CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

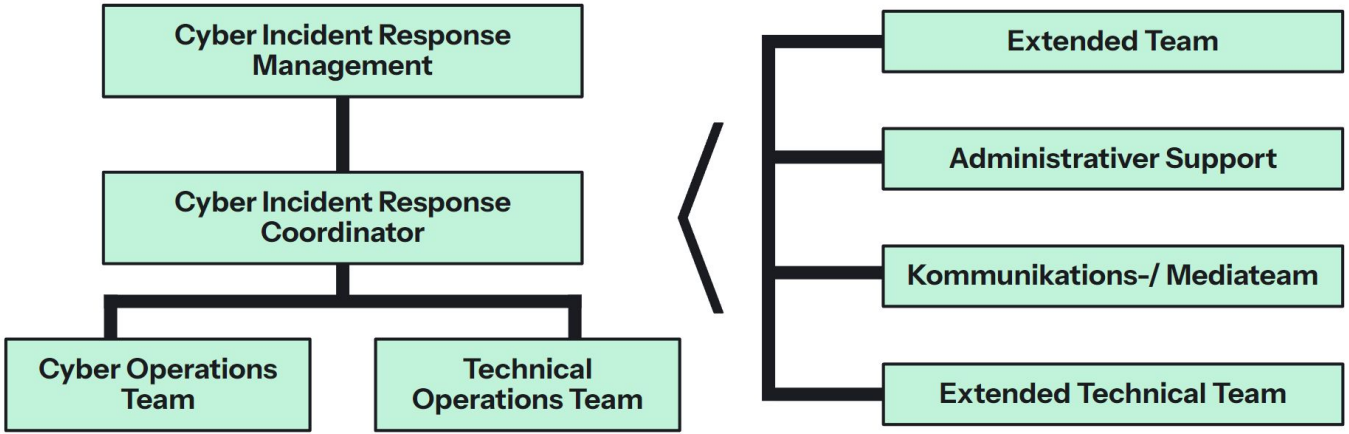
CloudCommand GmbH chr.schumacher@gmx.tm

Incident Response Team

Definition Incident Response Team

Gruppe von Personen, in der Regel bestehend aus **Sicherheitsanalysten**, die organisiert sind, um unmittelbare **Maßnahmen zur Eindämmung, Entfernung und Wiederherstellung bei Computer-Sicherheitsvorfällen** zu entwickeln, empfehlen und koordinieren.

Allgemeiner Aufbau



Arten von Incident Response Teams

- Computer Security Incident Response Teams (CSIRTs)
- Computer Emergency Response Teams (CERTs)
- Security Operations Centers (SOCs)

Computer Security Incident Response Teams (CSIRTs)

Aufgaben:

- CSIRTs sind spezialisierte Teams, die für die Erkennung, Analyse und Reaktion auf Sicherheitsvorfälle in einer Organisation verantwortlich sind.

Teamzusammensetzung:

- Sie setzen sich aus Experten für Sicherheitsvorfälle zusammen, die forensische Analysen durchführen, Bedrohungen bewerten und Gegenmaßnahmen ergreifen.

Computer Security Incident Response Teams (CSIRTs)

Kommunikation:

- CSIRTs spielen eine Schlüsselrolle in der internen und externen Kommunikation bei Sicherheitsvorfällen, indem sie Informationen an das Management, andere Abteilungen und gegebenenfalls externe Behörden weitergeben.

Proaktive Maßnahmen:

- Neben der Reaktion auf Vorfälle arbeiten CSIRTs auch proaktiv daran, Schwachstellen zu identifizieren und Sicherheitsmaßnahmen zu verbessern, um zukünftige Vorfälle zu verhindern.

Computer Emergency Response Teams (CERTs)

Aufgaben:

- CERTs sind Organisationen oder Teams, die sich auf die Koordinierung und Reaktion auf Cyber-Notfälle spezialisiert haben.

