» You better know your enemy. «

CONSECUR CYBER DEFENSE CENTER (CDC)

ConSecur
[security and consulting]

Als herstellerunabhängiges Beratungs- und Dienstleistungsunternehmen befasst sich die ConSecur GmbH mit der Planung und Umsetzung von Maßnahmen zur Informationssicherheit. Unsere Leidenschaft ist die Entwicklung, Bewertung und Realisierung von IT-Sicherheitskonzepten für Unternehmen. So beschützen wir die Information, die Sie täglich für Einkauf, Produktion, Dienstleistung, Logistik und Korrespondenz benötigen. ConSecur hat sich darauf spezialisiert Informationssicherheit an die Geschäftsprozesse im organisatorischen und informationstechnischen Umfeld anzubinden.

CONSECUR – NEXT LEVEL INFORMATION SECURITY

INHALT

Cyber Defense Center	4
Warum Cyber Defense mit ConSecur?	6
Warum brauchen wir Securiosity?	7
Managed Cyber Defense aufbauen	8
IT-Security Analyse	10
SIEM Engineering	12
Threat Intelligence	14
Digital Forensics and Incident Response (DFIR)	16

Cyber Defense Center

Im Cyber Defense Center erkennen wir Sicherheitsereignisse in Netzwerk-Infrastrukturen – zügig und 24/7.

Unternehmen und Organisationen buchen diesen Schutzschild als Managed Service inklusive Fachpersonal und modernster technologischer Unterstützung.

Im Cyber Defense Center sehen wir besser zweimal hin, um Cyber Attacken auf die Spur zu kommen. Dieses Intrinsische, die Extra-Meile zu gehen, verbindet uns.

Warum brauchen wir Securiosity?

Im Cyber Defense Center arbeiten wir 24/7 in drei Schichten zusammen, um Cyber Attacken zu erkennen.

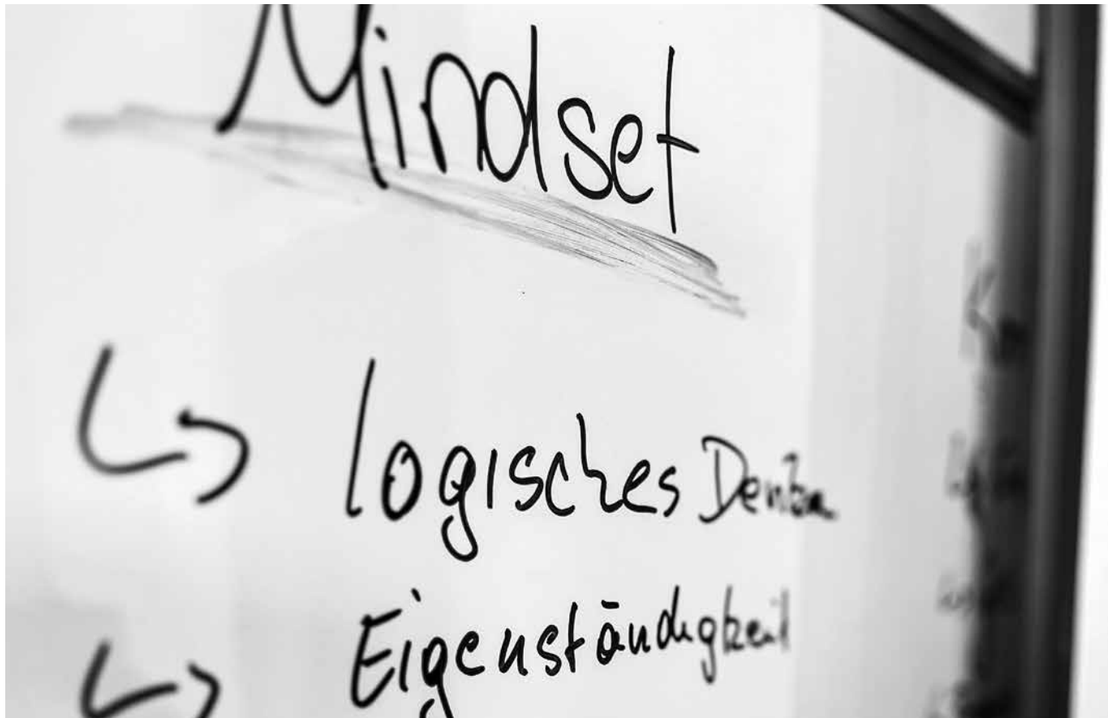
Angriffe, die mit krimineller Energie entwickelt worden sind.
Angriffe, die mit Unterstützung künstlicher Intelligenz raffinierter werden.
Angriffe, die mit großer Motivation täglich neu gedacht werden.
Angriffe, die morgen anders aussehen als heute.
Angriffe, die ins Schwarze treffen wollen.

