

ZERO TRUST
PENTESTING
CVE-SCAN
INTRUSION
DETECTION
PREVENTION
MONITORING
ASSET
MANAGEMENT

UNSICHTBARES SICHTBAR MACHEN

Unsicheres sicher machen!



Seien Sie den Angreifern einen Schritt voraus.
Schaffen Sie eine **proaktive IT-Sicherheit** ganz automatisch.

Dabei erhalten Sie mit Enginsight eine einmalige Kombination aus Angriff und Verteidigung!

Auf Basis unserer einzigartigen IT-Architektur, schützen Sie Ihre IT mit modernsten Technologien, welche bisher nur Großunternehmen zugänglich waren.



Über 200 Vertragskunden mit unterschiedlichen Anwendungsfällen

Gemeinsam mit unserem Partner bieten wir Lösungen für alle Branchen:

- Verschiedene verarbeitende Industrien
- Öffentlicher Sektor
- Gesundheitssektor
- Kritische Infrastrukturen, z. B. Energieversorger, öffentliche Versorgungsunternehmen
- Immobilien/Wohnungsbaugenossenschaften

 Leipziger

 Langeoog

 HanseYachts
Aktiengesellschaft



 HDI



 REGIOCAST
Deutsches Radiounternehmen

 NEUROLOGISCHE
KLINIK WESTEND



Mehr als ein Zuhause



Freistaat
Thüringen  Ministerium
für Bildung,
Jugend und Sport

**STADTWERKE
MÜHLACKER**

Energie • Menschen • Service

 Qsil

Cybersecurity ist ein Megatrend, aber kein einfaches Thema. Simplify Security ist das nächste große Ding!

4,4 Billionen Euro: Schadenswert für die nächsten 5 Jahre

60% der Cyberangriffe zielen auf KMU

60% der KMU-Opfer haben sich nicht erholt und innerhalb von 6 Monaten den Betrieb eingestellt.

68% haben/hatten kein systematisches Cybersicherheitskonzept




Cyber Security become the game changer for companies.




Cybersecurity is a business problem.



Security hole Log4Shell: Internet on fire



**Fast alle Unternehmen sind blind in ihrer internen IT.
Deshalb nehmen erfolgreiche Angriffe
auch trotz Firewall und Antivir zu.**



Innovation durch Einfachheit!

Eine einzigartige IT-Architektur zur Früherkennung und Abwehr von Cyberangriffen.



- Security Analytics & Threat Detection
- Dezentrale Architektur
- Ihr Weg zu Zero Trust

ANGRIFF

VERTEIDIGUNG

100% selfmade in Jena

100% own code base / OPEN API

- Individuelle Metriken
- Monitoring Prozesse/Services
- Anomalieerkennung

- Schwachstellen-Scans
- Sicherheits-Konfigurationen
- Ports, Software, Verbindungen

- Live Inventar
- Asset Management
- Health Checks (Ping,Port,SNMP)

