Cyber Defence & Incident Response

Beseitigen Sie Cyberrisiken mit InfoGuard

InfoGuard
SWISS CYBER SECURITY

24/7 Cyber Defence Services aus der Schweiz

Managed Detection & Response
Hunting & Intelligence
Security Operations
Incident Response & Recovery
Forensics

Cyber Defence Services
Weil Cybercrime, Fachkräftemangel und reduzierte Budgets Realität sind

Die höchste Gefahrenstufe ist erreicht. Aktuelle Studien prognostizieren Schäden von $ 10,5 Billionen jährlich. Cyberattacken zählen zu den grössten operationellen Unternehmensrisiken und sind vergleichbar mit einer heimtückischen Naturgewalt, die mit fataler Kraft zuschlagen kann. Jederzeit und überall.

Im schlimmsten Fall überrollen Cyberangriffe Unternehmen unvorbereitet – genau wie eine Lawine, die plötzlich und ohne Vorwarnung zuschlägt. Weil jede Sekunde zählt und jede Bewegung die Lawine ins Rollen bringen kann, ist ein dediziertes Security Operations Center (SOC) die Lösung. Das erfolgreiche Zusammenspiel von erfahrenen Expert*innen, neuester Technologie und etablierten Prozessen innerhalb eines SOC hilft Unternehmen, sich effizient und effektiv vor Angriffen zu schützen.

Eine enorme Herausforderung! Für Unternehmen jeder Grösse ist es äusserst schwierig, erfahrene Sicherheitsfachleute zu finden. Gleichzeitig bedeutet der Aufbau und 24/7-Betrieb eines SOC eine beträchtliche Investition. Ein Unterfangen, das sich sehr viele Unternehmen nicht leisten wollen.

Was Sie nicht sehen, können Sie nicht schützen

Erschwerend kommt hinzu, dass die meisten Unternehmen keinen vollständigen Einblick in ihre Sicherheitsinfrastruktur haben und täglich mit einer riesigen Flut von Warnungen konfrontiert werden. Dies führt zu einer Überlastung der Sicherheitsteams, kritische Alarme werden übersehen und es entstehen Lücken in der Cybersicherheit.

Cyber Defence ein Muss für Ihre Compliance

Angesichts der wachsenden Bedrohung durch Cyberangriffe ist es unerlässlich, die eigene Cyberresilienz zu stärken. Das NIST Cybersecurity Framework, Cyber Resilience Act, NIS2, DORA, IKT-Minimalstandard und viele weitere Regulatorien fordern dies explizit ein. Eine Nichterfüllung hat massive Sanktionen zur Folge. Darüber hinaus verursachen Cybervorfälle existenzbedrohende Schäden und resultieren in einem massiven Reputationsverlust.

Wie gehen Sie damit um?

- Kennen Sie die aktuelle Cyberbedrohungslage für Ihr Unternehmen?
- Haben Sie die notwendige Visibilität, um Cyberangreifer in Ihrem Netzwerk zu erkennen?
- Können Sie 24/7 Cyberangriffe abwehren, bevor ein Schaden entsteht?
- Sind Sie in der Lage, auf Cyberangriffe umgehend zu reagieren?
- Können Sie im Ernstfall zeitnah Ihre Handlungsfähigkeit wiederherstellen?

Die Lösung: Die Auslagerung dieser anspruchsvollen Aufgabe an einen erfahrenen Managed Detection & Response (MDR) Dienstleister.

Cyber Defence & Incident Response
Cyberangriffe erkennen, abwehren und handlungsfähig bleiben

Höchste Priorität der InfoGuard Cyber Defence Services geniesst die Rund-um-die-Uhr-Überwachung – als SOC-as-a-Service oder Co-Managed SOC – Ihrer gesamten Infrastruktur, damit Cyberangriffe umgehend erkannt und erfolgreich abgewehrt werden können. Damit der Cyber Defence Service schnell aktiviert werden kann, basiert dieser auf Ihrer bestehenden Infrastruktur.

Die Inhouse-Entwicklungsarbeit der InfoGuard, fortlaufende Investitionen in unser Cyber Defence Center, der Einsatz von «Best of Breed» Sensorik sowie unsere in der Schweiz entwickelte und gehostete Plattform stellen sicher, dass auf veränderte Kundenbedürfnisse, neue regulatorische Vorgaben und technologische Weiterentwicklungen schnell reagiert werden kann.

Bei einem Sicherheitsvorfall stehen der Schutz vor einem Business-Impact und die rasche Wiederherstellung Ihrer Handlungsfähigkeit durch unser eigenes CSIRT im Zentrum. Gleichzeitig analysieren wir mittels forensischer Untersuchungen die Ursachen und Angriffsvektoren, damit Ihre Cybersicherheit nachhaltig optimiert wird.

