IT-Sicherheit als Service

CONET Security Operation Center (SOC)

Monitoring – Response – Reporting – Support

Sicherheit in der IT kann man nicht von der Stange kaufen

Das CONET SOC hat die Spezialisten in den Bereichen IT-Sicherheit und Infrastruktur, die passgenau Ihren bestmöglichen Schutz gewährleisten!

Sie müssen und wollen Ihr Unternehmen schützen.

Der Aufwand dafür misst sich an dem möglichen Schaden, der eintreten könnte und der durch rechtzeitige Gegenmaßnahmen verhindert werden kann.

Um sich gegen ausgefeilte Angriffe zu schützen, sollten Sie auf die Erfahrung von Spezialisten vertrauen, die Ihre Sicherheit nicht als Produkt verstehen, sondern als Prozess begreifen, der sich an Ihren Bedürfnissen und Rahmenbedingungen orientiert.

Es treten immer neue Schwachstellen auf.

Aufgrund der rasanten technischen Entwicklung müssen immer wieder neue Schwachstellen in Ihren Systemen berücksichtigt werden.

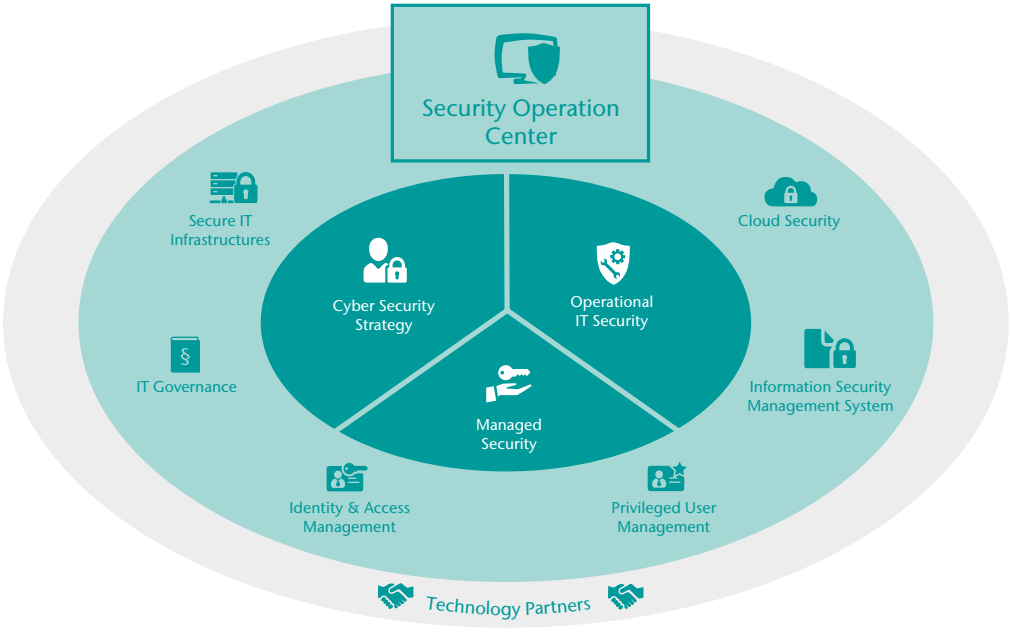
Die Maßnahmen für Ihre IT-Sicherheit müssen deshalb fortlaufend angepasst werden, um Lücken schon zu berücksichtigen, bevor ein Angreifer diese ausnutzen kann – und somit der Schaden abgewendet wird, noch bevor er entsteht.

Eine Prüfung ist eine Momentaufnahme – aktive Sicherheit bedarf einer ständigen Überwachung.

Eine Prüfung stellt immer nur die augenblickliche Situation dar – die Ereignisse, die zwischen den Überprüfungen stattfinden, werden nicht beurteilt. Wir wollen, dass Sie ständig sicher sind: Für aktive Sicherheit bedarf es einer permanenten Überwachung (Security Monitoring).

