Alternativen zu einem SIEM Webinar
09. & 15. November 2023

Webinar: Alternativen zu einem SIEM

Tobias Balschun
Tec Lead Cyber Defense
balschun@avantec.ch

Robin Helbling
Cyber Defense Specialist
helbling@avantec.ch

Christian Grob
Head of Security Services
grob@avantec.ch

Agenda

1	**Einleitung**	Christian Grob
2	**Vorstellung Hunters SOC Platform inkl. Live Demo**	Robin Helbling
3	**Vorstellung Recorded Future Intelligence Portal inkl. Demo**	Tobias Balschun
4	**Q&A**	Alle

Alternativen zu einem SIEM Webinar
09. & 15. November 2023

Herausforderungen

AVANTEC
Competence. Security. Trust.

bei der Threat Detection mit klassischem SIEM Ansatz

1

Ungenügende Threat Coverage

- Aufwendiges Use Case Engineering, trotzdem geringe Erkennungsraten
- Transparenz hinsichtlich Abdeckung fehlt oder wird Dynamik der Bedrohungslandschaft nicht gerecht

2

Stetig steigende, zu hohe Kosten

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

3

Zu viele Security Events/False-Positives

- Überlastete Teams aufgrund hoher false positives
- Zeitverlust durch manuelle Analysen durch eine hohe Anzahl an Events

Fokus heutiges Webinar

AVANTEC
Competence. Security. Trust.

Cyber Defense Portfolio

CROWDSTRIKE

Managed EDR

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

VECTRA

Managed NDR

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

tenable

Vulnerablity Scanning

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

KADUU

Dark Web Monitoring

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

Webinar

Hunters.

Managed Security Analytics

- 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

Recorded Future

Threat Intelligence

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

AVANTEC
Competence. Security. Trust.

Alternativen zu einem SIEM Webinar
09. & 15. November 2023

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 Platform sicher	▪ Kunde integriert neue Log-/Daten-Quellen
AVANTEC Support	▪ Pauschal im Service inkludiert	▪ Time & Material

Managed Security Analytics mit Hunters

Top drei Use Cases

- Security Analytics: Vendor agnostisches Security Analytics mit planbaren Kosten
- SIEM Alternative: Ablösung SIEM durch eine moderne SOC Plattform mit «Detection Engineering als Service»
- Threat Hunting: Schnelle, optimierte Suche von Threats/IOCs über die gesamte Umgebung, egal ob in der Cloud oder on-premise

Security Analytics mit Hunters Plattform

- Kostentransparenz: keine Limiten für Log Ingestion und somit keine Einschränkungen bei der Anbindung von Logs
- Up-to-Date Detection: 75-95% des Detection Engineerings wird durch Hunters in einer hohen Qualität sichergestellt
- Tiefe False-Positive Rates: Detectors werden kontinuierlich weiterentwickelt, getestet und optimiert
- Hoher Automatisierungsgrad: für Alert Korrelierung, Triage, Enrichment und Investigation

Individualisierbar

- Umfangreiche Integrationen out-of-the-box
- Custom Log Sources
- Threat Intelligence-Feeds Integration via STIX/TAXII
- Custom Use Cases und individuelles Scoring von Assets

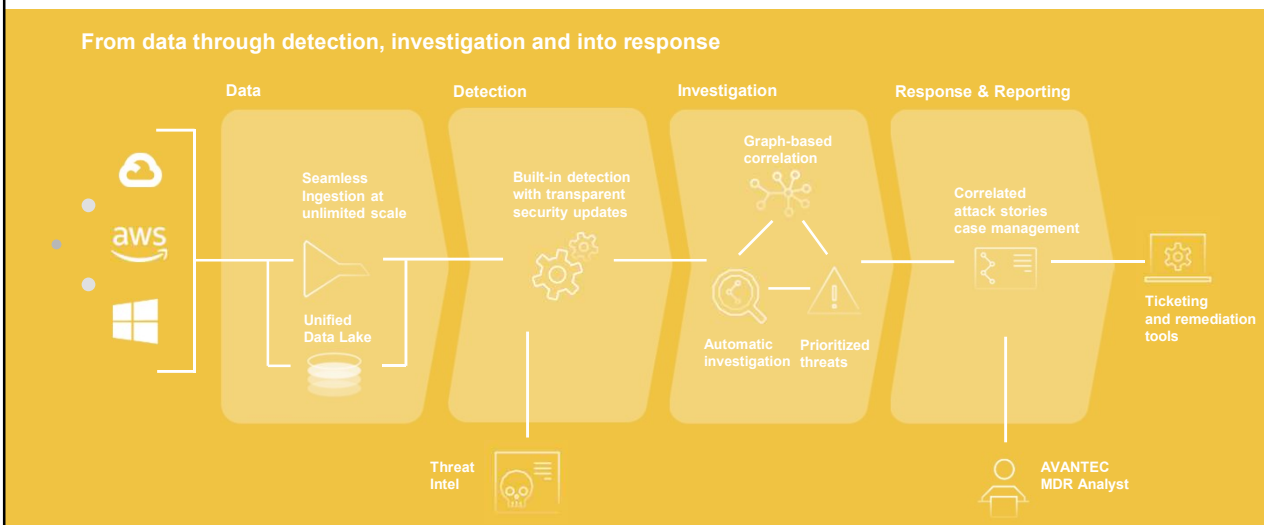
Microsoft · zscaler · aws · Office 365 · CROWDSTRIKE · STIX TAXII · Azure · paloalto · Cisco Umbrella

AVANTEC
Competence. Security. Trust.

