Cybersecurity Berufe: Anforderungen und Kompetenzen

Diese Präsentation beleuchtet die vielfältigen Berufe in der Cybersicherheit, beschreibt die notwendigen Kompetenzen und stellt die unterschiedlichen Abschlüsse vor.

by Christian Schumacher

Cyber-Sicherheitsanalyst: Aufgaben und Kompetenzen

Aufgaben

Überwachung von Netzwerken und Systemen auf Sicherheitsvorfälle, Analyse von Daten und Logs, Erstellung von Sicherheitsberichten, Implementierung von Sicherheitsmaßnahmen.

Kompetenzen

Netzwerkkenntnisse, Kenntnisse von Sicherheits-Software und -Tools, analytisches Denkvermögen, Problemlösungsfähigkeiten, Kommunikationsfähigkeit.

Cyber-Sicherheitsberater: Expertenwissen und Beratungskompetenzen

Expertenwissen

Tiefes Verständnis von Sicherheitsbedrohungen, Best Practices, gesetzlichen Vorgaben, Sicherheitslösungen.

Beratungskompetenzen

Fähigkeit, Sicherheitskonzepte zu entwickeln, Risiken zu bewerten, Sicherheitslösungen zu empfehlen, Kunden zu schulen.

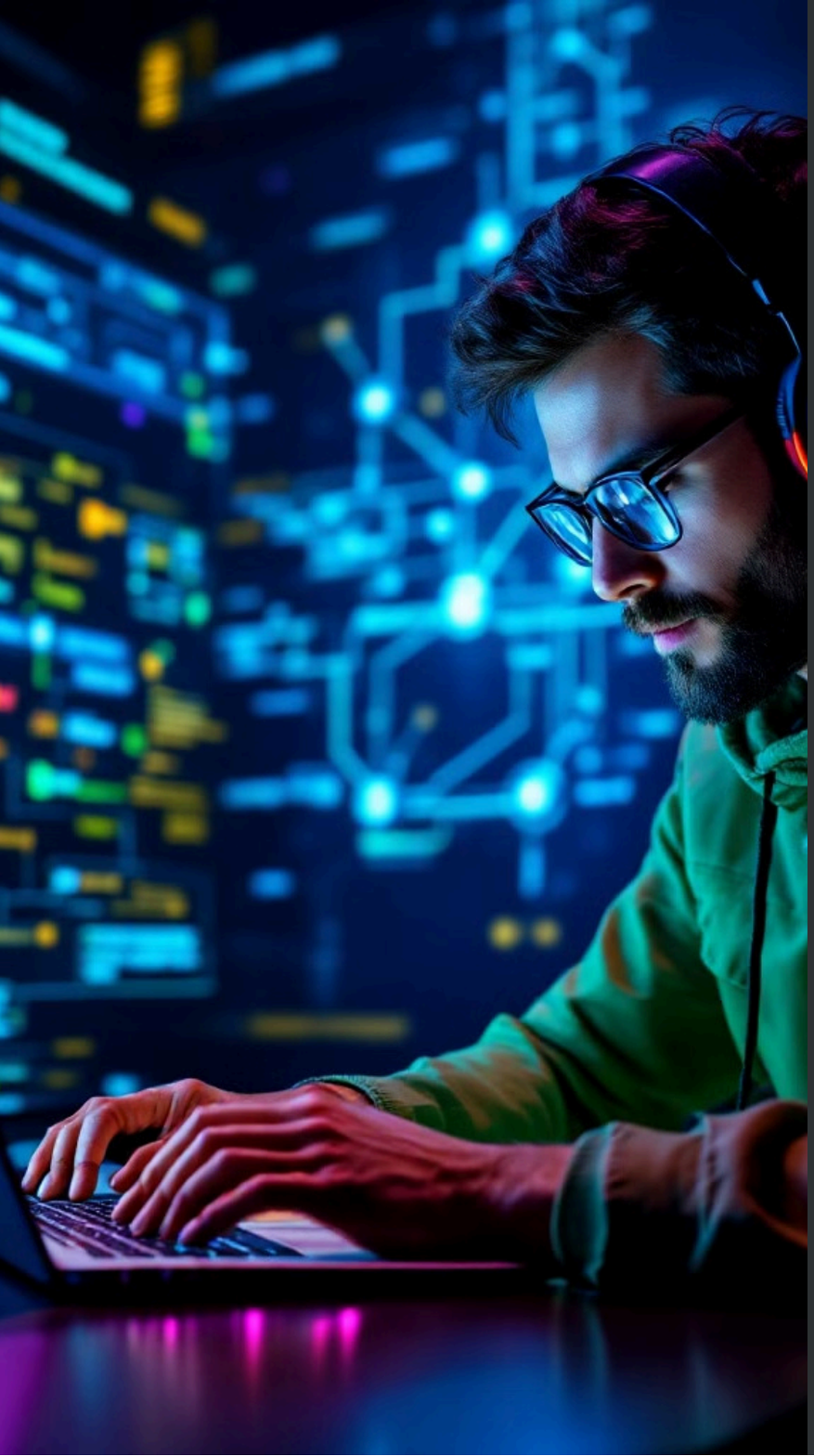
IT-Infrastruktursicherheit: Technische Fähigkeiten und Prozessmanagement