Unser hochqualifiziertes Personal hat jahrelange Erfahrung und stellt sicher, dass jedes Ereignis seine entsprechende Einschätzung erfährt. Sie werden zielgruppengerecht über Gefährdungen informiert und erhalten detaillierte Handlungsempfehlungen für die Fälle, in denen Gegenmaßnahmen notwendig sind.

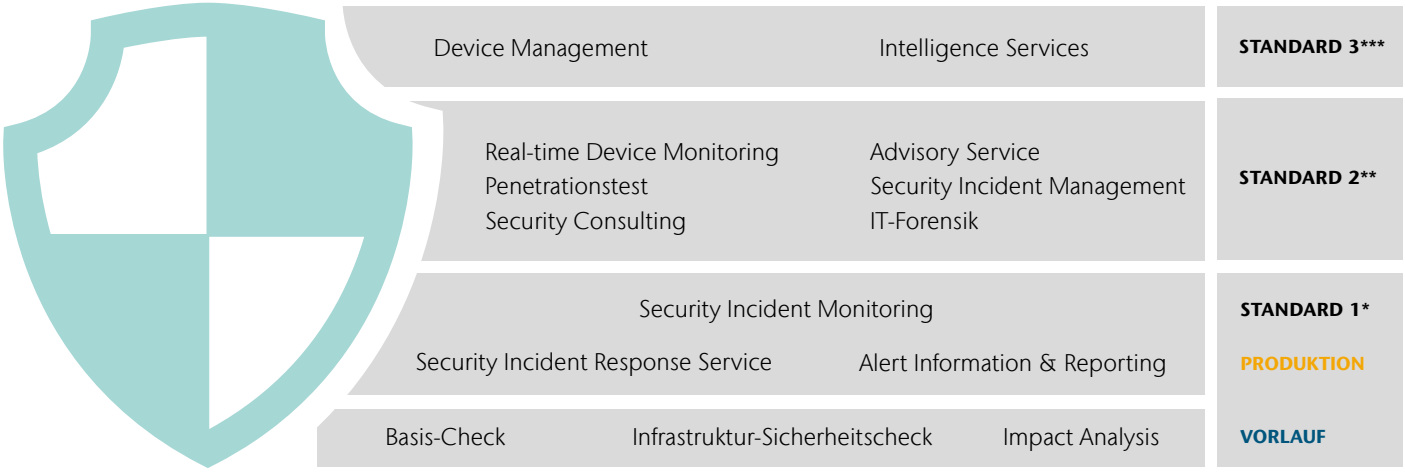
Das SOC ist Kernelement der CONET Cyber Security Strategy



Wir helfen Ihnen, sich zu schützen!

Die Gesamtleistung zur Erreichung des angestrebten Schutzniveaus setzt sich aus einer Vielzahl von Einzel-Services zusammen. Diese werden von den Spezialisten des CONET SOC in Zusammenarbeit mit den Mitarbeitern der Kundenorganisation oder der Dienstleister erbracht.

Jeder Service-Kunde startet im Paket Standard 1 mit den Phasen „Vorlauf“ und Übergang in „Produktion“. Zielführend ist ein ausgewogenes Verhältnis zwischen der individuellen Bedrohungslage und dem zu wählenden Service-Umfang. Insbesondere sind die Service-Zeiten (SLA) individuell zu ermitteln.