- Automatische Pentests
- Remote Actions
- Patchmanagement

- Intrusion Detection
- Intrusion Prevention
- Mikrosegmentierung

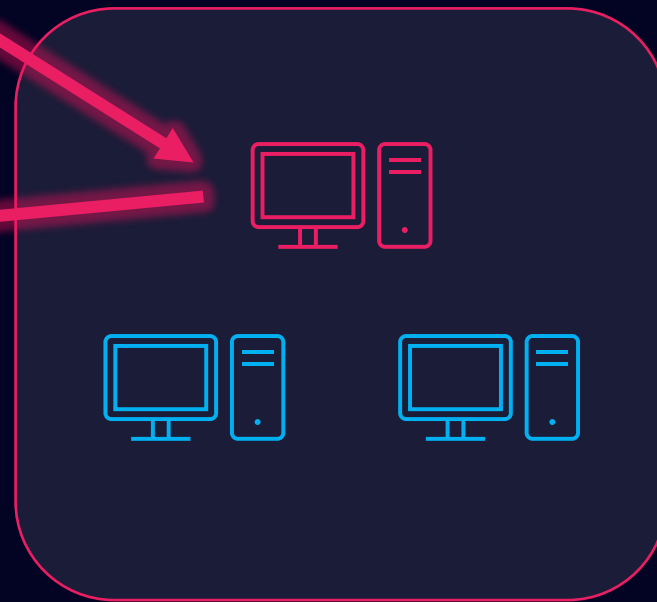
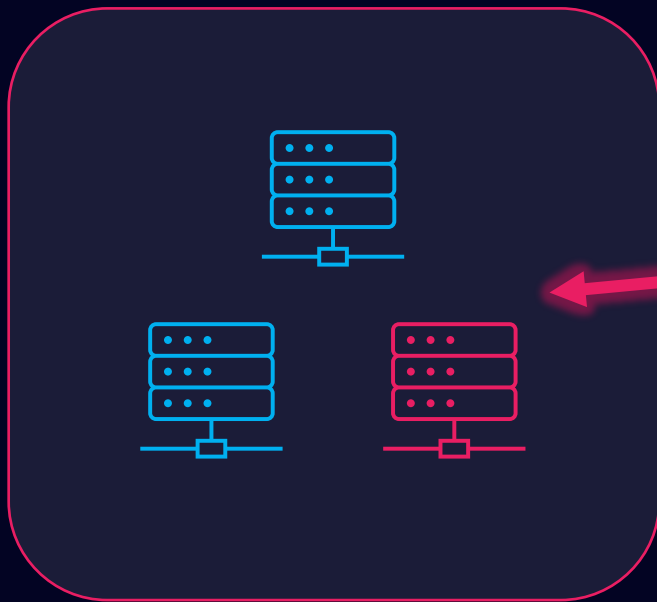
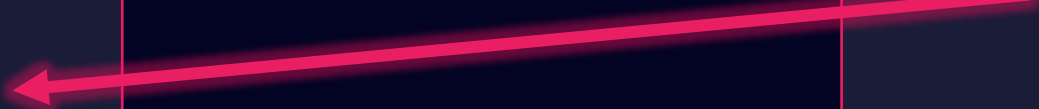
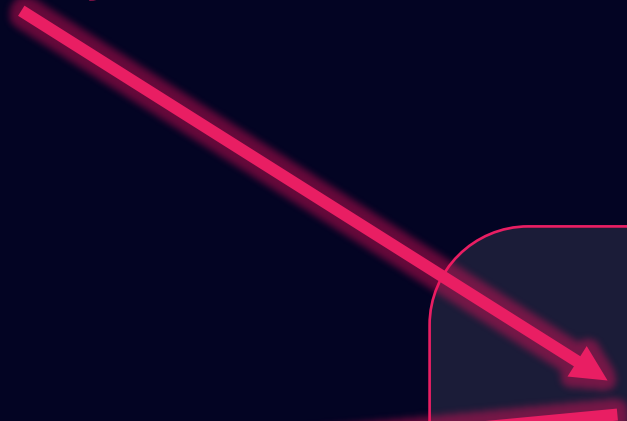
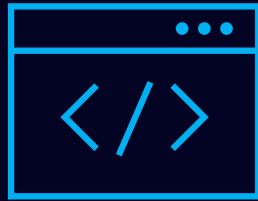
KI-Monitoring

IT-SEC Frühwarnsystem

IT-Management

Security Automation

Netzwerksicherheit



1. Teil eines Botnetzwerk (Strafrecht)
2. Korrumpierung der Webseiten-Nutzer (DSGVO)
3. Trusted Domain Zugriff auf interne Systeme



Ihr Start mit Enginsight

 ENGINSIGHT

In eine sichere Zukunft

Sec Audit

- Automatisches Pentesting der gesamten IT
- Web-Security + BSI-Check Webseite
- Schwachstellen-Scan
- Konfig-Checks
- Patchstand
- Netzwerkanomalie-Erkennung

Lizenzgeschäft

- Enterprise Security für den Mittelstand
- Host basiertes Intrusion Detection / Prevention
- Mikrosegmentierung
- Automatische Securityüberwachung
- Attraktives Partnermodell
- Planbare, wiederkehrende Umsätze