Kriminelle werden noch besser darin werden wollen, mit Cyber Attacken Sicherheitsvorkehrungen auszuhebeln, um größtmöglichen Schaden anzurichten. Wir erleben das täglich 24/7. Mit IT-Security-Wissen, Verantwortungsbewusstsein und dem detektivischen Ansporn, vermeintlich Gegebenes zu hinterfragen, kommen wir ihnen auf die Schliche. Dieses Intrinsische treibt uns an im Cyber Defense Center. Securiosity.

Warum Cyber Defense mit ConSecur?

Wer Cyber-Attacken identifizieren will, braucht bestes Personal und beste Technologie. Diese traditionelle Gleichung haben wir bei ConSecur um ein Extra erweitert, das den Unterschied in der Cyber Defense ausmacht. **Dieses Extra ist Securiosity.**

Securiosity ist die Motivation jedes einzelnen im Cyber Defense Center, mit fachlicher Expertise die Extra-Meile zu gehen. Dieser Antrieb, lieber zweimal hinzugucken, um Anomalien zu identifizieren, verbindet uns im Cyber Defense Center.



Managed Cyber Defense aufbauen – wie ConSecur dabei vorgeht

Beim Aufbau einer Cyber Defense gehen wir von Anfang an sehr gründlich vor. Das tun wir aus Erfahrung und im beidseitigen Interesse.

Die Vorbereitung, an der im Idealfall alle Ansprechpartner beteiligt sind, beginnt mit der Bestandsaufnahme von Netzwerkinfrastrukturen, Prozessen und Tools.

In der Bestandsaufnahme werden wir auch danach fragen, welche Erwartungshaltung die Beteiligten mit dem Aufbau sowie mit dem laufenden Betrieb eines Managed Cyber Defense Centers verbinden? Welche „dos and don'ts" gibt es?

Nach der Vorbereitung, die in verschiedenen Workshops stattgefunden haben wird, werden wir IT-Landschaft und Infrastruktur-Details aus dem Effeff kennen.

Bevor die Managed Cyber Defense ihren Betrieb aufnehmen kann, sind Runbooks entwickelt, interne Prozesse mit der Cyber Defense verzahnt und Aufgabe definiert worden.

Auch in der Folgezeit werden wir dem Operationalisieren viel Aufmerksamkeit widmen, sodass Abläufe eingespielter werden und der Fokus auf dem reibungslosen Betrieb der Cyber Defense liegt.

PROOF OF CONCEPT – IHR WEG ZUM CYBER DEFENSE CENTER.

SIEM-Pilotierung vereinbaren

»Wir wissen, dass Kunden uns einen Vertrauensvorschuss geben.«

STEPHAN ILIC | CYBER DEFENSE CENTER MANAGER

Schwachstellen identifizieren, Risiken kennen, aufräumen, loslegen. Cyber Defense Center unserer Kunden starten wir mit dem kompletten Durchblick. Wir fragen so lange, bis wir die IT-Infrastruktur in einer kompletten Übersicht vor uns liegen haben.

IT-Security Analyse – Was passiert hier?

Was geht hier ab? IT-Infrastrukturen sind organisch gewachsen. In der IT-Security-Analyse stellen wir fest, wie sicher Ihre IT ist. Wir decken Sicherheitsvorfälle auf und benennen potentielle Gefahrenpunkte in Anwendungen und Komponenten, die Kriminelle als Einfallstore für Cyber-Attacken ausnutzen könnten.