Ursprung:

- Das Konzept der CERTs entstand in den 1980er Jahren am Carnegie Mellon University's Software Engineering Institute (SEI) als Reaktion auf Computerwürmer und Viren.

Computer Emergency Response Teams (CERTs)

Koordinierung:

- CERTs arbeiten oft mit verschiedenen Parteien zusammen, einschließlich Regierungsbehörden, Unternehmen und anderen CERTs, um auf großangelegte Cyber-Vorfälle zu reagieren.

Schulung und Bewusstsein:

- CERTs bieten Schulungen und Bewusstseinskampagnen an, um Organisationen und Einzelpersonen für Sicherheitsrisiken zu sensibilisieren und bewährte Praktiken zu fördern.

Security Operations Centers (SOCs)

Aufgaben:

- SOCs sind spezialisierte Einheiten oder Abteilungen, die sich auf die kontinuierliche Überwachung von IT-Systemen und Netzwerken zur Erkennung und Reaktion auf Sicherheitsvorfälle konzentrieren.

Teamzusammensetzung:

- SOCs beschäftigen Sicherheitsanalysten, die verdächtige Aktivitäten analysieren, Schwachstellen bewerten und geeignete Gegenmaßnahmen ergreifen.

Security Operations Centers (SOCs)

Tools und Technologien:

- Sie nutzen fortschrittliche Sicherheitswerkzeuge und -technologien wie SIEM-Systeme, IDS/IPS, Firewalls und Antivirus-Software, um Bedrohungen zu identifizieren.

24/7-Betrieb:

- Viele SOCs arbeiten rund um die Uhr, um eine kontinuierliche Überwachung und schnelle Reaktion auf Vorfälle zu gewährleisten.

Aufbau des Incident Response Teams

Security Analyst:

- Kontinuierliches Monitoring des Umfelds auf Sicherheitsrisiken
- Durchführung von Ursachenermittlung
- Eskalation bzw. Auflösung von Alerts

Aufbau des Incident Response Teams

Technical Lead:

- Anwendung von Software-Patches und Updates
- Entwicklung von Strategien zur Eindämmung, Eliminierung und Erholung von Vorfällen
- Oft Kooperation mit anderen Teams um das Zusammenspiel von Sicherheits-Prioritäten mit wirtschaftlichen Prioritäten zu koordinieren

Aufbau des Incident Response Teams

Incident Coordinator:

- Zusammenarbeit mit relevanten Bereichen eines Unternehmens, um eine übergreifende Herangehensweise zu gewährleisten
- Sicherstellung offener und klarer Kommunikation

Aufbau des Security Operations Center

Tier 1 SOC Analyst:

- Überwachen, Überprüfen und Priorisieren von Benachrichtigungen basierend auf ihrer Wichtigkeit oder Schwere.
- Erstellen und Schließen von Benachrichtigungen mithilfe von Ticketing-Systemen.
- Eskalieren von Benachrichtigungstickets an Tier 2 oder Tier 3.

Aufbau des Security Operations Center

Tier 2 SOC Analyst:

- Entgegennahme eskalierter Tickets von L1 und die Durchführung von tiefergehenden Untersuchungen
- Konfiguration und Verfeinerung von Sicherheitstools
- Berichterstattung an den SOC-Leiter

Aufbau des Security Operations Center

Tier 3 SOC Lead:

- Leitung der Operationen ihres Teams
- Erforschung von Erkennungsmethoden durch die Anwendung fortgeschrittener Erkennungstechniken wie Malware- und Forensik-Analyse
- Berichterstattung an den SOC-Manager

Aufbau des Security Operations Center

SOC Manager:

- Einstellung, Schulung und Bewertung der Mitglieder des SOC-Teams.
- Schaffung von Leistungskennzahlen und die Verwaltung der Leistung des SOC-Teams.
- Erstellung von Berichten zu Vorfällen, Compliance und Prüfungen.
- Kommunikation der Ergebnisse an Interessengruppen wie das Top-Management.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm