# Berater und Dienstleister für Cyber-Sicherheit

## Vorbemerkung

AXA bietet Unternehmen Versicherungsschutz gegen die unterschiedlichsten IT- und Cyber-Risiken. Viele Kunden fragen nach Unterstützung zur Verbesserung ihrer IT-Sicherheit, zur Erstellung von Notfallhandbüchern, Durchführung von Sicherheits-Audits, Schulungen, Beratung in Rechtsfragen etc.

Um die Suche nach geeigneten Beratern zu erleichtern, möchten wir unseren Kunden eine unverbindliche Liste von Ansprechpartnern aus IT- und Beratungsunternehmen zur Verfügung stellen.

Im Falle eines versicherten Schadens weisen wir darauf hin, dass Beauftragungen von externen Beratungsunternehmen gemäß den Versicherungsbedingungen und sofern nicht anders vereinbart vorab mit AXA abzustimmen sind.

Weiterhin empfehlen wir bei Hacker- oder DoS-Angriffen, Cyber-Erpressung und –Betrug die Einschaltung des zuständigen Cyber-Dezernates im jeweiligen Landeskriminalamt. Weitere Informationen mit Kontaktdaten finden Sie jeweils aktuell unter www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html.

In besonderen Fällen wie dem Verdacht der Wirtschaftsspionage empfehlen wir, den Verfassungsschutz zu kontaktieren (www.verfassungsschutz.de).

## Angaben zu den Unternehmen

### 1. Swiss IT Security Deutschland GmbH

Swiss IT Security Deutschland GmbH - Stollwerckstraße 27-31 – 51149 Köln - www.sits-d.de
Kontaktperson: Ulrich Gärtner / ☎0221 337784-12 / eMail: sales@sits-d.de
Dienstzeiten: 9 bis 18 Uhr (nach Absprache auch 24x7)
140 Mitarbeiter – Standorte: Wiesbaden, Köln und Dortmund

### 2. TÜV Rheinland i-sec GmbH

TÜV Rheinland i-sec GmbH – Am Grauen Stein - 51105 Köln - www.tuv.com/informationssicherheit
Kontaktperson: TÜV i-sec Zentrale / ☎ 0221/806-4050 / eMail: service@i-sec.tuv.com
Dienstzeiten: Mo-Fr 9 bis 17 Uhr
163 Mitarbeiter – Standorte: Köln, Hallbergmoos, Gelnhausen, Saarbrücken, Dresden

### 3. Materna GmbH

Materna GmbH – Voßkuhle 37 – 44141 Dortmund – www.materna.de
Kontaktperson: Thorsten Kuhles / ☎0152/59180143 eMail: thorsten.kuhles@materna.de
Dienstzeiten: 8 bis 18 Uhr – 24-Stunden-Hotline für Cyber-Vorfälle
Service Support Desk (SSD) / +49 (231) 72099720 / servicedesk@materna-communications.com
3.500 Mitarbeiter – Standorte: Dortmund, Bad Vilbel, Berlin, Bremen, Dresden, Düsseldorf, Erlangen, Hamburg, Köln, München, Stuttgart, Wien, Bratislava

### 4. TÜV TRUST IT GmbH

TÜV TRUST IT GmbH - Waltherstr. 49-51 - 51069 Köln - www.it-tuv.com
Kontaktperson: Stefan Möller / ☎ +49 (0)221 / 969789-60 / eMail: stefan.moeller@it-tuv.com
Dienstzeiten: 8 – 18 Uhr
200 Mitarbeiter – Standorte: Köln – Düsseldorf – Hannover – Bornheim - Wien

**5. 8com GmbH & Co. KG**
8com GmbH & Co. KG – Europastr. 32 – 67433 Neustadt a.d.W. – www.8com.de
BSI-gelisteter APT-Response-Dienstleister
Kontaktperson: Götz Schartner / ☎ 06321/48446-0 / eMail: goetz.schartner@8com.de
Notfallnummer: 06321/ 67606
Dienstzeiten: 24/7, Notfallservice 24/7 bei entsprechender Beauftragung
80 Mitarbeiter – Standort: Neustadt a. d. Weinstraße

**6. secunet Security Networks AG**
secunet Security Networks AG – Kurfürstenstr. 58 - 45138 Essen - www.secunet.com
Forensik Hotline 0201/5454-1337 für Forensik-Notfälle / Incident Response
Dienstzeiten: 9 – 18 Uhr - Support-Line: 24/7
Ca. 1000 Mitarbeiter – Standorte: Essen, Siegen, Hamburg, Berlin, Frankfurt, Dresden, München, Bonn, Ilmenau, Stuttgart, Paderborn

**7. Hogan Lovells International LLP**
Hogan Lovells International LLP - Kennedydamm 24 - 40476 Düsseldorf - www.hoganlovells.com
Kontaktpersonen: Dr. Marcus Schreibauer, Partner, Fachanwalt für Informationstechnologierecht; ☎ 0211-1368-351; eMail: marcus.schreibauer@hoganlovells.com / Dr. Kim Lars Mehrbrey, Partner; ☎ 0211-1368-473; eMail: kim.mehrbrey@hoganlovells.com
Dienstzeiten: 8 – 20 Uhr (bei Bedarf auch außerhalb der Bürozeiten)
350 Anwälte in Deutschland – Standorte: Düsseldorf, Frankfurt, Hamburg, München und international

**8. REVOLVERMÄNNER GmbH**
REVOLVERMÄNNER GmbH – Burgunderstr. 29 - 40549 Düsseldorf - www.revolvermaenner.com
Kontaktperson: Christian Scherg/Helena Hohnke ☎ 0211 5206360 /
eMail: contact@revolvermaenner.com
Dienstzeiten: 9 – 18 Uhr (im Krisenfall wird auch nach Vereinbarung über die Zeiten hinaus oder am Wochenende eine Erreichbarkeit sichergestellt)
12 Mitarbeiter – Standort: Düsseldorf und Essen

**9. @-yet GmbH**
@-yet GmbH - Schloß Eicherhof - 42799 Leichlingen - www.add-yet.de
BSI-gelisteter APT-Response-Dienstleister
Kontaktperson: Wolfgang Straßer / ☎+49 2175 1655-0 / eMail: wolfgang.strasser@add-yet.de/
Florian Straßer / ☎ 0163 5556522 / eMail: florian.strasser@add-yet.de
Dienstzeiten: 8 – 19 Uhr (Notfallhandy und dedizierter Notfall-Email-Account möglich) – Bereitschaft 7 Tage, 7 bis 21 Uhr
44 Mitarbeiter – Standort: Leichlingen und Aachen