Technische Fähigkeiten

Kenntnisse von Betriebssystemen, Netzwerkprotokollen, Sicherheitshardware und -software, Virtualisierungstechnologien.

Prozessmanagement

Fähigkeit, Sicherheitsrichtlinien zu erstellen, Sicherheitsvorfälle zu managen, Sicherheitsaudits durchzuführen, Prozesse zu optimieren.



Cyber-Sicherheitsingenieur: Konzeption und Implementierung von Sicherheitslösungen

Firewall

Konfiguration und Verwaltung von Firewalls zur Abwehr von Angriffen.

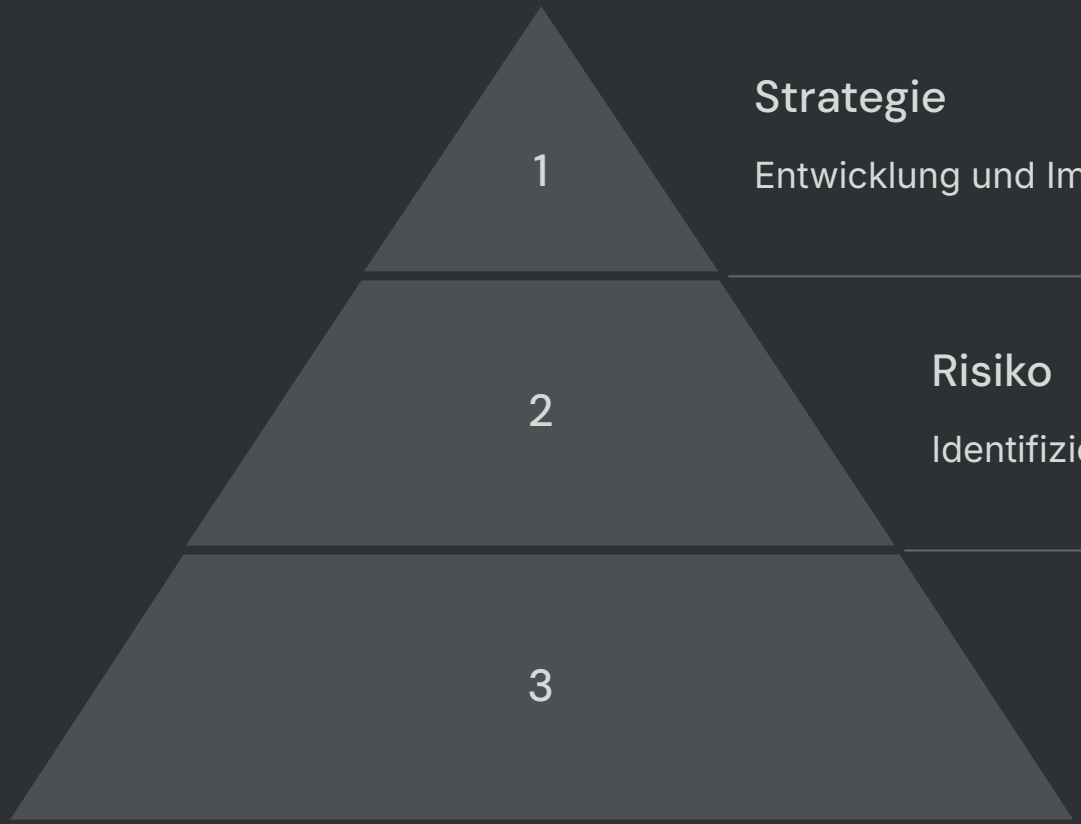
Intrusion Detection System (IDS)

Entwicklung und Implementierung von IDS-Systemen zur Erkennung von Eindringlingen.

Verschlüsselung

Implementierung von Verschlüsselungstechnologien zum Schutz sensibler Daten.

