DATASHEET

8com Security Operations Center
Analyse

HIGHLIGHTS

- **Tiefgehende Threat-Untersuchung durch SOC-Analysten**
  Erfahrene SOC-Analysten untersuchen ausgegebene Alarme und garantieren schnelles und hocheffizientes Threat Handling.
- **Malware Analysis**
  Durch Debugging und Reverse Engineering wird selbst das Verhalten raffiniertester Programme erfasst und die Erkennung dementsprechend konfiguriert.
- **Einbezug unterschiedlichster Bedrohungsinformationen**
  Threat Feeds, Indicators of Compromise (IoC) und die Erkenntnisse anderer Fachabteilungen liefern wichtige Hinweise auf Bedrohungen.
- **Analysen durch IT-Forensiker**
  Vorfallanalysen liefern wertvolle Einblicke zur Vermeidung künftiger Vorkommnisse.
- **Interdisziplinärer Wissensaustausch**
  Täglicher Wissensaustausch unterschiedlicher Expertenteams.

Ausgegebene Bedrohungsalarme werden im ersten Schritt von SOC-Operatoren untersucht. Sie entscheiden, ob es sich um True Positives oder False Positives handelt.

True Positives werden umgehend zur weiteren Untersuchung an die SOC-Analysten gemeldet. Die Resultate der False-Positive-Bewertung dienen der kontinuierlichen Verbesserung der Bedrohungserkennung.

Bei der Untersuchung von True Positives bedienen sich die SOC-Analysten unterschiedlichster Indikatoren und branchenspezifischer Bedrohungsinformationen. Umfassende Malware-Analysen liefern wichtige Erkenntnisse zum Verhalten von Schadprogrammen und den Ausbreitungswegen von Cyberangriffen.

Tiefgreifende forensische Untersuchungen dienen nicht nur der gerichtsverwertbaren Beweissicherung sondern auch der Analyse und Aufklärung von Störungen oder Fehlfunktionen zur Vermeidung künftiger Vorfälle.

8com GmbH & Co. KG

Europastraße 32
67433 Neustadt a. d. Weinstraße
Germany

+49 6321 48446-0
info@8com.de
www.8com.de