Leistungsbereiche im Detail – Standards

Basisabsicherung – Fokussierung auf Detektion als Voraussetzung für Maßnahmen der Reaktion

* STANDARD 1

Basis-Check

- ✔ Inventarisierung sicherheitsrelevanter Infrastrukturkomponenten und baulicher Einrichtungen
- ✔ grundsätzliche Einschätzung (Security Devices, Sicherheitsmaßnahmen & Strategien, Bedrohungspotenziale & Risiken)
- ✔ zielgruppenorientierte Dokumentation der Ergebnisse

Infrastruktur-Sicherheitscheck

- ✔ detaillierte Analyse (> Ergebnisse Basis-Check)
- ✔ automatisiertes Scannen von Hardware und Software auf Sicherheitslücken
- ✔ Untersuchen der vorhandenen Sicherheitsprozesse

Impact Analysis

- ✔ Bewertung und Einordnung der Check-Ergebnisse
- ✔ Vereinbarung einer Eskalationsmatrix (Vorgehensweise, Schadenspotenzial und Meldewege bei Sicherheitsvorfällen)

Security Incident Monitoring	✔ werkzeugbasierte Überwachung der IT-Infrastruktur & Netzwerkelemente ✔ Identifikation & Klassifizierung IT-sicherheitsrelevanter Zwischenfälle (Incidents)
Security Incident Response Service	✔ Event-basierte Information des Kunden und/oder mit der IT betrauter Dienstleister (automatisierte Sofortnachricht & individualisierte Nachricht über den Incident-Status)
Alert Information & Reporting	✔ Bereitstellung von Echtzeit-Information über die Sicherheitslage ✔ Bereitstellung regelmäßiger schriftlicher (Status-) Berichte über die Sicherheitslage ✔ Information über kritische Sachverhalte per E-Mail, SMS oder Telefon

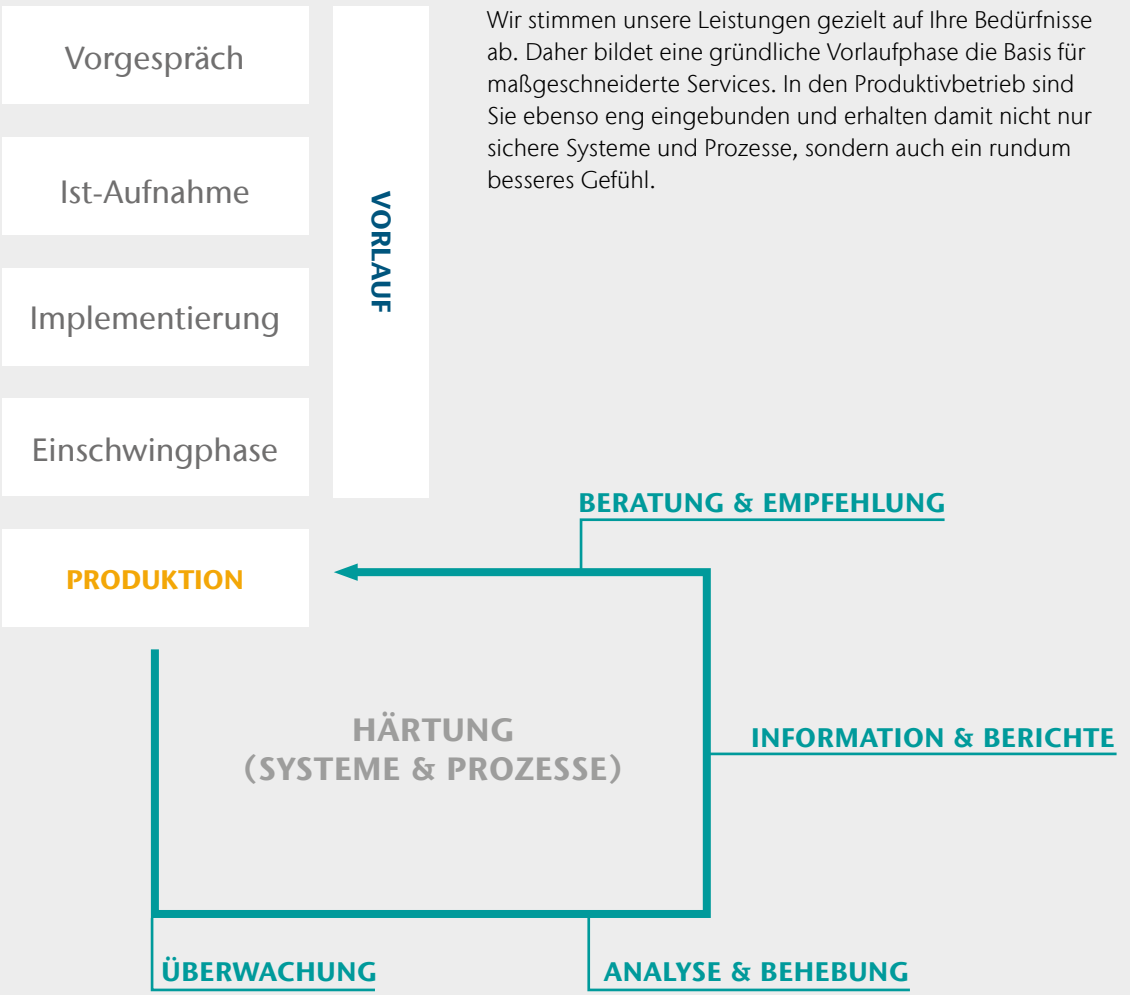
Absicherung und Services – Umfassende Services zur Detektion, Response und Analyse