Cyber-Sicherheitsmanager: Strategisches Risikomanagement und Führungskompetenz



Strategie

Entwicklung und Implementierung einer umfassenden Cybersecurity-Strategie.

Risiko

Identifizierung und Bewertung von Sicherheitsrisiken.

Kontrolle

Implementierung von Sicherheitskontrollen zur Minimierung von Risiken.

Penetrationstester: Ethical Hacking und Schwachstellenanalyse

1

Systeme analysieren

Identifizierung von Schwachstellen in Systemen und Netzwerken.

2

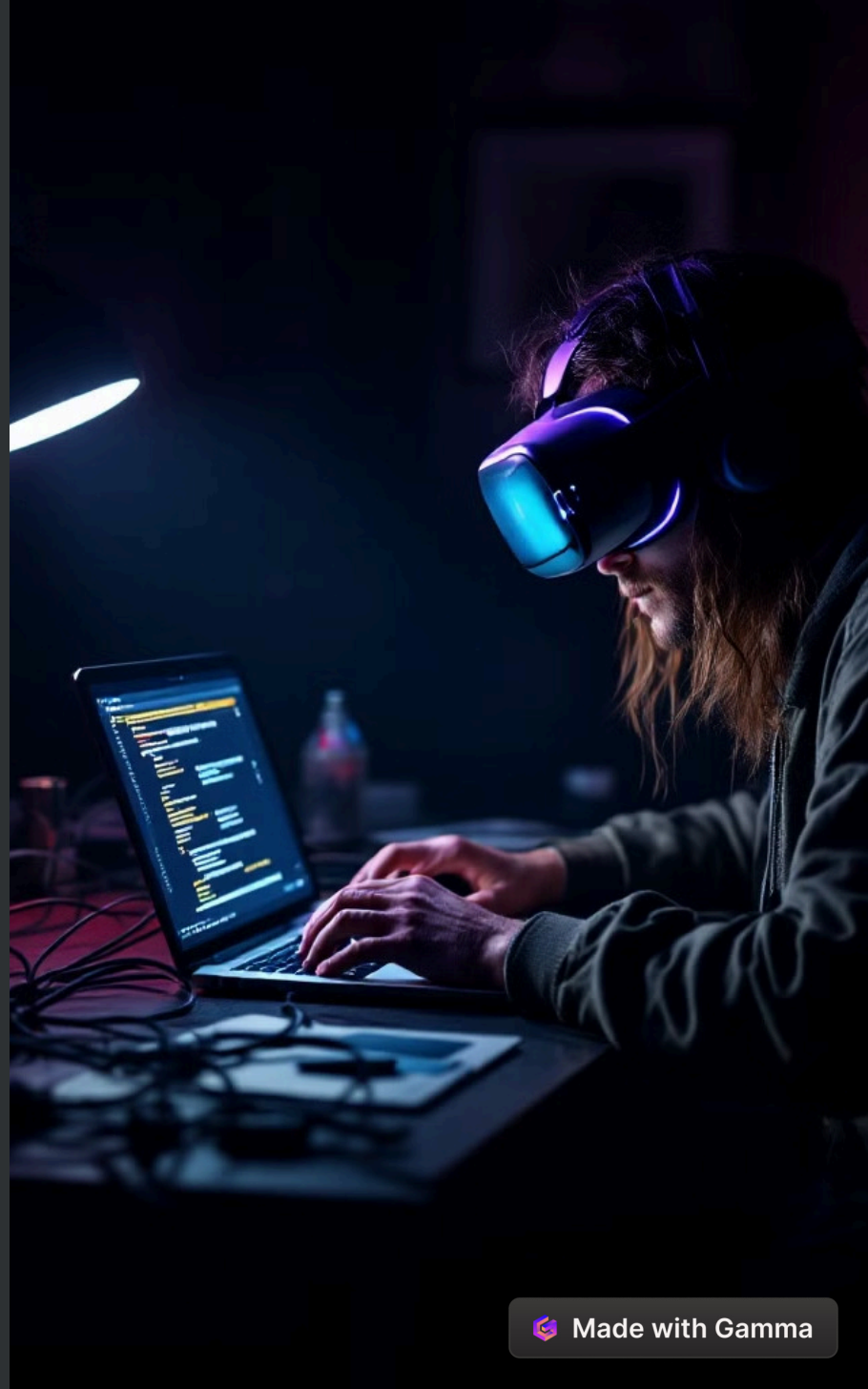
Angriffe simulieren

Simulation von realen Angriffen, um die Effektivität von Sicherheitsmaßnahmen zu testen.