Wir begleiten Sie auf Ihrer ganzen Security Journey. Unser Service-Management-Team trifft sich regelmässig mit Ihnen, um vergangene Ereignisse zu reflektieren, Optimierungsmöglichkeiten zu diskutieren und über Veränderungen der Cyberbedrohungslage zu orientieren. Dank unserer Erfahrung und Erkenntnissen bei vielen anderen Kunden profitieren Sie von massgeschneiderten Sicherheitsempfehlungen, die Ihre Cybersicherheit stetig verbessern.

Bei all unseren Kunden mit einem MDR-Service konnten wir erfolgreich Business-Impacts durch Cyberangriffe verhindern.

InfoGuard CYBER DEFENCE CENTER

Profitieren Sie von unserer langjährigen Erfahrung:

24/7
Managed Detection & Response Services aus unserem CDC in der Schweiz

80+
Experten in dedizierten SOC-, CSIRT- und Threat-Intelligence-Teams, Total 250+ Experten

12+
Jahre SOC-Erfahrung & Kompetenz

300+
Cyber Defence- & CSIRT-Kunden

4
Wochen für das strukturierte SOC-Onboarding

Hunderte Incident-Response-Fälle pro Jahr

BSI-qualifizierter APT-Response-Dienstleister, FIRST-Mitglied

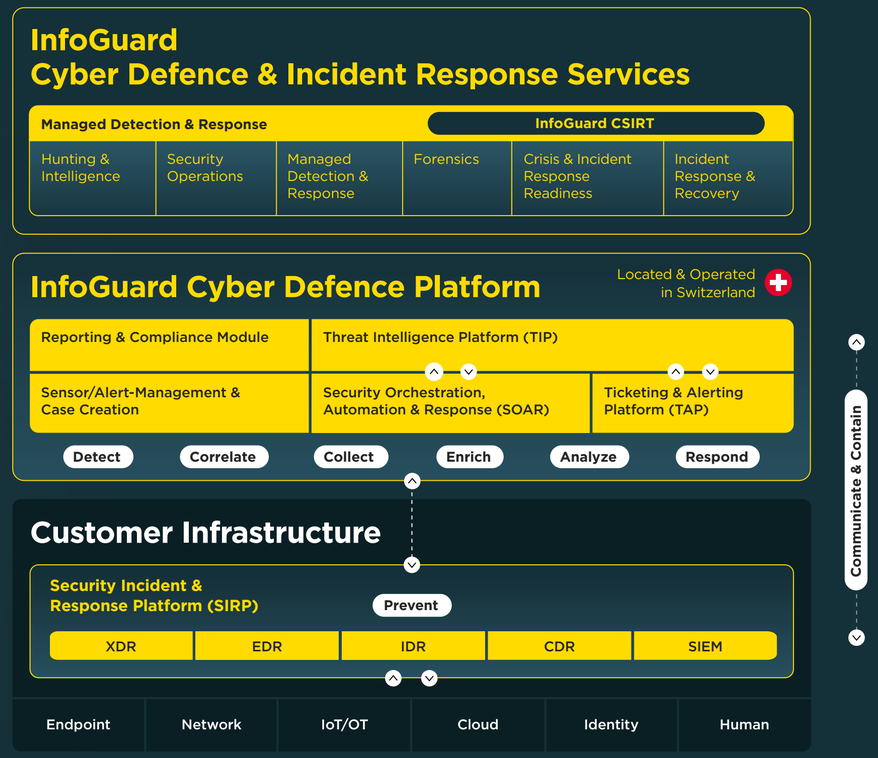
Swiss SOC Platform

InfoGuard Cyber Defence Platform – Herzstück einer effektiven und effizienten Cyberabwehr

Die eigenentwickelte, hochskalierbare und On-prem in der Schweiz betriebene InfoGuard Cyber Defence Platform bildet das Kernstück unserer Cyber Defence Services und basiert auf einer offenen XDR-Architektur. Dies erlaubt es Ihnen, unsere Services auch als Co-Managed SOC zu nutzen. Um sicherzustellen, dass wir Bedrohungen aus allen Blickwinkeln sehen, sammelt die Plattform Daten von Endgeräten, Netzwerken, IoT-/OT-Infrastrukturen, Cloudumgebungen und Identitäten. Durch die Automatisierung lassen sich individuelle Kundenbedürfnisse effizient umsetzen.

