Orange
Cyberdefense

Managed Threat Detection [log]

Terabytes von Informationen machen noch kein Wissen. Ein guter Threat Hunter erkennt auch Angriffe, die den Automatismen entgehen

Damit Ihrer Abwehr nichts entgeht

Keine Schutzmaßnahme ist unfehlbar. Umso wichtiger ist es, für den Fall gerüstet zu sein, wenn Angreifer Schutzmaßnahmen aushebeln oder umgehen. Mögliche Eindringlinge zuverlässig erkennen zu können, ist die essentielle Grundlage für die erfolgreiche Abwehr von Cyber-Angriffen und eine Schlüsselfunktion für Organisationen, um sich vor Schäden durch Cyber-Attacken zu schützen.

Die Cyber Security Analysten in unseren 10 globalen Cyber SOCs überwachen mit Hilfe modernster Technologie die IT-Infrastrukturen unserer Kunden. Ganz gleich, ob mittelständiges Produktionsunternehmen oder global agierender Technologiekonzern– wir sind den Angreifern auf der Spur und sorgen dafür, dass Sie über auftretende Bedrohungen, Sicherheitsrisiken und Regelverstöße informiert werden und stehen Ihnen mit Rat und Tat zur Seite..

Network & Infrastructure

- Security Information und Event Management (SIEM)
- Network Intrusion Detection (NIDS)
- Network Behavior Analysis (NBA)
- Sandboxing
- Threat Intelligence
- System Monitoring

User & Identity

- User und Entity Behavior Analysis (UEBA)
- Cloud Access

Endpoint & Application

- Endpoint Behavior Analytics
- Hostbased Intrusion Detection (HIDS)
- File Integrity Monitoring (FIM)

Threat Detection [log] – Managed SIEM

Problem:

Das SIEM-System ist die Alarmanlage der Cyber-Abwehr, doch nur, wenn sie funktioniert und scharf geschaltet ist, erfüllt sie ihren Zweck. Dafür sind Experten notwendig, die die Funktionsfähigkeit Ihres SIEM-Systems gewährleisten und zwar 24 Stunden am Tag, 365 Tage im Jahr.

Lösung:

Mit Managed Threat Detection [log] – Managed SIEM kümmern wir uns um alle Belange Ihres SIEM-Systems und sorgen dafür, dass es Ihnen als schlagkräftiges Verteidigungsmittel gegen Cyber-Angriffe zur Verfügung steht.

Das Managed SIEM Paket enthält:

- Incident Management
- Remote Troubleshooting
- Remote Fault Remedy
- SIEM Monitoring
- Hardware Monitoring (for hardware appliances)
- OS and Application Monitoring
- System Function Monitoring
- Log Source Monitoring
- Lifecycle Management
- Configuration Change Management
- Backup & Restore
- Content Updates
- Software Upgrades
- 8×5 or 24×7 Service

Pro Service

Erfahren Sie mehr dazu, wie Sie Angriffe erkennen, bevor sie Schaden anrichten:
orangecyberdefense.com/de/detect/

Problem:

Viele SIEM-Implementierungen scheitern, weil zwar massive Datenmengen in das SIEM eingespeist werden, dieses aber out-of-the-box nur einen begrenzten Mehrwert bietet.

Auch die meist zahlreich mitgelieferten Detection Use Cases sind oft nur in sehr begrenztem Umfang nutzbar. Einige lassen sich nach umfangreichen Anpassungen verwenden. Mit unseren Standard Use Cases decken wir weit verbreitete Angriffsszenarien ab und schaffen so unmittelbaren Mehrwert. Werden SIEM-Installationen nicht kontinuierlich aktualisiert, um auch neue Bedrohungen erkennen zu können, sinkt ihr Nutzen rapide.

