Orange
Cyberdefense

Analyst as a Service

Erleben Sie Cyberdefense aus einer neuen Perspektive

Cyberkriminelle sind heute aktiver denn je und wenden ständig wechselnde Taktiken an, um digitale Schwachstellen auszuhebeln. Zur Bewältigung dieser Herausforderungen ist gut ausgebildetes IT-Security-Fachpersonal erforderlich, welches nur schwer am Arbeitsmarkt zu finden ist oder langfristig intern ausgebildet werden muss. Vor diesem Hintergrund sind bestehende IT-Security-Teams häufig unterbesetzt und bei komplexeren Sicherheitsvorfällen überfragt. Dies führt dazu, dass hochentwickelte Angriffe, wie beispielsweise Advanced Persistent Threats (APTs), oftmals lange Zeit unerkannt bleiben und dadurch die Wahrscheinlichkeit für schwerwiegende Auswirkungen auf das Unternehmen zunehmend steigt.

Digitalisierung um jeden Preis

Um nicht den Anschluss an den Markt zu verlieren, sind Unternehmen im Zuge der immer schneller voranschreitenden digitalen Transformation gezwungen, ihre bestehenden Geschäftsprozesse zu optimieren und diese durch innovative und schlanke Prozesse zu ersetzen. Dabei spielen neue digitale Technologien, wie beispielsweise Cloud Computing oder künstliche Intelligenz sowie eine weiterhin zunehmende globale und mobile Vernetzung eine zentrale Rolle.

Hinzu kommen noch weitreichende interne und externe Anforderungen an den Sicherheitsbetrieb um den Ansprüchen der Compliance und Regulatorik zu genügen. So werden oftmals neue Produkte und Services auf der Basis neuer Trends und Möglichkeiten auf den Markt gebracht, ohne dass diese ausreichend auf vorhandene Risiken hin untersucht werden oder sicher betrieben werden können.

Cybersecurity Manpower und Expertise

In der „Cybersecurity Workforce“ Studie der führenden Zertifizierungsorganisation (ISC)^2 gaben beinahe zwei Drittel (65%) der Unternehmen einen Mangel an IT-Security-Fachkräften an und mehr als die Hälfte (51%) der Befragten meldeten, dass Ihr Unternehmen aufgrund des Mangels an IT-Security-Fachkräften einem hohen Risiko ausgesetzt ist.

Eine passgenaue und effiziente Lösung bieten hierbei unsere Analysten, welche Ihr Security-Team entscheidend unterstützen können. Durch die Erfahrung aus unterschiedlichsten Kundenprojekten können unsere Analysten Ihr In-House-Team gleichermaßen beim Aufbau Ihres Security Operations Centers (SOC) sowie bei der Optimierung Ihrer Prozesse begleiten. Profitieren Sie von unserer Expertise und Manpower für kurz- oder langfristige Einsätze und stärken Sie Ihre digitale Verteidigung.

Unsere Erfahrung

Mit Orange Cyberdefense als strategischem Partner greifen Sie auf umfassende Erfahrungen aus fast 20 Jahren Cybersecurity im Rahmen vielseitiger Kundenprojekte zurück, vom organisatorischen und technischen Aufbau von SOCs bis hin zu zeitkritischen CSIRT-Einsätzen.

Unsere Analysten und Incident Responder werden gleichermaßen wie unsere Mitarbeiter in den weltweit 17 Orange Cyberdefense SOCs ausgebildet und nehmen unter anderem auch an den Cyber Range Simulation (CSR) Schulungen des Information Security Hub (ISH) Trainingscenters am Flughafen München teil.

Darüber hinaus besteht auch jederzeit die Möglichkeit, Teilbereiche Ihrer Cybersecurity-Strategie auf Grundlage unserer Managed Security Services auszulagern. Auf diese Weise passen wir uns optimal an die Anforderungen Ihres Geschäftsbetriebs an. Gehen Sie den nächsten Schritt, und bringen Sie Ihre Cyberdefense auf das nächste Level.