**10. Applied Security GmbH**
Applied Security GmbH - Einsteinstr. 2a - 63868 Großwallstadt - www.apsec.de
Kontaktperson: Alexander Scherf / ☎ 06022/26 338 - 202 / eMail: alexander.scherf@apsec.de
Dienstzeiten: 9 – 17 Uhr
60 Mitarbeiter - Standorte: Großwallstadt (Hauptsitz), Berlin

**11. T-Systems Multimedia Solutions GmbH**
T-Systems Multimedia Solutions GmbH – Riesaer Straße 5 - 01129 Dresden – it-security.t-systems-mms.com
Kontakt: Tobias Kasch / ☎ 0351-2820 5804 / eMail: Tobias.Kasch@t-systems.com
Dienstzeiten: 8 – 17 Uhr
Notfallkontakt 24x7: 0351 2820-7535 / forensik@t-systems-mms.com
Ca. 1.700 Mitarbeiter - Standorte: Dresden und deutschlandweit

**12. KPMG AG Wirtschaftsprüfungsgesellschaft**
KPMG AG Wirtschaftsprüfungsgesellschaft – Klingelhöferstr. 18 - 10785 Berlin – www.kpmg.de/forensic
BSI-gelisteter APT-Response-Dienstleister
Kontakt zum Cyber Incident Response Team:
24/7 Hotline: 0800 / SOS KPMG (0800 767 5764) oder +49 202 251557146 (from outside Germany)
oder de-SOS@kpmg.com
Kontakt: Michael Sauermann / ☎ 030-2068-4624 / eMail: msauermann@kpmg.com
Dienstzeiten: 8 – 19 Uhr vor Ort – 24 Stunden-Hotline für Cyber-Vorfälle
11.500 Mitarbeiter – Standorte: deutschlandweit

**Hinweis: Sollten Sie Interesse an den Leistungen einer der Unternehmen haben, wenden Sie sich bitte direkt an den jeweiligen Ansprechpartner. Die Leistungen werden ausschließlich direkt zwischen dem Dienstleister und Ihnen vereinbart. AXA übernimmt daher keine Haftung.**

**AXA Versicherung AG**

Kompetenzstelle Cyber
51171 Köln
it-check@axa.de

## Angebotene Dienstleistungen

| Dienstleistung | Unternehmen | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Swiss IT** | **TÜV Rheinland i-sec** | **Materna** | **TÜV Trust IT** | **8com** | **secunet** | **Hogan Lovells** | **Revolver-männer** | **@yet** | **AppSec** | **T-Systems MMS** | **KPMG** |
| Kurzfristige Krisenunterstützung / Incident Response | X | X | X | X | X | X | X | X | X | | X | X |
| IT-Forensik | X | X | X | | X | X | | X | X | | X | X |
| Datenrettung / Wiederherstellung | | | | | X | | | X | X | | | X |
| Krisenmanagement | X | X | | X | X | | X | X | X | | X | X |
| Krisenkommunikation | X | | | X | X | | | X | X | | | |
| Rechtsberatung IT- und Datenschutzrecht | X | X | | X | | | X | | X | | | X |
| Stellung des externen Datenschutzbeauftragten | X | X | X | X | | X | X | X | X | X | X | |
| Beratung zu Fragen der IT-Sicherheit | X | X | X | X | X | X | X | X | X | X | X | X |
| Penetrationstests | X | X | X | X | X | X | | X | X | X | X | X |
| Erstellung von Krisen- und Notfallplänen | X | X | X | X | X | X | | X | X | X | X | X |
| Awareness-Training | X | | | | x | | | x | x | | X | |
| ISMS-Beratung | | X | x | X | | | | | x | x | X | |
| Managed Security Services (z. B. SOC) | X | X | | X[1] | X | | | | X | | X | |

1: .Angebot eines mSOC über CSOC GmbH

# Security Consulting für unsere Partner

Die Experten der Swiss IT Security Group sorgen für Ihre Sicherheit

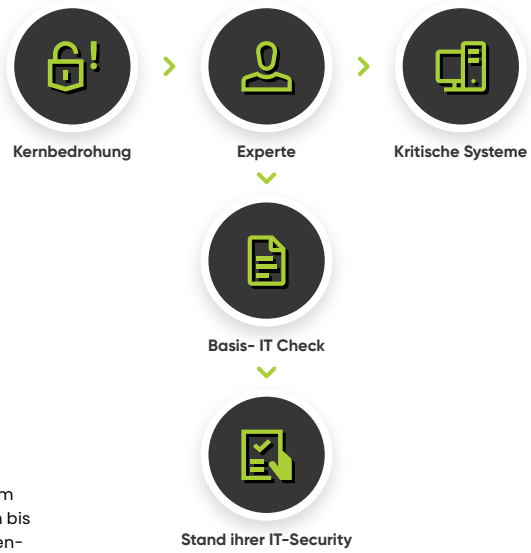
**Eine gute und angemessene IT-Sicherheit braucht passende technische Komponenten und ein geeignetes organisatorisches Gerüst. Beides kann mit dem aus dem Qualitäts-management bekannten PLAN-DO-CHECK-ACT-Zyklus (PDCA) nachhaltig gesteuert werden, weil man die IT-Sicherheit als Qualitätsdimension der IT auffassen kann. Für die Phasen PLAN und CHECK ist externes Experten-Know-how angeraten, damit der Blick über den eigenen Tellerrand hinausgeht.**

**Wir haben Module definiert, um den Beratungseinstieg leicht zu machen.**


## Modul 1: Basis IT Check

Mit unserem Basis Check IT-Security erlangen Sie einen ersten Überblick zum Stand ihrer IT-Security.
Schaffen Sie die Grundlagen für die Ableitung von Maßnahmen in die Verbesserung ihrer IT-Sicherheit. Dabei überprüft ein Experte im Rahmen eines Interviews mit einem Basis-Check das IT-Management und exemplarisch die IT-Infrastruktur anhand ihrer Dokumentation von Netzwerkkomponenten, Servern, Arbeitsplatzsystemen sowie der Umgebungsinfrastruktur. Ergänzt wird unser Angebot durch ein persönliches Gespräch, remote oder vor Ort mit ihren IT-Verantwortlichen.
Der Basis IT Check schärft das Verständnis der Geschäftsleitung für die für das Business wirklich kritischen Risiken und macht Geschäftsleitung und IT-Personal die beiderseitige Verantwortlichkeit bewusst.