Lösung:

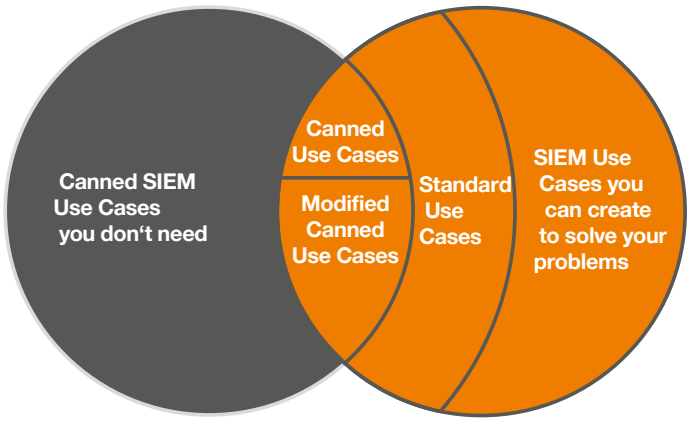
Auch wenn die Analyse von sicherheitsrelevanten Ereignisdaten einen hohen Automatisierungsgrad erfordert, ist sie doch kein vollständig automatisierbarer Prozess. Nur wem es gelingt, modernste Analysetechnologie mit dem Know-how menschlicher Experten zu verknüpfen, wird den Angreifern weiterhin ein Stück voraus sein und die Oberhand behalten. Genau diesen Ansatz verfolgen wir in unserem Advanced Cyber Defence Center, indem wir modernste Sensorik und Analysemethoden mit der Expertise unserer Cyber Security Analysten kombinieren und in Form unseres Security Analysis Service unseren Kunden zur Verfügung stellen.

Managed Threat Detection [log] – Security Analysis basiert auf der Analyse von sicherheitsrelevanten Logdaten aus der IT-Infrastruktur unserer Kunden. Diese Logdaten werden durch ein SIEM-System gesammelt, das in diese Infrastruktur integriert wird. Ein SIEM-System sorgt für gute Transparenz und Visibilität hinsichtlich sicherheitsrelevanter Ereignisse. Doch Daten zu sammeln ist ein Schritt, daraus die richtigen Schlüsse zu ziehen ein weiterer.

Die gesammelten Daten müssen korreliert und mit weiteren Informationen angereichert werden, bevor sie durch Experten interpretiert werden können. Erst dann ist es möglich daraus wichtige Erkenntnisse abzuleiten, um die richtigen Maßnahmen zur Verhinderung oder Eindämmung von Security Incidents zu ergreifen.

Unser Advanced Cyber Defence Center entwickelt fortwährend neue Erkennungsmethoden für sog. Indikatoren, die in unsere Standard Use Cases integriert werden. Ihre Investition in Ihr SIEM-System ist damit dauerhaft geschützt!

Use-Case-based Approach



Quelle: basiert auf Dr. Anton Chuvakin, Research VP, Gartner's GTP Security and Risk Management Group

Unsere Standard Use Cases decken verbreitete Angriffsszenarien ab. Sie erfüllen damit die Anforderungen aus verschieden Security Standards und Frameworks wie CIS Critical Security Controls, ISO/IEC 27001 oder PCI-DSS.

Das Managed SIEM - Security Analysis Paket enthält:

- 8×5 oder 24×7 Service
- Use-Case-basierter Analyseansatz zur zuverlässigen-Erkennung von Sicherheitsvorfällen
- Standard Use Cases inklusive – Unsere Standard Use Cases sorgen für eine sofortige Operationalisierung Ihres SIEMs.
- **Optional:** Überwachung von Add-On Use Cases – Hiermit werden auch kundenspezifische Erkennungsszenarien nahtlos integriert.
- **Optional: Threat Hunting** – Die ideale Ergänzung zum deterministischen Ansatz eines SIEMs, um neue Angriffsvektoren zu identifizieren und Erkennungsszenarien und die dafür notwendigen Indikatoren zu aktualisieren.

Mehr Infos finden Sie auf
www.orangecyberdefense.de

Orange Cyberdefense
Paul-Gerhardt-Allee 24, 81245 München

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