Mehrstufige Cyber-Angriffe sofort detektieren
03. & 12. September 2024

HUNTERS

AVANTEC
Competence. Security. Trust.

Durch Korrelation und Auto-Investigation mehrstufige Cyber-Angriffe detektieren

Christian Grob
Head of Security Services
grob@avantec.ch

Ian Forrest (Hunters)
Vice President Sales Engineering
ian.forrest@hunters.security

Fokus heutiges Webinar

AVANTEC
Competence. Security. Trust.

Cyber Defense Portfolio

Managed EDR (CROWDSTRIKE)
- Erkennung & Verhinderung der Ausbreitung von Cyberangriffen mittels schlankem Endpoint Agent
- Next GEN AV, EDR , Threat Hunting
- Umfangreiche Handlungsoptionen, direkter Eingriff auf Endpoints

Managed NDR (VECTRA)
- Erkennung & Verhinderung der Ausbreitung von Cyberangriffen durch Überwachung des Netzwerkverkehrs
- Kombination verschiedener Analyse-Verfahren u.a. ML/AI
- Ohne Agent auf den Endpoints

Webinar

Managed Security Analytics (Hunters.)
- Korrelation & Analyse von sicherheitsrelevanten Daten auf Basis der Hunters SOC Plattform
- Moderne SOC Plattform mit «Detection Engineering als Service» - 75-95%
- Keine Limiten für Log Ingestion

Vulnerablity Scanning (tenable)
- Identifikation von Schwachstellen mit regelmässigen Scans von extern oder intern
- Verwaltung der Scan Policies
- Regelmässiges Reporting mit Empfehlungen
- Verwalten der False-Positives

Dark Web Monitoring (KADUU)
- Überwachung des Dark Web auf Data Leaks, Account Leaks & auffällige Erwähnungen in Foren
- Überwachung von Paste Sites, Onion Sites, Git
- Überwachung Ransomware Extortion Sites

Threat Intelligence (Recorded Future)
- Bereitstellung hochwertiger Threat Intelligence
- Unternehmensspezifische Threat Landscape
- Betrieb einer MISP Instanz inkl. Bereitstellung von Feeds - Indicators of Compromise (IOC)

AVANTEC
Competence. Security. Trust.

Mehrstufige Cyber-Angriffe sofort detektieren
03. & 12. September 2024

Herausforderungen

Im Bereich Security Analytics / «SIEM»

1

Ungenügende Threat Coverage

- Aufwendiges Use Case Engineering, trotzdem schlechte Erkennungsraten
- Transparenz hinsichtlich Abdeckung fehlt oder wird Dynamik der Bedrohungslandschaft nicht gerecht – Use Cases schnell veraltet

2

Wachsendes Log Volumen führt zu stetig steigenden Kosten

- Lizenzierung nach Log-Volumen führt zu schlechter Planbarkeit
- Relevante Logs werden aufgrund der Kosten nicht berücksichtigt

3

Zu viele Security Alerts/False-Positives

- Überlastete Teams aufgrund hoher false positive Raten
- Zeitverlust durch manuelle Analysen und durch eine hohe Anzahl an Alerts

Unterschied mit Hunters

… und wie die Herausforderungen adressiert werden

1

Ungenügende Threat Coverage

- ➡ Up-to-Date Detection: 75-95% des Detection Engineerings durch Hunters in hoher Qualität sichergestellt und weiterentwickelt
- ➡ Volle Transparenz in der Plattform mit MITRE ATT&CK Mapping (dynamisch)

2

Wachsendes Log Volumen führt zu stetig steigenden Kosten

- ➡ Host basiertes Lizenzmodell – mit unlimitierter «Log-Ingestion»
- ➡ Finanzielle Planungssicherheit über mehrere Jahre

3

Zu viele Security Alerts/False-Positives

- ➡ Massive Reduktion der zu analysierenden Alerts durch Korrelierung, Kontextualisierung und Auto Investigation
- ➡ L1/L2 Tätigkeiten grösstenteils obsolet

AVANTEC
Competence. Security. Trust.

Mehrstufige Cyber-Angriffe sofort detektieren
03. & 12. September 2024

Operating - Model

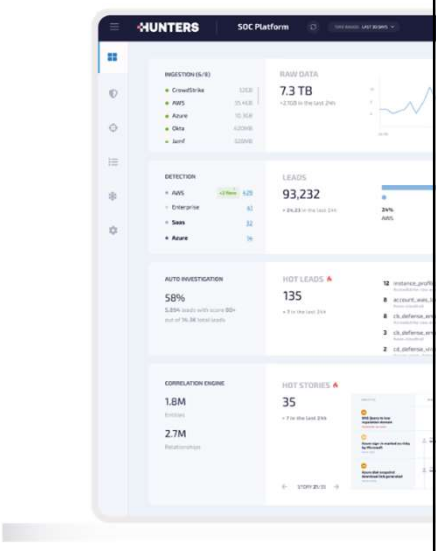
	MSSP - Managed Security Analytics	Resell - Hunters SOC Platform
Beschreibung	▪ AVANTEC stellt die Hunters SOC Platform als Teil des Managed Services zur Verfügung	▪ Kunde bestellt die Lösung via AVANTEC – Subscription

Security Monitoring
Investigation
Incident Response
	▪ AVANTEC Cyber Defense Team
	  ▪ analysiert und triagiert Security Alerts 24/7 gemäss SLA
	  ▪ führt bei Bedarf tiefergehende Investigation durch
	  ▪ leitet Massnahmen gemäss Playbooks ein
		▪ Kunde verfügt über eigene Cyber Defense - SOC Ressourcen

Erreichbarkeit	▪ 24/7 Zugriff auf zertifizierte Cyber Security Experten (u.a. GIAC Certified Forensic Analyst (GCFA), GIAC Continuous Monitoring (GMON)	▪ Bürozeiten
Status Überwachung	▪ AVANTEC überwacht die angebunden Log-/Daten Quellen	▪ Kunde überwacht Status
Verwaltung und Konfiguration	▪ AVANTEC verwaltet die Tenant Konfiguration und überprüft diese regelmässig	▪ Kunde verwaltet die Konfiguration
Onboarding von Log-/Daten-Quellen	▪ AVANTEC unterstützt beim Onboarding und stellt die korrekte Integration in der Plattform sicher	▪ Kunde integriert neue Log-/Daten-Quellen
AVANTEC Support	▪ Pauschal im Service inkludiert	▪ Time & Material

AVANTEC
Competence. Security. Trust.

HUNTERS SOC PLATFORM



AVANTEC
Competence. Security. Trust.