Das Angebot hat einen Beratungsumfang von maximal 4 Stunden. Die Beratungszeit ist für Sie als Kunden kostenfrei.




Entstehende Reisekosten bei vor-Ort-Einsätzen werden mit 1,25 € (exkl. MwSt.) pro gefahrene Kilometer ab dem nächstgelegenen Standort der Swiss IT-Security Deutschland GmbH berechnet. Reisekosten für Entfernungen bis 200 km zum Kundenstandort werden nicht berechnet. Übernachtungskosten werden nach tatsächlich anfallendem Aufwand abgerechnet.

**Pallas GmbH**
Stollwerckstr. 27-31, 51149 Köln
Telefon+49 221 337 784-12
vertrieb@pallas.com

Wenn Sie Interesse oder Fragen zu unserem Angebot haben, dann rufen Sie uns gern direkt an. Wir freuen uns auf Sie!

## Modul 2: IT Quick Audit

Kompakte Beratung zum Stand ihrer IT-Sicherheit in zwei Tagen. Inklusive Ist-Analyse, Berichterstellung und Ergebnispräsentation.

### ANGEBOT

- Analyse der aktuellen IT-Sicherheit
- Berichterstellung über die Resultate
- Ergebnispräsentation
- Bericht dient als Handlungsleitfaden für Verbesserungen der vorhandenen Maßnahmen
- Wir zeigen auf, welche Erweiterungen für die Optimierung der Sicherheit sinnvoll sind

Eine Vertraulichkeitsvereinbarung ist Grundlage der aufgeführten Leistung.

### WAS WIRD GEPRÜFT

Bewertung des aktuellen Status Ihrer IT- Sicherheit anhand von Interviews und Prüfungen. Dabei können unter anderem folgende Bereiche geprüft werden:

- IT-Sicherheitsorganisation und deren Umsetzung
  - · Datensicherungskonzept
  - · Zugriffskonzept
  - · Updatepolitik
- Physischer Schutz
- Internet-/Netzwerk-Security
- Endpoint-Security
- Mobile-Security
- Stichprobenartige Prüfung von Sicherheitssoftware und -komponenten

Gerne berücksichtigen wir ihre individuellen Anforderungen und nehmen diese auf.

## Ablauf der Auditierung

**1. Überprüfung der Infrastruktur**
Wir führen eine Überprüfung der Infrastruktur und der relevanten Konzepte in Anlehnung an gängige Standards wie den BSI-IT-Grundschutz-Katalog und ISO27001 durch. Das Audit erfolgt stichprobenartig, ohne Anspruch auf Vollständigkeit, wobei das Augenmerk auf Risiken mit hohem Risikopotenzial gelegt wird.
Volumen: 1 Personentag

**2. Analyse und Berichterstellung**
Nach Auswertung der Informationen aus dem Audit erhalten Sie eine Zusammenfassung der Ergebnisse in einem schriftlichen Bericht. Der Bericht beschreibt die ermittelten sicherheitskritischen Risiken und enthält mögliche Handlungsempfehlungen zur Risikominimierung.
Volumen: 1 Personentag

**3. Ergebnispräsentation**
Gerne präsentieren wir die Ergebnisse des Audits ihrer Geschäftsleitung online oder vor Ort. Eine einstündige Online-Präsentation ist inklusive. Eine Präsentation vor Ort wird zusätzlich nach Aufwand berechnet.

### Ihr Nutzen

- Überprüfung der Infrastrultur und Konzepte nach BSI / ISO 27001
- Ermittlung und Bewertung von Schwachstellen nach Risikoklassen in einem schriftlichen Bericht
- Verständnis und Bewusstsein der Geschäftsleitung für die kritischen Sicherheitsrisiken schärfen

**JETZT ANFRAGEN UND INDIVIDUELL BERATEN LASSEN**

**Pallas GmbH**
Stollwerckstr. 27-31, 51149 Köln
Telefon+49 221 337 784-12
vertrieb@pallas.com

Wenn Sie Interesse oder Fragen zu unserem Angebot haben, dann rufen Sie uns gern direkt an. Wir freuen uns auf Sie!

MATERNA
*Information & Communications*

# Materna ist Ihr ganzheitlicher Security-Experte für kritische Geschäftsmodelle und Infrastrukturen

**Cyber-Angriffe verursachen in der deutschen Wirtschaft und öffentlichen Verwaltung Schäden in Milliardenhöhe. In fast einem Drittel der erfolgreichen Angriffe werden wertvolle Daten gestohlen. Die eigenen Beschäftigten sind hier oftmals die größte Gefahr für Organisationen. Als „First Line of Defence" müssen sie raffinierten Social Engineering-Attacken standhalten. Weitere Herausforderungen für die Cyber-Sicherheit sind Kunden- und Compliance-Anforderungen, die Auslagerung der IT in die Cloud und gesetzliche Vorgaben.**

Schützen Sie Ihre Organisation nachhaltig mit unseren Leistungen aus dem Cyber Defence Center. Wir begleiten Sie bei der Planung, Erstellung und Umsetzung von ganzheitlichen Cyber Security-Maßnahmen: von der Awareness über die Beratung hin zur Projektierung und dem sicheren Betrieb der Cyber Security-Lösungen in unserem professionellen Security Operations Center (SOC).

Unsere weiteren Themen sind unter anderem Incident Response, Forensik, Security Operations Center, Schwachstellenmanagement sowie Informationssicherheitsmanagement. Wir helfen Ihnen vor, während und nach einer Bedrohungslage.

**Incident Response Service**
Sicherheitsvorfälle beruhen häufig auf Schwachstellen in Systemen, Verfahren oder innerhalb der Organisation selbst. Durch den nachhaltigen Incident Response Service nach ISO 27035-1:2016 betrachten wir Ihr System ganzheitlich und schützen Ihre Daten.