Vertraulich



Erstellt von
Showcase GmbH
Endpunktbericht

Bericht erstellt für

http://enginsight.com

Bericht vom
12.10.20 14:26:13 CEST
Bericht für den Zeitraum
05.10.20 14:26:13 CEST - 12.10.20 14:26:13 CEST

Technischer Verantwortlicher
—
CName
—
Fachlicher Verantwortlicher
—
Zertifikat gültig bis
30.11.2020 01:05:58 CET

Domain
enginsight.com

DNS Records
78.47.155.68

Mit ❤️ erstellt von Enginsight

Seite 1 von 20 | 12.10.2020 14:26:13 CEST

Ihr Security-Audit

- Prüfung auf Schwachstellen aus der Sicht eines Angreifers
- Server-, Client-, Web- und Netzwerksicherheit
- Durchführung: 1-2 Tage

Suchen +

Penetrationstests > Audits > Zusammenfassung

→ ZU DEN DETAILS + REPORT ERSTELLEN

DRINGLICHKEIT	ERGEBNISSE	KATEGORIEN	ANZAHL
CRITICAL	<p>Kritische Sicherheitslücke Es wurden kritische Sicherheitslücken (CVE) detektiert. Die verwundbaren Systeme gefährden massiv den sicheren Betrieb der IT-Umgebung.</p> <p>Empfehlung Es sollte unmittelbar überprüft werden, ob alle verfügbaren Sicherheitspatches eingespielt wurden und gegebenenfalls Updates eingespielt werden. Sofern für veraltete Systeme keine Updates mehr erscheinen, sollte ein Umstieg auf einen aktuellen Service erwogen werden.</p> <p>► Details anzeigen</p>	CVEs	2
CRITICAL	<p>Bruteforce HTTP Web Forms Für HTTP Web Forms werden eine oder mehrere unsichere Benutzer-Passwort-Kombinationen verwendet.</p> <p>Empfehlung Die Anmeldedaten sollten zügig nach den Kriterien für sichere Passwörter angepasst werden.</p> <p>► Details anzeigen</p>	Authentication	2
HIGH	<p>Verwendet gewöhnlichen Community String Für SNMP werden eine oder mehrere Community Strings zur Nutzerauthentifizierung verwendet, die häufig verwendet werden und daher besonders unsicher sind.</p> <p>Empfehlung Falls möglich, sollte eine Umstellung auf SNMPv3 erfolgen, da ab dieser Version eine Authentifizierung mittels Benutzername und Kennwort zur Verfügung steht.</p> <p>► Details anzeigen</p>	Enumeration	3
HIGH	<p>Anfällig für Logjam Attacken Indem eine Schwachstelle im Diffie-Hellman-Schlüsselaustausch ausgenutzt wird, kommen Angreifer an die geheimen Schlüssel.</p> <p>► Details anzeigen</p>	Encryption	2
HIGH	<p>Erlaubt Lesezugriff Ein Lesezugriff auf Object Identifier (OID) ist via SNMP möglich.</p> <p>Empfehlung</p>	Privileges	3

Risikoscore
Am stärksten gefährdete Assets gemäß Risikoscore.

192.168.178.69	32
192.168.178.83	27
192.168.178.22	27
192.168.178.44	7
192.168.178.1	6

Kategorien
Anzahl der nicht-bestandenen Checks pro Kategorie.

Enumeration	122
Encryption	22
Application	8
Authentication	5
CVEs	4
Privileges	3

Dringlichkeit
Anzahl der durchgeführten Checks pro Dringlichkeit.

Oks	451
Lows	107
Mediums	40
Highs	13
Criticals	4
Errors	268

WENN RECHT IST
STARTE ICH DEN
ANGRIFF
AUF IHR NETZWERK
SO GEGEN 10?*

* kein Hacker, jemals

Warten Sie nicht darauf,
sondern testen Sie
Enginsight noch heute!

kostenlos unter:
enginsight.com