RISIKOANALYSE – PRIORISIEREN UND AUFRÄUMEN

Die IT-Security-Analyse ist eine Risikoanalyse. Wir durchleuchten alle Aktivitäten innerhalb der IT-Infrastruktur, verschaffen uns einen Überblick, priorisieren Maßnahmen und räumen auf.

SCHWACHSTELLEN KÖNNEN AUCH FEHLERHAFTE BERECHTIGUNGEN SEIN

Klassische Schwachstellen, die wir identifizieren, können zum Beispiel bekannte Sicherheitslücken in Anwendungen sein oder fehlerhafte Berechtigungen in Benutzerkonten, deren Befugnisse und Rechte nicht angepasst worden sind.

Nach der IT-Security-Analyse besitzen wir ein Gesamtbild Ihrer IT-Infrastruktur

LEISTUNGEN DER CONSECUR

- Identifikation von Sicherheitsvorfällen anhand eingehender Meldungen & Alarmen
- Bewertung der Sicherheitsvorfälle (Priorisierung)
- Security Helpdesk (Hotline & E-Mail)
- Subtle Event Detection – Langzeitanalysen

Cyber Defense ist das Ergebnis der perfekten Orchestrierung von Mensch und Maschine. (Wo kommen wir auch hin, wenn IT-Security-Anlaysten jede Anomalie einzeln ansehen müssten?) Bekannte Muster identifizieren Maschinen, die wir auf die Detektion von Cyber Attackenprogrammiert haben, automatisiert.

SIEM Engineering – Angriffe automatisiert erkennen

Wie können wir potentielle Angriffe automatisiert erkennen? Dafür haben wir technische Assistenten, die diese Aufgabe innerhalb des IT-Security-Monitorings übernehmen. Diese Detektionsmechanismen unterscheiden erwünschte und unerwünschte Aktivitäten in IT-Netzwerken automatisch und in kürzester Zeit.

BEKANNTE CYBER-ATTACKEN ALS REGELN DEFINIEREN

Ihre Fähigkeit haben Detektionsmechanismen durch Regeln erhalten, die IT-Security-Engineers entwickelt, geschrieben und im SIEM-Tools abgelegt haben. Regeln gibt es für erlaubte Zugriffe, andere Regeln beinhalten den Abdruck bekannter Cyber-Attacken.

IM PROAKTIVEN BETRIEB RISIKOSZENARIEN LEICHTER ERKENNEN

Sobald ein implementierter Detektionsmechanismus einen Alarm ausgelöst hat, übernehmen unsere IT-Security-Analysten. Diese untersuchen den potentiellen Sicherheitsvorfall.

SIEM-Engineering ist die Implementierung des SIEM-Systems auf den proaktiven Betrieb, um Risikoszenarien leichter zu erkennen und Gegenmaßnahmen frühzeitig einzuleiten.

IBM Silver Partner

splunk>

LEISTUNGEN DER CONSECUR

- Konzeption, Installation und Konfiguration der SIEM-Lösung
- Betrieb und Wartung der SIEM-Lösung
- Anbindung neuer Log-Quellen und Konfiguration des Parsing für neue Use Cases

»You better know your enemy.«

CHRISTOPH KRONABEL | CYBER THREAT INTELLIGENCE LEADMANAGER

Threat Intelligence – Was kommt auf uns zu?

Was brüten Internet-Kriminelle aus? Welche Bedrohungen können auf IT-Netzwerke von Unternehmen und Organisationen zukommen? Welche Maßnahmen können wir ergreifen, um gewappnet zu sein?

Die Cyber Threat Intelligence im Cyber Defense Center beschäftigt sich mit den Cyber-Angriffen von morgen. Cyber Threat Intelligence ist Wachsamkeit.

