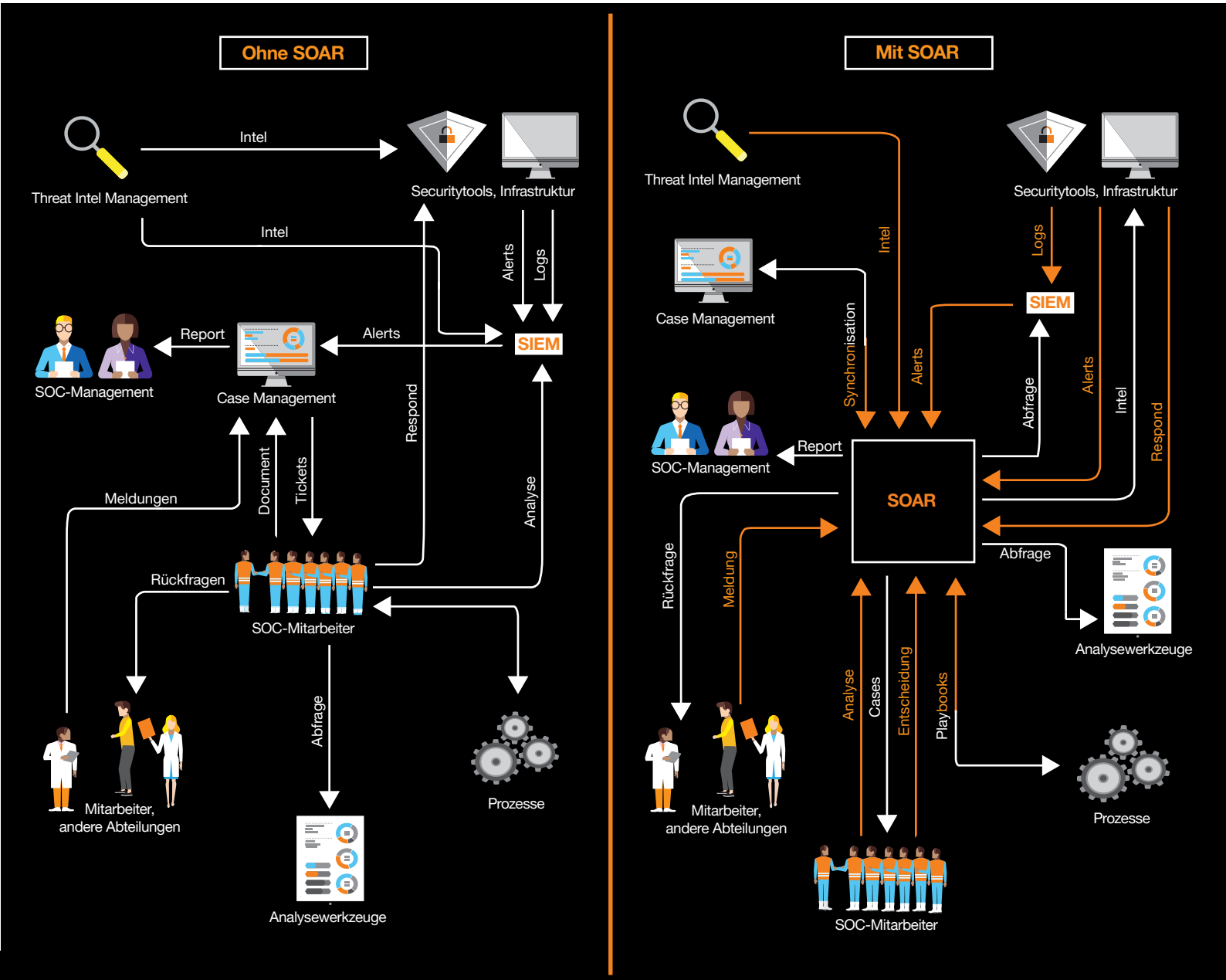
Orange
Cyberdefense

Das SOC der Zukunft: Security Orchestration, Automation and Response

Mehr Sicherheit und Effizienz durch Automatisierung

Analysten im Security Operations Center (SOC) sind einen Großteil ihrer Zeit mit sich wiederholenden Aufgaben beschäftigt. Immer wieder die gleichen Schritte zur Informationsbeschaffung bei sich ähnelnden Vorfällen durchzuführen führt zu Frustration und zunehmender Nachlässigkeit, der sogenannten Alert Fatigue. Die Nutzung einer Software zur Security Orchestration, Automation and Response (SOAR) kann hier Abhilfe schaffen. Diese unterstützt Ihre Analysten durch automatisierte Anreicherung und Verknüpfung von Informationen. Durch Playbooks wird die Einhaltung Ihrer Security-Prozesse sichergestellt und deren Ablauf durch Automatisierung beschleunigt.



Schnellere Bewertung von Incidents

In der Regel werden die eintreffenden Alarme von verschiedenen Quellen wie etwa Security Incident and Event Management (SIEM), Endpoint Protection Software oder Meldungen von Nutzern in einem Ticketsystem gesammelt und durch ein Team von First Level Analysten bearbeitet. Diese nehmen eine erste Bewertung des Vorfalls vor, wofür der Alarm jedoch nur selten ausreichend Informationen enthält. Zunächst müssen daher die Indikatoren mit weiteren Daten angereichert werden, was beispielsweise durch Abgleich mit Merkmalen früherer Angriffe und Ausführung von Dateien in Sandboxes geschieht. Oft kommt dabei eine Vielzahl von Systemen und Webdiensten zum Einsatz, deren Ergebnisse dann wieder in das Ticketsystem übertragen werden.

Im SOAR lassen sich die genutzten Werkzeuge zur Anreicherung von Indikatoren direkt integrieren, so dass diese Schritte direkt aus der Oberfläche erfolgen können.