Mehr professionelle Schulungen finden Sie unter:
orangecyberdefense.com/de/academy

Welche Aufgaben hat ein Security Analyst im SOC

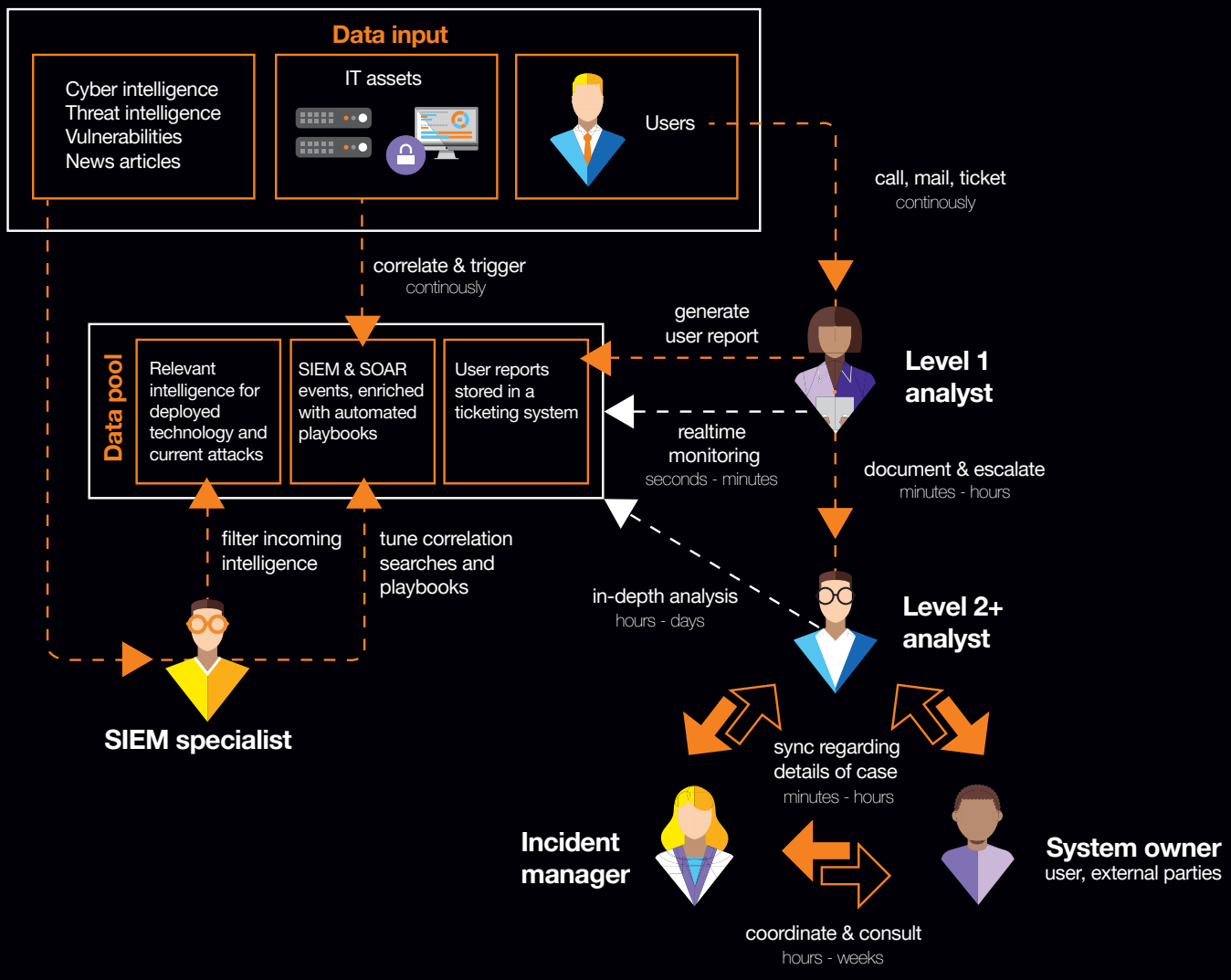
Security Analysten sind häufig die erste Instanz bei potenziellen Security-Vorfällen, indem Sie unter anderem Anomalien im Geschäftsbetrieb feststellen, Anrufe von Nutzern entgegennehmen oder erfasste Alarmierungen des Monitoring-Systems untersuchen. Sie lösen die Vorfälle durch eine systematische Auswertung vorhandener Daten mit Hilfe einer Kombination aus freien OSINT-Tools und kommerziellen Cybersecurity-Lösungen, welche zusammen den sogenannten „SOC Toolstack“ darstellen.