DIE BEDROHUNGSLAGE ALS GESAMTBILD ERFASSEN

Aufgabe der Cyber Threat Intelligence ist, aus verschiedenen Quellen Hinweise auf Bedrohungen zusammenzutragen und in Dossiers zusammenzustellen.

Diese Ausführungen zeichnen ein Gesamtbild der weltweiten Bedrohungslage. Angriffstechniken werden analysiert, ihre Muster identifiziert und Maßnahmen für aktives Handeln vorausschauend vorbereitet oder eingeleitet.

ANGREIFERN IN DER CYBER DEFENSE EINEN SCHRITT VORAUS SEIN

Cyber Threat Intelligence verändert die Ausgangsposition von IT-Security-Analysten und IT-Security-Engineers im Cyber Defense Centers entscheidend. Mit den Dossiers aus der Cyber Threat Intelligence sind wir vorbereitet auf das, was wächst und gedeiht: Wir können entsprechende Maßnahmen einleiten, um Angreifern einen Schritt voraus zu sein.

LEISTUNGEN DER CONSECUR

- Sammlung, Analyse, Bewertung und Bereitstellung von IoC zur Integration in die Korrelations-Engine
- Lieferung von Informationen über die aktuelle Bedrohungslage
- Monitoring & Detektion von exponierten kritischen Informationen und Typo-Squatting-Domain-Detection

Im Notfall gilt dieser Dreiklang: Schnelligkeit, Struktur und Planung. Bei einem Sicherheitsvorfall verlieren wir keine Zeit und wissen, wer was wo zu tun hat.

Digital Forensics and Incident Response (DFIR) – Den Regelbetrieb zügig wiederaufnehmen

Was machen wir, wenn es passiert ist? Jeder Notfall ist eine Krise. Mit DFIR führen wir Sie wieder heraus.

Wir handeln mit Sofortmaßnahmen (Incident Response) schnell und konzentriert, schließen Sicherheitslücken, rekonstruieren den Angriff und stellen Daten und Systeme wieder her, sodass Sie schnellstmöglich zum gewohnten Geschäftsbetrieb zurückkehren können.

GEGENMASSNAHMEN EINLEITEN UND SYSTEME BEREINIGEN

Im Notfall alarmieren IT-Security-Analysten im Cyber Defense Center die hauseigene IT über vorab definierte Meldewege.

Die Erstmaßnahme gleicht derer eines Notarztes an der Unfallstelle, der Betroffene versorgt: Wir isolieren alle Systeme, die das Ziel des Angriffs geworden sind, sodass sich Schäden nicht oder nicht weiter ausbreiten können. Im zweiten Schritt bereinigen wir die betroffen Systeme, sodass im dritten Schritt der Übergang zum gewohnten Regelbetrieb erfolgt.