Die Ergebnisse werden ebenso wie manuelle Notizen zu dem Incident dauerhaft gespeichert. In einem zweiten Schritt lässt sich die Anreicherung automatisieren, sodass das SOAR sie nach Erkennung eines Vorfalls selbstständig ausführt und den Analysten bei Öffnen des Tickets direkt die angereicherten Informationen vorliegen. Manuelle Standardtätigkeiten und die Wartezeit auf Analyseergebnisse können somit eingespart werden, und die Analysten können sich auf die Auswertung der aufbereiteten Information und tiefergehende Recherchen konzentrieren.

Die Experten von Orange Cyberdefense haben jahrelange Erfahrung mit verschiedensten Securitylösungen und beraten und unterstützen Sie bei deren Integration in Ihr SOAR. Als SIEM-Spezialisten optimieren wir Ihre SIEM-Alarme so, dass die von dort weitergeleiteten Incidents die nötige Qualität aufweisen und beide Tools ideal zusammenarbeiten.

Unterstützung bei der Reaktion auf Sicherheitsvorfälle

Ebenso wie die Werkzeuge zur Informationsbeschaffung lassen sich auch IT-Infrastruktur und IT-Security Systeme in das SOAR integrieren. Dadurch können direkt aus dem System heraus Response Aktivitäten ausgeführt werden, wie beispielswiese Verbindungen in der Firewall zu trennen, Rechner in Quarantäne zu stellen oder Informationen an Nutzer und Management zu versenden. Durch individuelle Playbooks lassen sich die bestehenden Prozesse inklusive der Einbindung von Entscheidungsträgern passgenau umsetzen, wobei bei jedem Schritt einzeln festgelegt werden kann, ob er automatisiert oder manuell durchgeführt werden soll. Wie zuvor bei der Informationsbeschaffung werden auch bei der Incident Response sämtliche manuell oder automatisiert durchgeführten Schritte zusammen mit dem Incident gespeichert und somit nachvollziehbar dokumentiert. Das umfasst auch zusätzlich zum Playbook manuell ausgeführte Kommandos. Für das SOC-Management stehen umfangreiche Dashboard- und Reporting-Möglichkeiten zur Verfügung, um stets über die aktuelle Lage und getroffene Maßnahmen informiert zu bleiben.

Orange Cyberdefense betreibt seit vielen Jahren eigene SOCs als Managed Service und unterstützt Kunden bei Aufbau und Betrieb ihres eigenen SOCs. Mit unserer Erfahrung beraten wir Sie gerne bei der Optimierung der Abläufe in Ihrem SOC und passen die mit Ihrem SOAR gelieferten Playbooks daran an, oder erstellen neue Playbooks gemäß Ihren Anforderungen. Dafür nötige Tools wie beispielsweise ein externes Ticketsystem werden dabei über die jeweiligen Programmierschnittstellen mit dem SOAR verbunden.

Threat Intelligence Management

Eine wichtige Maßnahme zur kontinuierlichen Verbesserung Ihrer IT-Sicherheit ist das Auswerten interner und externer Bedrohungsinformationen. Die Indicators of Compromise (IOCs) von gelösten Incidents bleiben daher im SOAR gespeichert, so dass bei neuen Incidents gegebenenfalls ein Bezug hergestellt und die Bewertung erleichtert werden kann. Viele SOAR-Lösungen unterstützen zudem die Anbindung einer Vielzahl von kostenfreien und kostenpflichtigen Threat Intelligence Feeds, um neue IOCs in die Datenbank zu integrieren und vorhandene IOCs um weitere Informationen zu ergänzen.

Wenn Sie bereits Threat Intelligence Feeds verwenden, integrieren wir diese in Ihr SOAR. Andernfalls beraten wir Sie gerne mit unserer Erfahrung bei der Auswahl und Bewertung geeigneter Angebote.

Anpassung und Erweiterung für Ihre Umgebung

Sämtliche Playbooks, Integrationen, Automatisierungen und weitere Inhalte im SOAR lassen sich modifizieren. Durch Hinzufügen eigener Inhalte können Systeme angebunden und Prozesse umgesetzt werden, die in der Standardinstallation nicht enthalten sind. Die Implementierung geschieht mit Standardtechnologien, sodass keine lange Einarbeitung nötig ist. Gemeinsam mit Ihnen sorgen wir dafür, dass Ihr SOAR ideal an Ihre Anforderungen angepasst ist und mit der Entwicklung Ihrer Security Organisation Schritt hält, damit Sie und Ihre Mitarbeiter sich ganz auf die relevanten Bedrohungen fokussieren können.

Unser Mehrwert

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 Security Spezialisten sind erfahren in Einrichtung und Betrieb einer breiten Palette von Securitylösungen und durch die Zusammenarbeit mit Analysten und Incident Respondern in den weltweit 17 Orange Cyberdefense SOCs stets über aktuelle Best Practices Betrieb informiert. Durch den Einsatz eines SOAR als Schaltzentrale Ihres SOC profitieren Sie davon optimal und ermöglichen Ihren Mitarbeitern, auf die relevanten Bedrohungen schnell zu reagieren. Wir können Sie sowohl bei der Evaluation Ihrer aktuellen Security Architektur als auch bei der Einführung und dem Betrieb eines SOAR unterstützen.

Darüber hinaus besteht auch jederzeit die Möglichkeit, Teilbereiche Ihrer Cybersecurity-Strategie durch unsere umfangreichen 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 mit uns Ihre Cyberdefense auf das nächste Level.

Mehr Infos finden Sie auf
www.orangecyberdefense.de

Orange Cyberdefense
Paul-Gerhardt-Allee 24, 81245 München

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