### Digital Forensic Service

Über die Maßnahmen der IT-Forensik ermitteln wir durch Analysen von Daten, Datenträgern oder auch Computernetzen Spuren zur Aufklärung von Sicherheitsvorfällen. Dazu folgen wir dem ISO-Standard 27037 und gewährleisten Ihnen im Rahmen unserer umfangreichen Lösungen eine 24/7-Erreichbarkeit unserer Expert:innen.

### Security Operations Center (SOC)

Über ein Security Operations Center gelingt die Echtzeit-Abbildung der Bedrohungslage von IT- und OT-Infrastrukturen, um frühzeitig Bedrohungen zu erkennen und so früh wie möglich zu beheben. Durch das umfassende Serviceangebot rund um das SOC ermöglichen wir es Ihnen, sich wieder auf Ihr eigentliches Kerngeschäft zu fokussieren und sicher zu sein, dass Sie dabei alle gesetzlichen Vorgaben und Compliance-Richtlinien erfüllen. Profitieren Sie von umfangreichem Support, der Unterstützung durch unsere Expert:innen und umfassende Features zur Sicherung Ihrer Daten – unabhängig davon, ob Sie sich für eine SOC as a Service-Lösung oder für den Aufbau Ihres eigenen Security Operations Center entscheiden.

### Schwachstellenmanagement

Ob mit schwerwiegendem Risiko oder normalen Risiko – Schwachstellen existieren in unterschiedlichsten Formen innerhalb von Unternehmen. Durch unser zielgerichtetes Vulnerability Management gelingt es, diese Schwachstellen rechtzeitig zu erkennen, diese regelmäßig zu prüfen und langfristig gewissenhaft zu managen – vom Schwachstellenscan bis hin zu Penetrationtesting steigern wir die Sicherheit Ihrer Daten.

### Informationssicherheitsmanagement (ISMS)

Es gibt verschiedene Ansätze für die Umsetzung von Informationssicherheit. Materna berät und unterstützt sowohl bei ISO 27001 als auch bei IT-Grundschutz. Von der Einführung eines Informationssicherheitsmanagements bis hin zur Begleitung der ISMS-Zertifizierung – unsere akkreditierten Security-Expert:innen begleiten Sie von der Integration über die Migration, Überarbeitung bis hin zur Auditierung.

### Sie haben weiterführende Fragen?

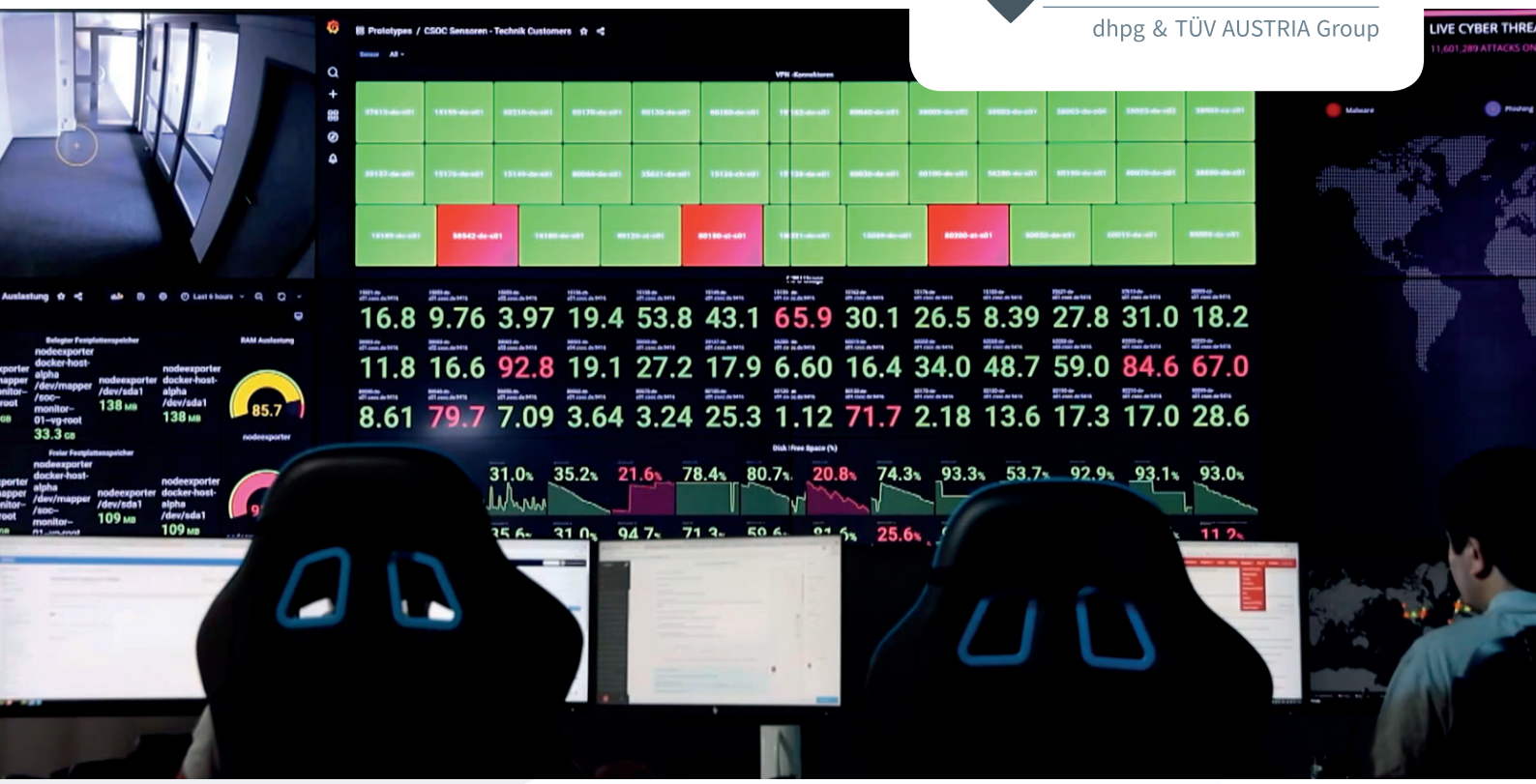
Ich freu mich darauf, Ihnen behilflich zu sein:
Thorsten Kuhles
Cyber Security Incident Manager
E-Mail: thorsten.kuhles@materna.de