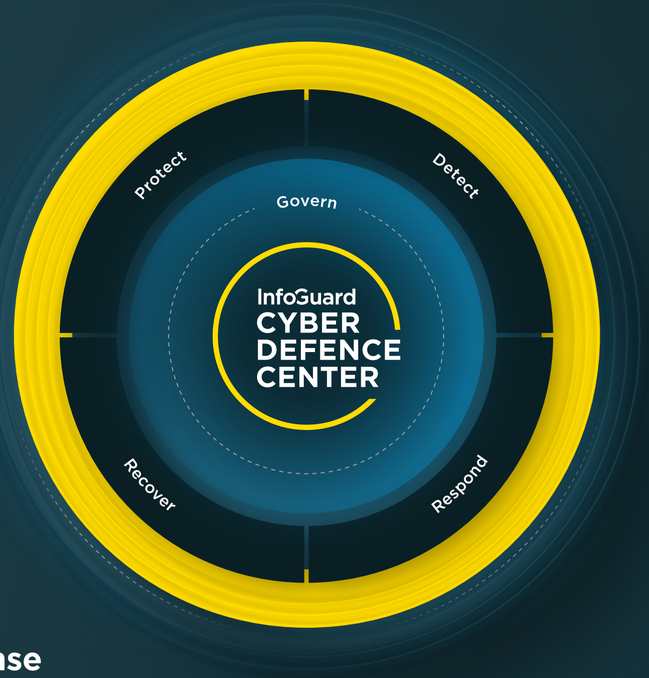
Durch die Nutzung unterschiedlicher Erkennungsmethoden, einschliesslich Machine und Deep Learning, kann die Plattform schnell Anomalien und verdächtige Verhaltensweisen aufdecken und mit Erkenntnissen aus aktuellen Sicherheitsvorfällen, simulierten Cyberattacken und Threat-Intelligence-Feeds anreichern. Dank der Schwarmintelligenz von Hunderten Kunden, täglich Tausenden von Sicherheitsereignissen und Hunderten von IR-Fällen ist der bestmögliche Schutz und die schnellstmögliche Reaktion garantiert. Bedrohungsalarme können bei verteilten IT-Infrastrukturen gezielt an die zuständigen Stellen weitergeleitet werden.

Die Plattform bietet umfassende Transparenz und arbeitet nahtlos mit Ihrem bestehenden Technologie-Stack zusammen. Dies verkürzt das Onboarding und eliminiert die Herstellerabhängigkeit. Zudem ist sichergestellt, dass sensitive Kundendaten jederzeit geschützt sind und ausschliesslich in unserem Data Center in der Schweiz gespeichert werden.



Cyber Defence & Incident Response Services vom Schweizer Experten

Umfassender Schutz vor Cyberangriffen



Govern, Identify & Protect

Hunting & Intelligence

Unser Threat-Intelligence-Team sucht aktiv nach Angriffsindikatoren in Ihrer Infrastruktur und Cyberbedrohungen im Darknet. Profitieren Sie von unseren Erfahrungen aus aktuellen Cybercrime-Vorfällen, Hunderten von Incident-Response-Fällen sowie aus Erkenntnissen unseres Red Teams.

- Compromise Assessment
- Threat Hunting
- Cyber Threat Intelligence (CTI)
- Cyber Deception
- Security Consulting
- Cyber Security Assessments
- Penetration Testing & Red Teaming

Protect

24/7 Security Operations

Dank dem Einsatz unserer Managed XDR- und SIEM-Services werden Cyberangriffe erkannt und gezielt abgewehrt. Zur Bewältigung der sich ständig verändernden Bedrohungslandschaft gehört auch die permanente Schwachstellenüberprüfung und Überwachung potenzieller Angriffsrisiken. Unsere Cybersecurity-Spezialist*innen decken frühzeitig Veränderungen Ihrer Schwachstellen und Fehlkonfigurationen auf.

- Managed XDR, SIEM/Vulnerability
- Vulnerability Management
- Digital Risk Exposure Service
- Cloud Security
- Managed Security & Network

Detect & Respond

24/7 Managed Detection & Response (MDR)

Überwachung Ihrer Endgeräte, Identitäten, Netzwerke und Cloud-Umgebungen durch unser Cyber Defence Center in der Schweiz, eigener Cyber-Defence-Plattform, erfahrenen Expert*innen und etablierten Prozessen sowie dem Einsatz führender, KI-basierter Detection & Response-Technologie, damit Sie moderne Cyberangriffe erkennen, abwehren und Ihre Handlungsfähigkeit sicherstellen können.