** STANDARD 2	
Real-time Device Monitoring	✔ Überwachung der IT-Sicherheitseinrichtungen per Fernzugriff (Firewalls, Virenschutz, Intrusion Detection / Prevention-Systeme), um Sicherheitsanomalien rechtzeitig zu erkennen (Scan, Monitoring, Log-Korrelation, Analysen und Tests)
Security Incident Management	✔ bestmögliche Unterstützung der Beteiligten bei der Behandlung eines eingetretenen Vorfalls (Eindämmung, Abwehrmaßnahmen (z. B. DDoS), Wiederherstellung, Forensik)
Advisory Service	✔ Bereitstellung einer normierten Anlaufstelle (Sicherheits-Hotline und Sicherheitswarnungen)
Security Consulting	✔ Beratungsleistungen im Kontext des Security Monitorings (Technik- und Management-Berichte, Lösungsfindung IT-sicherheitsrelevanter Fragestellungen)
Penetrationstest	✔ Identifikation bekannter und unbekannter Schwachstellen (Methodik potenzieller Angreifer), um das Niveau einer bestimmten Sicherheitsbedrohung sowie die entsprechende Einschätzung der Auswirkung zu dokumentieren
IT-Forensik	✔ Identifikation und Ausschluss krimineller Handlungen ✔ Analyse oder Rekonstruktion von technischen Sachverhalten zum Zweck der rechtsverbindlichen Beweisführung

Erweiterter Sicherheits-Service – Full Service und Umfeld-Analyse

*** STANDARD 3	
Device Management	✔ Verwaltung der IT-Sicherheitseinrichtungen per Fernzugriff (Firewalls, Virenschutz, Intrusion Detection / Prevention-Systeme) mit dem Ziel, den systemtechnisch aktuellen Stand zu gewährleisten (Konfiguration & Härtung, Wartung, Policy Management & Implementierung)
Intelligence Services	✔ Bereitstellung aufklärender Informationen aus der Analyse gespeicherter Massendaten, um Trends, Beziehungen und Anomalien zu entdecken

Ablauf von Service-Aufnahme und Betrieb



Wir stimmen unsere Leistungen gezielt auf Ihre Bedürfnisse ab. Daher bildet eine gründliche Vorlaufphase die Basis für maßgeschneiderte Services. In den Produktivbetrieb sind Sie ebenso eng eingebunden und erhalten damit nicht nur sichere Systeme und Prozesse, sondern auch ein rundum besseres Gefühl.

www.conet.de/DE/cyber-security

Ich berate Sie gerne!

Manfred Müller
Sales Manager Cyber Security

cyber-security@conet.de
+49 2242 939-187
www.conet.de

CONET • www.conet.de • info@conet.de
Humperdinckstraße 1 • 53773 Hennef • Telefon: +49 2242 939-0