befinden.

Die Webfilterkontrollen wurden für bösartige Remote-Überwachungs- und -Verwaltungssoftware sowie für Remote-Desktop-Softwareanwendungen, die bei der Ausnutzung bösartiger Exploits helfen, verstärkt.

FALLSTUDIE

Ein Angriff auf die Lieferkette nutzt eine schlechte Netzwerksegmentierung aus, um die OT-Umgebung zu infiltrieren

Überprüfung des Netzwerkumfangs und der Segmentierung

Cyberkriminelle haben einen HLK-Anbieter ins Visier genommen, um sich Fernzugriff auf das OT-Netzwerk seiner Kunden zu verschaffen. Sobald sie drinnen waren, bewegten sich die Angreifer seitlich vom Standortnetzwerk zum OT-Netzwerk in der Produktionsanlage.

Ziel	Erhalten Sie Einblick in die Wirksamkeit kompensierender Kontrollen in der OT-Umgebung. Zur Überprüfung: OT-Systeme sind trotz des Patch-Lebenszyklus ausreichend geschützt.
Prüfen	Wir führten Angriffe in kritischen Prozessbereichen durch – Validierung von Segmentierungsrichtlinien, Netzwerkkontrolle und Bedrohungsprävention in kritischen Segmenten, innerhalb jedes Prozessbereichs und zwischen Prozessbereichen. Endpunktangriffe, um zu überprüfen, ob native Schutzmaßnahmen wie Anwendungs-Whitelisting und Sperrrichtlinien gegen bestimmte Angreifer wirksam sind Techniken haben wir es möglich gemacht.
Ergebnisse	Die Simulationsergebnisse bestätigten, dass die Sicherheitskontrollen durch die Implementierung minimaler Zugriffsmuster und eine umfassende Verteidigung gestärkt werden können, um erfolgreiche Ausnutzungsversuche zu verhindern. Lateral-Movement-Simulationen bestätigten die Notwendigkeit einer erweiterten Netzwerksegmentierung durch die Unterteilung von OT-Netzwerken nach Rollen und Anforderungen.

OTD BİLİŞİM
GLOBAL VAD

Mit Secure Breach für OT...

"SafeBreach hat uns wirklich geholfen, einen umfassenderen Blick auf unsere IT- und OT-Netzwerke zu werfen. Durch das Testen unserer Kontrollen über potenzielle Eintrittspunkte und kritische Verbindungen zwischen den beiden Netzwerken konnten wir unsere Behebungsbemühungen viel effizienter priorisieren."

Globaler Pharma-CISO

SafeBreach

Danke

OTD BİLİŞİM GLOBAL VAD

ICT OTD PREFER EXPERIENCE ONLINE Since 2011