- Extended Detection & Response (XDR)
- Endpoint Detection & Response (EDR)
- Identity Detection & Response (IDR)
- Network Detection & Response (NDR)
- Cloud Detection & Response (CDR)
- Security Information & Event Management (SIEM)

Respond & Recover

Incident Response & Recovery

Erfolgreiche Cyberangriffe können nie vollständig ausgeschlossen werden. Entscheidend ist die schnelle und professionelle Intervention durch ausgewiesene Expert*innen. Unser eigenes CSIRT (Computer Security Incident Response Team) steht Ihnen rund um die Uhr zur Seite und garantiert Ihnen eine schnelle Wiederherstellung Ihrer Handlungsfähigkeit. InfoGuard ist BSI-qualifizierter APT-Responder, Mitglied bei FIRST (Forum of Incident Response and Security Teams) und agiert zudem als Incident-Response-Partner und Schadensabwickler von führenden Versicherungen und Brokern. Der Incident Response & Recovery-Prozess ist in jedem SOC-Prozess nahtlos integriert.

- Incident Response & Recovery
- Incident Response Retainer
- Crisis & Recovery Management
- Negotiation & Legal Support
- Payment Support

Recover

Forensics

Wenn Cyberangriffe zu einer Datenverletzung oder zu einem Cybervorfall führen, benötigen Sie einen erfahrenen Partner an Ihrer Seite. Unsere Analysten und Forensiker helfen Ihnen bei der Aufklärung von Sicherheitsvorfällen mit forensischen Analysen und stellen sicher, dass Sie Ihre Cybersicherheit nachhaltig optimieren können. Dabei kümmern wir uns aktiv um die Sicherung, Analyse und Bewertung von digitalen Spuren und Beweismitteln in Ihrer gesamten Infrastruktur. Die Analysen und Beweise können vor Gericht verwendet werden.

- Large Scale Forensics
- Network, Computer & Memory Forensics
- OT & IoT Forensics
- Cloud, Mobile & E-Mail Forensics
- Malware Reverse Engineering
- Expert & 2nd Opinion for IR Cases

Prevent & Recover

Crisis & Incident Response Readiness

Für Unternehmen ist es entscheidend, sich professionell auf einen möglichen Sicherheitsvorfall vorzubereiten. Zusammen mit Ihnen erarbeiten wir in einem gemeinsamen Workshop entlang unserer eigens entwickelten und bewährten Templates sowie unserer Erfahrung aus Hunderten von Cybervorfällen den Notbetrieb, das Krisenmanagement, die Bewältigung und Wiederherstellung der Infrastruktur sowie den kontinuierlichen Verbesserungsprozess.

- IR Readiness Assessment
- IR & Recovery Plan
- IR Table Top Simulation

Securing
Your Digital
World

InfoGuard
SWISS CYBER SECURITY

Ihre Cybersicherheit
Unsere Leidenschaft & Expertise

Cyber Defence & Incident Response sind entscheidend, aber nur zwei Aspekte einer umfassenden und erfolgreichen Cybersicherheit. Unser 360°-Cyber-Security-Ansatz umfasst zudem Cloud Security, Managed Security & Network Solutions für IT-, OT- und Cloud-Infrastrukturen, Penetration Testing & Red Teaming sowie Security Consulting Services. Unsere Services erbringen wir aus dem ISO 27001-zertifizierten und ISAE 3000 Typ 2 überprüften Cyber Defence Center in der Schweiz.

2001
Erfahrung und Expertise seit über 20 Jahren

100%
eigenständig

250+
Sicherheits-expert*innen

4
Standorte in der Schweiz, Deutschland und Österreich

24/7
Echtzeit-überwachung und Notfall-Intervention

ISO 27001
ISO 14001
ISAE 3000 Typ 2

Swiss Cyber Defence Center CDC

CSIRT
Computer Security Incident Response Team
BSI-qualifizierter APT-Response-Dienstleister und FIRST-Mitglied

Haben Sie einen Sicherheitsvorfall?
Wir unterstützen Sie jederzeit schnell, kompetent und erfahren.

+41 41 749 19 99

DE +49 896 142 9677

AT +43 1 442 0177

investigations@infoguard.ch

Baar (Hauptsitz)
InfoGuard AG
Lindenstrasse 10
6340 Baar
Schweiz
+41 41 749 19 00
info@infoguard.ch
infoguard.ch

Bern
InfoGuard AG
Stauffacherstrasse 141
3014 Bern
Schweiz
+41 31 556 19 00
info@infoguard.ch
infoguard.ch

München
InfoGuard Deutschland GmbH
Landsberger Straße 302
80687 München
Deutschland
+49 896 142 9660
info@infoguard.de
infoguard.de

Wien
InfoGuard GmbH
Graben 19
1010 Wien
Österreich
+43 1 442 0170
info@infoguard.at
infoguard.at