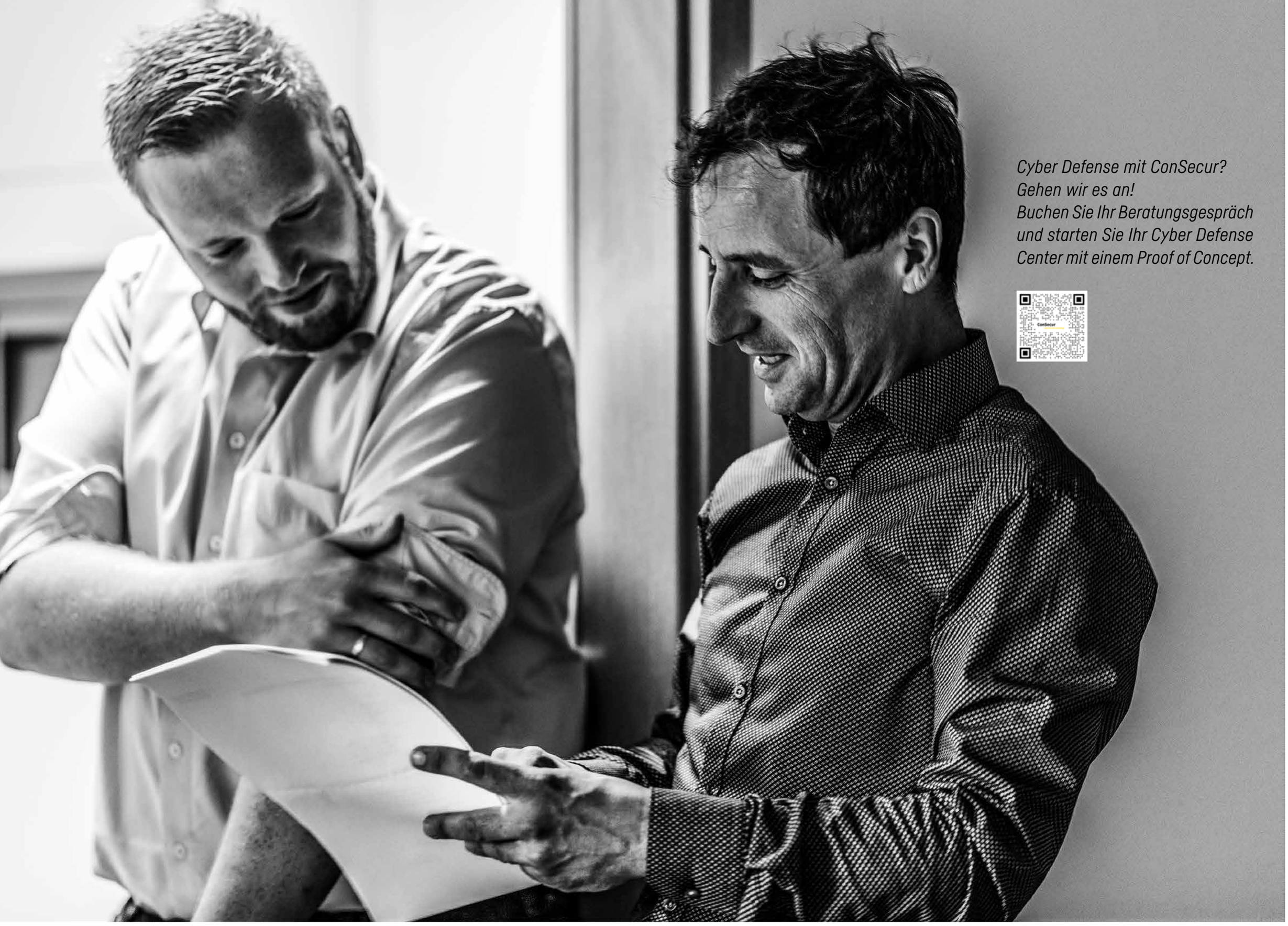
KOORDINATION UND KOMMUNIKATION – NAHTLOSE ZUSAMMENARBEIT ZWISCHEN IT-ABTEILUNG UND CYBER DEFENSE CENTER

Jeder Sicherheitsvorfall löst eine zielführende Handlungskette aus, um zügig zum Regelbetrieb zurückzukehren. Dieses geschlossene, eingespielte Handeln ist das Ergebnis einer nahtlosen Zusammenarbeit, die wir bei ConSecur für die größtmögliche Schutzwirkung anstreben.

Gemeinsam wehren IT-Abteilung und Cyber Defense Center die Cyber Attacke ab.

LEISTUNGEN DER CONSECUR

- Qualifiziertes Personal (vor Ort / remote) auf Abruf innerhalb von 24 Stunden
- Fachliche Unterstützung
- Emergency Response Leistungen (die Kohlen aus dem Feuer holen)
- Koordinierung hoch bewerteter Sicherheitsvorfälle
- Beratung und Unterstützung bei der Lösung von Vorfällen
- Dokumentation und Aufbau einer Know-how Datenbank
- Schnittstelle vom ConSecur CDC zum Kunden



Cyber Defense mit ConSecur?
Gehen wir es an!
Buchen Sie Ihr Beratungsgespräch
und starten Sie Ihr Cyber Defense
Center mit einem Proof of Concept.

ConSecur
[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

TEL.: +49 5931 9224-0
info@ConSecur.de
www.ConSecur.de