Mehr Infos: www.materna.de

### Über Materna

Materna deckt das gesamte Leistungsspektrum eines Full-Service-ITK-Dienstleisters im Premium-Segment ab: von der Beratung über Implementierung bis zum Betrieb. Kunden sind IT-Organisationen sowie Fachabteilungen in Privatwirtschaft und Verwaltung.

dhpg & TÜV AUSTRIA Group




# CERTIFIED SECURITY OPERATIONS CENTER GmbH (CSOC)

# SOC as a Service

## SOCaaS – die Kernleistung des CSOC

Das SOC as a Service überwacht die IT-Systeme des Auftraggebers auf mögliche Cyberangriffe und schützt diese somit vor eventuellen Produktionsausfällen, Datenverlusten, Imageschäden etc. und damit verbundenen finanziellen Risiken. Eine Kombination aus automatischer Erkennung und dem Einsatz von Expertenwissen gewährleistet eine schnellstmögliche Detektion verschiedener Angriffsszenarien. Sollte eine erkannte, aktive Bedrohung der Infrastruktur des Auftraggebers vorliegen, treten umgehend die vertraglich individuell mit dem Auftraggeber vereinbarten Maßnahmen in Kraft. Das SOCaaS der Certified Security Operations Center GmbH (CSOC) besteht aus Standardleistungen (Kernleistungen) sowie aus optionalen Leistungen. Diese setzen sich wie folgt zusammen:

- IT-Monitoring, technische Überprüfung, Verifizierung und Qualitätssicherung Ihrer Alarme durch die Leitstelle
- Active Response
- Auto Escalation

Das SOCaaS ist in drei **LEISTUNGSBAUSTEINE** aufgeteilt. Alle drei Bausteine sind Bestandteil der Leistung, sie gehören für eine ganzheitliche Überwachung zusammen. Jeder der Bausteine kann einzeln ausgeführt werden. Während des Onboardings entscheidet der Kunde, welcher der Bausteine für die Überwachung aktiviert wird. Ziel ist immer alle verfügbaren Bausteine zu aktivieren:

## SOCaaS – Bausteine unserer ganzheitlichen Überwachung
Flexibel und modular

**Ein- und ausgehender Datenverkehr** → **Eventbasiert**
- *Anomalie-Erkennung*
- *NetFlow-Analyse*
- *Machine Learning - Unterstützung im Scoring-Verfahren*

**Eventdaten aus Firewall, Endpoint-Lösung, Switchen, Routern** → **Eventbasiert**
- *Weiterführende Analysemöglichkeiten durch Kollaboration der Daten*

**Eventdaten von Clients und Servern** → **Systembasiert**
- *System- und Prozessüberwachung*
- *SIEM*
- ***USE CASE** - basierte Analyse auf Basis von MITRE ATT&CK und Machine Learning*

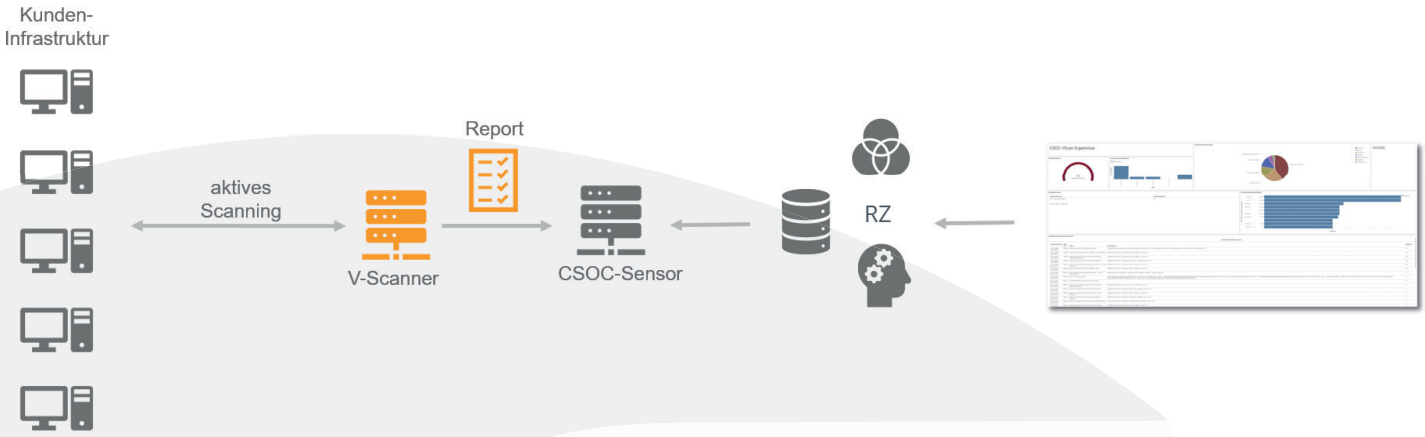
Die technische Überwachung ist bei unserem SOCaaS 24x7 **IMMER** gewährleistet. Unser System weist auf Basis der installierten CSOC-Agents automatisiert und rund um die Uhr die gewichteten Alarme aus.

## Erweiterbare Leistungskomponenten und Flexibilität

Ergänzend beinhaltet das SOCaaS die Option des Active Response sowie die Auto Escalation Funktion. Damit kann das System im Falle eines Angriffs auf Wunsch automatisch einschreiten und Systeme vom Netz nehmen oder sperren (Active Response) sowie andere Systeme aktiv warnen (Auto Escalation). Für die weitere, auch personelle Unterstützung im Angriffsfall kann unser 24x7 Leitstellenservice und Incident Response Service ergänzend hinzugebucht werden. Der ebenfalls optionale V-Scanner (Schwachstellenscanner) untersucht Ihre Zielsysteme aktiv auf tatsächlich vorhandene Schwachstellen in Bezug auf Ihr Betriebssystem, die Services und Konfigurationen.