3

Berichte erstellen

Dokumentation von Schwachstellen und Empfehlungen zur Behebung.



IT-Forensiker: Digitale Spurensuche und Beweissicherung

1

Beweise sichern

Identifizierung und Sicherung von digitalen Spuren.

2

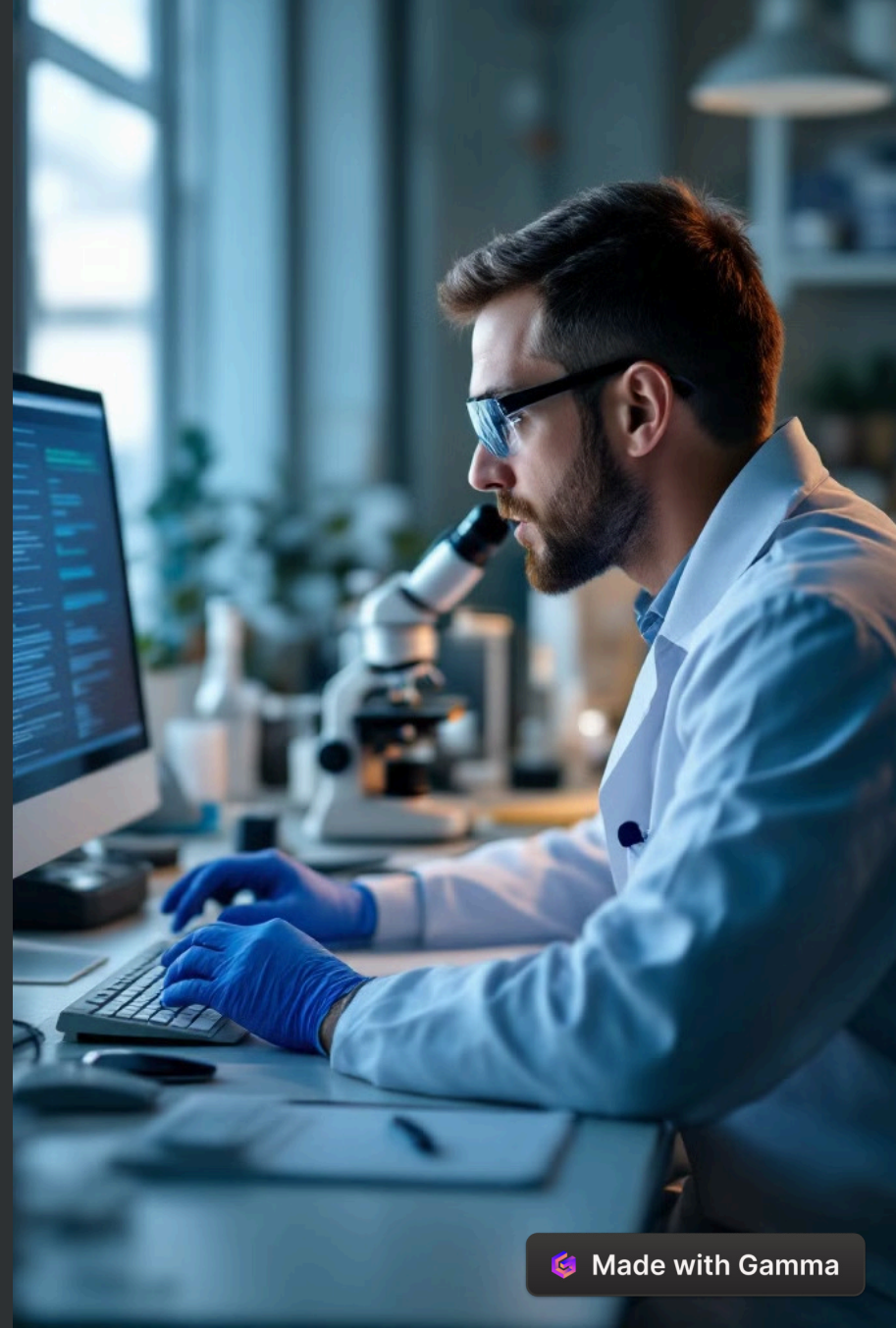
Daten analysieren

Analyse von Daten, um den Tathergang zu rekonstruieren.

3

Berichte erstellen

Erstellung von forensischen Berichten für Strafverfolgungsbehörden.



Cyber-Abwehranalyst: Erkennung und Reaktion auf Sicherheitsvorfälle

1

Vorfälle erkennen

Überwachung von Netzwerken und Systemen auf verdächtige Aktivitäten.