Das Team der Security Analysten lässt sich hinsichtlich unterschiedlicher Aufgabenfelder sowie Erfahrungen in Spezialbereichen wie Forensik oder CSIRT-Einsätze unterscheiden. Analysten auf Level 1 bilden hier die Schnittstelle anderer Teams und Nutzer zum SOC und starten in Echtzeit den Bearbeitungsprozess des gesamten Spektrums der auftretenden Security-Vorfälle und beurteilen die Kritikalität dieser. Nach dem Erstkontakt mit dem Vorfall übergibt der Level 1 Analyst die weitere Bearbeitung anhand definierter Kriterien und Prozesse an Level 2 & 3 Analysten.

Level 2 & 3 Analysten sind Experten hinsichtlich der eingesetzten Tool- und Systemlandschaften und besitzen viel Erfahrung hinsichtlich wiederkehrender Angriffsvektoren, aktuell eingesetzter Malware und der optimalen Verteidigung. Sie beschäftigen sich vor allem mit der detaillierten Untersuchung der Vorfälle und ermitteln die zugrundeliegende Ursache dieser. In den meisten Fällen ist hierbei auch ein Austausch mit beteiligten Fachbereichen notwendig. Für die Nachverfolgung und vollständige Beseitigung der Vorfälle erfolgt eine planmäßige Übergabe der Bearbeitung vom Analysten an die Incident Manager.

Das Hauptaugenmerk der Incident Management Rolle ist hierbei die Synchronisation aller Bemühungen und die Kommunikation mit beteiligten Fachkräften und Stakeholdern. Zur Erfüllung dieser Aufgabe ist eine einzigartige Synergie aus analytischen, pragmatischen und koordinativen Kompetenzen erforderlich.

Rollenverteilung in einem SOC Team



Mehr professionelle Schulungen finden Sie unter:
orangecyberdefense.com/de/academy

Leistungsumfang Analyst as a Service

Strategische Unterstützung:

- Unterstützung bei der Planung und dem Aufbau eines SOCs
- Beratung bei der Optimierungen Ihrer SOC Prozesse
- Erarbeitung von Empfehlungen hinsichtlich der Erweiterung der Monitoring Fähigkeiten
- Unterstützung bei der Bewertung und Auswahl von SOC-Technologien

Projektbezogene Unterstützung:

- Systematische Verarbeitung von Security-relevanten Alarmen im Rahmen einer Level 1 Analyst Rolle
- Erstellung einer Dokumentation der Analyseergebnisse für den Incident Management Prozess, sowie für IT Security Audits
- Koordinierte Durchführung von Threat Hunting innerhalb und außerhalb Ihrer Organisation sowie eine schnelle Verifikation von festgestellten Schwachstellen
- Gestaltung von Dokumentationen und Wissensdatenbanken für häufig auftretende Vorfälle sowie für bestehende Prozesse

Organisatorische und operative Unterstützung:

- Unterstützung bei der Erstellung von Indikatoren im SIEM / Threat Intelligence Umfeld
- Entwurf von Playbooks (toolgestützt automatisiert oder manuell) für die standardisierte Abarbeitung von Security-Indikatoren / Tickets
- Beratung zum Aufbau und der Pflege einer Configuration Management Database (CMDB)
- Aufgabenverteilung und -kommunikation gemäß der drei beschrieben Rollen im SOC-Umfeld

Leistungsumfang der Level 1-3 Security Analysten	Level 1	Level 2	Level 3
Standardisierte Abarbeitung von Sicherheitsvorfällen innerhalb festgelegter SLAs	✓	✓	✓
Einsatz definierter Playbooks und Threat Intelligence Systeme	✓	✓	✓
Realtime Überwachung von Informationssystemen und Dashboards	✓	✓	✓
Playbook und Use Case Development	✗	✓	✓
Detaillierte Untersuchung von Sicherheitsvorfällen	✗	✓	✓
Proaktives Threat Hunting	✗	✓	✓
Malware Analyse und Reversing	✗	✗	✓
Training und Weiterbildung von Level 1 und 2 Analysten	✗	✗	✓
Beratung hinsichtlich Planung und Aufbau eines SOC, inkl. relevanter Prozesse	✗	✗	✓

Mehr Infos finden Sie auf
www.orangecyberdefense.de

Orange Cyberdefense
Paul-Gerhardt-Allee 24, 81245 München

info@de.orangecyberdefense.com
+49 89 2000148 00