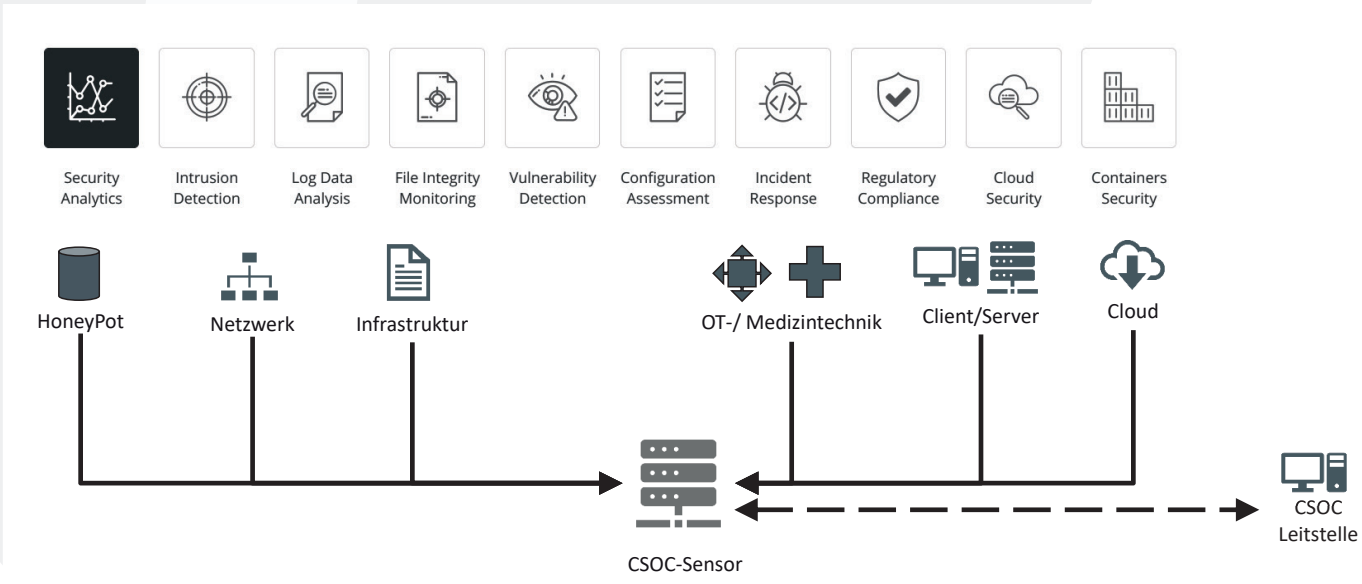
## V-Scanner-Anbindung an SOCaaS

Aktives Schwachstellen-Management für Ihre IT-Systeme




## Eventkanäle des SOCaaS

Als Eventkanäle des SOCaaS können sowohl die klassischen aktiven Komponenten der IT-Umgebung als auch diverse Steuerungssysteme aus dem OT-Bereich (OT-SOCaaS) herangezogen werden. Auch das unterstreicht die extrem hohe Skalierung des SOCaaS:



## Implementierung und Nutzung des SOCaaS

Für welche Ihrer Systeme und ab welchem Schwellwert dieser Service greifen soll, wird gemeinsam während des Onboardings individuell festgelegt. Dabei spielen sowohl die Relevanz Ihres Systems als auch die genaue Definition des jeweiligen Use Cases eine wichtige Rolle. Die Einführung und Nutzung des SOCaaS ist in folgende Phasen aufgeteilt:

## Anbindung an SOCaaS
Die Anbindungsphasen


## CSOC – Historie

Seine Geburtsstunde erlebte das CSOC unter dem Dach der Wirtschaftsprüfungs- und Steuerberatungsgesellschaft dhpg Dr. Harzem & Partner mbB (dhpg), wo es unter dem Namen Cyber Security Operations Center betrieben wurde. Mit mehr als 600 Mitarbeitern unterstützt die dhpg als interdisziplinär arbeitendes Unternehmen die unterschiedlichsten Kunden wie Familienunternehmen und Mittelständler, Großunternehmen, Verwaltungen der öffentlichen Hand, gemeinnützige Organisationen und Privatpersonen und beschäftigt dabei Wirtschaftsprüfer, Steuerberater, Rechtsanwälte sowie IT-Spezialisten.

Anfang 2021 kam es schließlich zu einem Joint-Venture der dhpg und der Kölner TÜV TRUST IT GmbH Unternehmensgruppe TÜV AUSTRIA (TÜV TRUST IT), die sich bereits als unabhängiger Partner für Beratungs- und Zertifizierungsleistungen rund um die Themen Informationssicherheit und Datenschutz am Markt etablieren konnte. Das Unternehmen setzt durchgängig erfahrene, zertifizierte Experten, Auditoren und IS-Revisoren ein und unterliegt als vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierter IT-Sicherheitsdienstleister für

IS-Revision und IS-Beratung sowie IS-Penetrationstests einer dauerhaften unabhängigen Kontrolle. So ergänzen sich nun die Leistungsportfolios der TÜV TRUST IT und der dhpg ideal, um zukunftsorientierte Lösungen am Markt zu positionieren – die TÜV TRUST IT als unabhängiger Berater für Informationssicherheit und die dhpg mit ihrem Wissen um vertrauliche und schützenswerte Daten.

Fortan operiert das SOC unter der Bezeichnung **CERTIFIED SECURITY OPERATIONS CENTER (CSOC)** an einem neuen, hochmodern ausgestatteten Standort in Bornheim, wo neben dem Onboarding und Monitoring der Kundeninfrastrukturen auch auf die kundenorientierte Weiterentwicklung des CSOCs viel Wert gelegt wird.

Im Zuge der Digitalisierung steigen nicht nur die Herausforderungen zur Abwehr der Cyber-Kriminalität überproportional, sondern auch regulative Vorgaben wie beispielsweise durch das IT-Sicherheitsgesetz 2.0. Ziel ist es daher, die Leistungsfähigkeit des CSOCs weiterhin stetig auszubauen und an den aktuellen Anforderungen auszurichten, um das führende Mittelstands-SOC Deutschlands zu werden.

## Bündelung von IT-Security Kompetenzen → CSOC


**CERTIFIED SECURITY OPERATIONS CENTER GMBH**
Adenauerallee 45-49 · 53332 Bornheim
Telefon: +49 2222 99222-0 · info@csoc.de

CSOC
dhpg & TÜV AUSTRIA Group

8COM
CYBER SECURITY

# Cyberangriffe erkennen und abwehren


Managed Security Services für IT und OT

Unser Security Operations Center (SOC) ist die Leitstelle für Ihre Cybersicherheit: Mit unseren Managed Security Services widmen wir uns der Prävention, Detektion und Reaktion und steigern so langfristig die Cyber Security unserer Kunden.

## So schützt 8com Sie vor Cyberangriffen:

### Sichtbarkeit herstellen

Schaffen Sie einen einfachen Überblick über alle Assets komplexer IT- und OT-Infrastrukturen. Wir überwachen Ihr gesamtes Netzwerk auf Schwachstellen und Anomalien inklusive Risikobewertung.