2

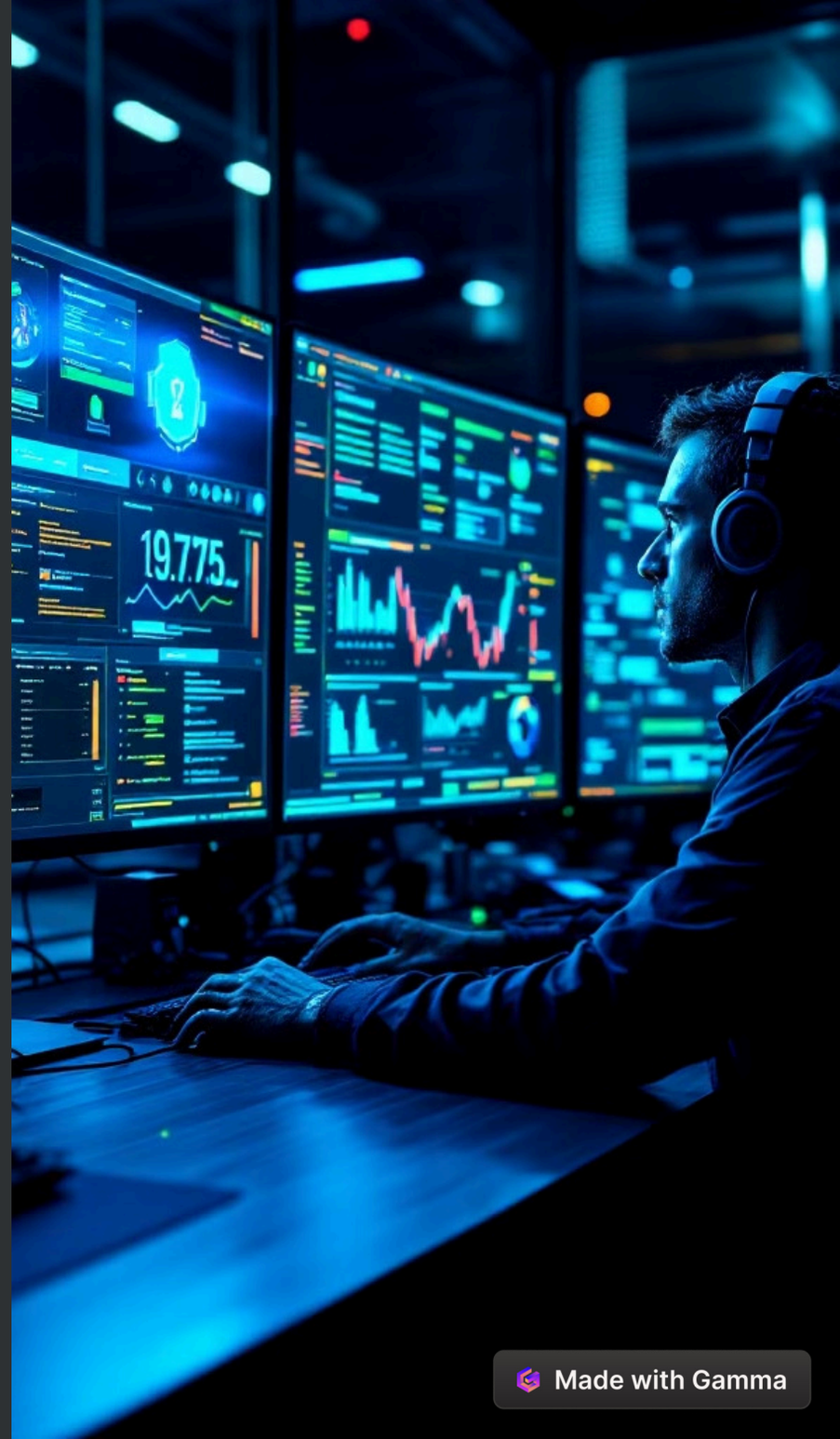
Vorfälle analysieren

Analyse von Daten, um den Ursprung und die Auswirkungen eines Vorfalls zu bestimmen.

3

Maßnahmen ergreifen

Implementierung von Maßnahmen zur Eindämmung und Behebung des Vorfalls.



Compliance-Manager: Einhaltung von Gesetzen und Vorschriften

1

Gesetze kennen

Verständnis der relevanten Datenschutz- und Sicherheitsgesetze.

2

Vorschriften einhalten

Sicherstellung der Einhaltung von Sicherheitsrichtlinien und -standards.

3

Kontrollen durchführen

Durchführung von regelmäßigen Sicherheitsaudits.