### Angriffe erkennen und abwehren

Unser Security Operations Center erkennt Angriffe in Echtzeit und leitet Abwehrmaßnahmen ein – vom Client bis zur Produktivumgebung. Unsere erfahrenen Analysten sind rund um die Uhr für Sie aktiv, 365 Tage im Jahr.

### Notfallhilfe

Im Notfall sind wir für Sie da: Von der IT-Forensik über das Krisenmanagement bis hin zur Wiederinbetriebnahme unterstützen wir Sie im Falle eines Cyberangriffs und sorgen dafür, dass Sie schnell wieder geschäftsfähig sind.

## Damit Sie sich auf Ihr Kerngeschäft konzentrieren können.

## Ihr verlässlicher Partner in der DACH-Region

Seit 2004 ist 8com Cyber-Security-Partner des Mittelstandes. Als Managed Security Service Provider (MSSP) schützen wir unsere Kunden vor Cyberangriffen. Seit der Gründung verfolgt 8com nur ein Ziel: die Steigerung der Cyber Security mittelständischer Unternehmen, Behörden und Organisationen.

Angefangen mit Penetrationstests und Security Awareness hat 8com sich zum Fullservice Managed Security Provider entwickelt und ist für seine Kunden 24/7/365 im Einsatz.

Unser Kernbereich SOC ist ISO 27001-zertifiziert auf Basis des BSI IT-Grundschutzes.

- Prävention, Detektion und Reaktion aus einer Hand
- Cyber Security für IT und OT seit 2004
- Jahrelange branchen-spezifische Erfahrung

## 8com Security Operations Center

**SIEM** as a Service
Security Monitoring zur Erkennung von Anomalien und Cyberangriffen

**EDR** as a Service
Angriffserkennung und direkte Abwehr auf allen Endpunkten

**NDR** as a Service + **Rhebo Industrial Protector**
Nicht-invasive Netzwerküberwachung und Erkennung von sicherheitsrelevanten Ereignissen

**Vulnerability Management** as a Service
Erkennung von Schwachstellen mit Risikobewertung

**Incident Response** as a Service
Schnelle Reaktion im Ernstfall und Wiederherstellung des Regelbetriebs

**IT-Forensik**
Analyse von Sicherheitsvorfällen samt Gutachten


- Zertifizierter Schutz: ISO 27001-Zertifikat auf Basis von BSI-IT-Grundschutz
- Schutz sowohl für IT als auch OT
- Rund um die Uhr für Sie im Einsatz (24/7/365)
- Individuelle Betreuung

## Penetration Testing

**IT-Sicherheitsüberprüfungen**
aus Sicht des Angreifers

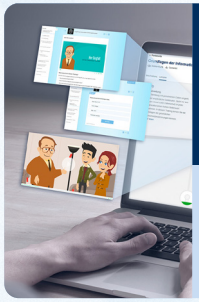
**Wir stärken Ihre menschliche Firewall**

## Security Awareness

**Phishing Test**
Wir versenden in Ihrem Auftrag Phishing-Mails und testen die Security Awareness Ihrer Mitarbeitenden

**8com Academy**
E-Learning leicht gemacht – Schulen Sie Ihre Mitarbeitenden zu Gefahren aus dem Netz

**Live-Hacking-Vorträge**
Faszinierend, informativ, lösungsorientiert: Wecken Sie das Gefahrenbewusstsein Ihrer Mitarbeitenden



8COM ACADEMY

**Jetzt Demo-Zugang anfordern:**
www.8com.de/academy

# SERVICE

## STATT EINFACH NUR TECHNOLOGIE

| Tobias Rühle | Alexander Spieß | Götz Schartner |
|---|---|---|
| Head of SOC | Lead Service Manager | CEO |

Aus unserer langjährigen Erfahrung wissen wir, worauf es ankommt. Cyber Security Services müssen auf jede IT-Infrastruktur und die Geschäftsprozesse des einzelnen Kunden individuell abgestimmt sein. Die ausführliche Beratung vor und die intensive Betreuung während der gesamten Zusammenarbeit sind uns daher besonders wichtig.

**Gerne beantworten wir Ihre Fragen im persönlichen Gespräch.**

## Direkt Termin vereinbaren:


+49 6321 48446-0
info@8com.de
www.8com.de

**8com GmbH & Co. KG**
Europastraße 32
67433 Neustadt a. d. Weinstraße
Germany


8COM CYBER SECURITY

Hogan Lovells

# Cybersecurity – rechtliche Unterstützung

## Unsere Leistungen

**Präventive Beratung von Versicherungsnehmern**

Proaktive Verringerung von Versicherungsrisiken durch:

- Beratung, einschließlich Schulungen zu rechtlichen Anforderungen an die Cyber-Sicherheit
- Prüfung und Optimierung von Verträgen mit Geschäfts-partnern im Hinblick auf mögliche Cyber-Risiken
- Beratung zu Reaktionsplänen bei Cyberangriffen

**Beratung von Versicherungsnehmern bei einem Cyberangriff**

Reduzierung von rechtlichen Risiken und Deckungskosten durch:

Rechtliche Begleitung bei sämtlichen rechtlichen Fragestellungen im Zusammenhang mit dem Angriff, insbesondere zu:

- Pflichten und Best Practice bei Aufklärung des Vorfalls, einschl. Prüfung von geleakten Datenbeständen
- Koordination mit IT-Forensik und Krisenkommunikation
- Begleitung von strafrechtlichen Ermittlungsverfahren
- Meldungen nach Datenschutzrecht an Behörden und Benachrichtigungen von Betroffenen

**Beratung von Versicherungsnehmern nach einem Cyberangriff**

Reduzierung von Folgekosten durch:

- Untersuchungen zur Aufklärung und Abstellung rechtlicher Schwachstellen, Verantwortlich-keiten und Haftungsrisiken
- Durchsetzung von Schadensersatzansprüchen (einschl. Sicherung betrügerisch erlangter Zahlungen weltweit)
- Abwehr von Schadensersatz-ansprüchen (z.B. von Geschäftspartnern)
- Prüfung und Durchsetzung arbeitsrechtlicher Konsequenzen

Hogan Lovells ist "TOP Kanzlei" in IT- und Datenschutzrecht *(WirtschaftsWoche 2020)*

Hogan Lovells ist Mitglied der Allianz für Cyber-Sicherheit

Rund 50 Standorte weltweit
Standorte in Deutschland: Düsseldorf, Hamburg, Frankfurt, München
2600+ Anwälte weltweit


**Hogan Lovells International LLP**
Kennedydamm 24 | 40476 Düsseldorf
www.hoganlovells.com


## Ihre Ansprechpartner


**Dr. Marcus Schreibauer**
Partner, Fachanwalt für Informationstechnologierecht

T +49 211 1368 352
M +49 174 6773036
(außerhalb der Bürozeiten)

marcus.schreibauer@hoganlovells.com



**Dr. Kim Lars Mehrbrey**
Partner,
Haftung & Rechtsstreitigkeiten

T +49 211 1368 473
M +49 173 7124708
(außerhalb der Bürozeiten)

kim.mehrbrey@hoganlovells.com

# Security Leistungen der T-Systems MMS

Informationsblatt zur
AXA Versicherung

MMS EXPERIENCE BEYOND DIGITAL

## Incident Response und IT-forensische Untersuchungen

Für viele Unternehmen stellt die schnelle und richtige Behandlung von IT-Sicherheitsvorfällen eine große Herausforderung dar. Mit unserem Portfolio im Bereich Incident Response und IT-Forensik unterstützten wir Sie Ad-Hoc bei der Bewältigung und Aufklärung von Sicherheitsvorfällen:

- Forensische Analysen von Clients, Servern, Appliances, Netzwerken und Malware
- Aufarbeitung von Sicherheitsvorfällen, Root-Cause Analyse, Definition Verbesserungsmaßnahmen
- Unverzügliche Unterstützung bei der Eingrenzung von Sicherheitsvorfällen, sowie dem Aufbau eines Notfallbetriebes ohne wichtige Spuren zu vernichten
- Versicherungskonforme Aufarbeitung und Dokumentation

## Krisenmanagement / BCM

Das BCM stellt die kontinuierliche Betriebsfähigkeit, auch unter nicht planbaren Bedingungen (z.B. Naturkatastrophen), sicher. Dabei werden zwei Ansätze verfolgt, einerseits die Notfallvorsorge und andererseits die Notfallbewältigung.
Wir unterstützten Sie mit unserem strukturierten Ansatz bei der Konzeption und Einführung von Notfallorganisationen und Notfallplänen.
Im Ernstfall stehen unsere qualifizierten Notfallmanager zur Gefahrenabwehr, Notfallbewältigung und Wiederherstellung zur Seite.

## Externen ISB/ CISO / Datenschutzbeauftragter

Qualifizierte und erfahrenen Experten im Bereich Datenschutz und IT-Sicherheit sind gefragte Stellen und auf dem aktuellen Arbeitsmarkt kaum zu besetzende Vakanzen. Außerdem macht nicht für jedes Unternehmen eine eigenständige Stelle Sinn.
Wir unterstützten Sie bei allen Ihren Datenschutz und IT-Sicherheitsanforderungen durch die Bereitstellung externer Datenschutzbeauftragter und interner Datenschutzkoordinatoren, sowie externen Informationssicherheitsbeauftragter.

T Systems

## IT-Security Beratung

In unserem ganzheitlichen Ansatz Beraten wir Sie zur Sicherheit von Applikationen, Systemen oder Infrastrukturen. Unser Leistungsspektrum umfasst dabei:

- Schutzbedarfs- und Risikoanalysen und Auswahl passender Maßnahmen
- Beratung/Begleitung bei der Einführung eines ISMS und zur Sicherheit von Applikationen, System oder Infrastrukturen
- Umsetzungsunterstützung bei ISMS/ISO27001, Kritis, TISAX, IT-Grundschutz
- Unterstützen bei der Absicherung bestehender Infrastrukturen
- Beratung bei der Auswahl geeigneter IT-Systeme und Security Appliances
- Erstellung von Sicherheitskonzepten

## Penetrationstest

Mit Sicherheitsüberprüfungen, Penetrationstests und Audits von Hardware, Software und Infrastrukturkomponenten reagieren wir präventiv auf Ihre Sicherheitsanforderungen. Dabei überprüfen wir, ob und inwiefern die Sicherheit eurer Anwendungen bzw. IT-Systemlandschaften von Bedrohungen wie Hackern, gefährdet ist und bewerten dabei das aktuelle Sicherheitsniveau. Gern zeigen wir euch auch geeignete Maßnahmen zur Vorbeugung und zur Behebung. Mit unseren über 80 Sicherheitstest-Experten decken wir ein sehr breites Spektrum an Technologien und Branchen ab und können immer optimal beraten

## Phishing und Awareness

Jeder Mitarbeiter in Ihrem Unternehmen ist ein potenzielles Ziel für externe und interne Angriffe. Mithilfe eines umfassenden Sensibilisierungskonzepts bestehend aus Newslettern, Präsenztrainings und E-Learning-Angeboten, befähigen Sie Ihre Mitarbeiter, verschiedene Angriffe wie Social Engineering auf das Unternehmen zu erkennen.

- Praxisnahe, interaktive und gezielte Trainings, Seminare und Workshops
- Abgestimmte Social-Engineering-Maßnahmen / Gezielte Attacken/ Wirksamkeitsüberprüfung
- Zeit- und ortsunabhängig einsetzbare E-Learnings für Führungskräfte und Mitarbeiter
- Beratung und Durchführung von zielgruppenorientierten Sensibilisierungskampagnen

## Managed Security Services

In unserem Bereich Managed Security Services bieten wir Implementierungs- und Betriebs-Knowhow für IT-Sicherheitslösungen aller Art an.

- Implementierung, Betrieb, Support und Verantwortung von Protection Lösungen wie bspw. Windows Defender, SIEM, Firewalls und WAFs, DDoS Prevention, Mail-Filtering, EDR/XDR, VPN, IDM etc.
- Implementierung, Betrieb, Support und Verantwortung von Vulnerability Assessment Lösungen wie bspw. Tenable Nessus, Qualys, Greenbone, etc.
- Implementierung, Betrieb, Support und Verantwortung von Entwicklungsbegleitender Security Services wie bspw. Dependency Checks, License Compliance, Statische und Dynamische Security Test, etc.

T Systems