Alternativen zu einem SIEM Webinar
09. & 15. November 2023

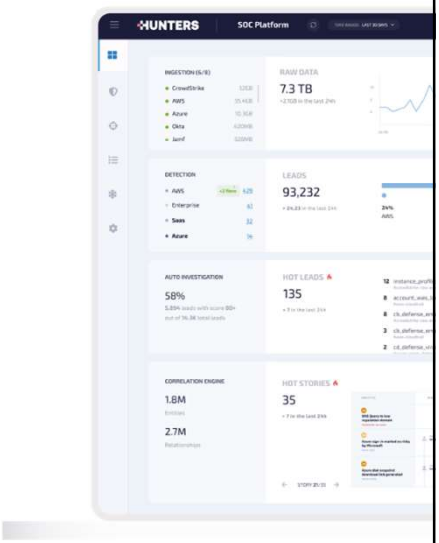
HUNTERS SOC Platform

AVANTEC
Competence. Security. Trust.



AVANTEC
Competence. Security. Trust.

HUNTERS SOC PLATFORM Demo



AVANTEC
Competence. Security. Trust.

Alternativen zu einem SIEM Webinar
09. & 15. November 2023

Threat Intelligence by Recorded Future

AVANTEC
Competence. Security. Trust.

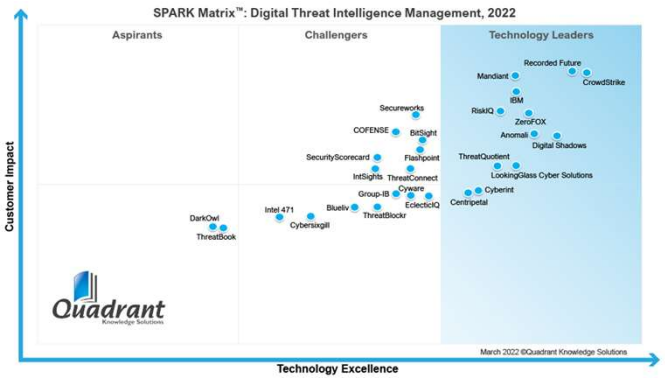
- Wer oder was ist Recorded Future
  - Führender Threat Intelligence Lieferant für hochqualitative Threat Intelligence
  - Geniesst das Vertrauen von 1700+ Kunden weltweit.
    - 6 der 10 grössten Firmen der Welt
    - 40+ der Forbes Global 100
    - 46 Regierungen
  - 9 verschiedene Module um verschiedene Aspekte von Threat Intelligence abzudecken
  - Über 1000 Mitarbeiter, darunter sehr viele Analysten
  - Der “Intelligence Graph” ist das grösste Repository für Intelligence

Marktübersicht

AVANTEC
Competence. Security. Trust.

Forrester Wave Q3 2023

Spark Matrix 2022



AVANTEC
Competence. Security. Trust.

Alternativen zu einem SIEM Webinar
09. & 15. November 2023

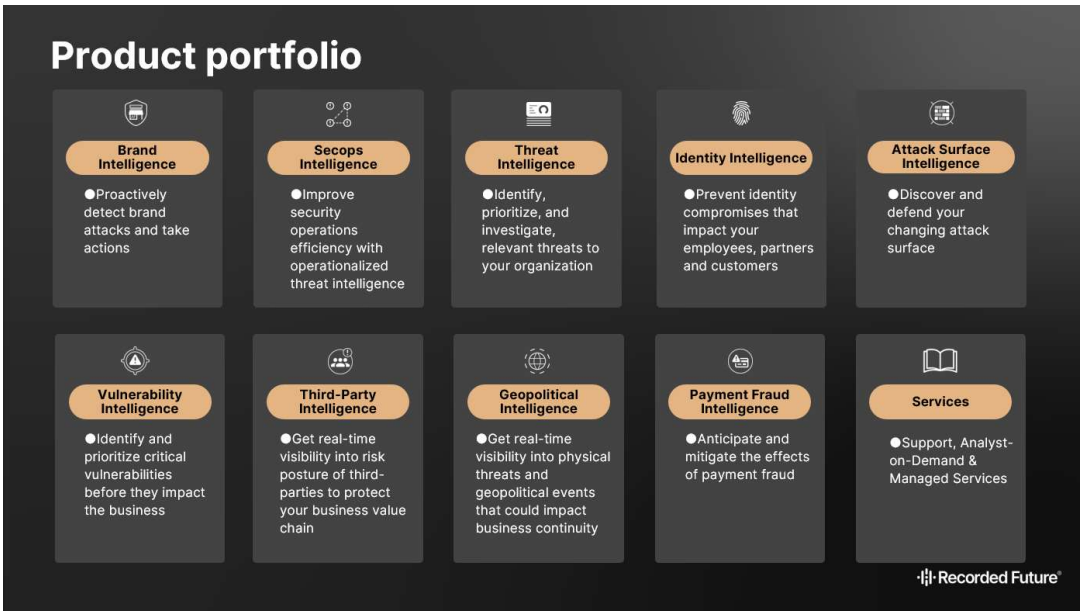
Threat Intelligence by Recorded Future

AVANTEC
Competence. Security. Trust.

- Woher kommen die Daten?
  - Offene Daten
    - Globale und lokale News
    - Paste Sites & Code Repositories
    - Social Media, Forums, Blogs, Messaging Plattforms
    - Company, Financial & Research Reports
  - Technische Daten
    - Threat Feeds, IOC Lists, Vulnerabilities
    - Malicious Traffic Analysis
    - Internet facing assets
    - Malware Sandbox / Honeypots
  - Dark Web
    - Marketplaces
    - Closed & Special access Underground Forums
    - Ransomware Extortion Sites
    - Data Breaches, Card Data, Credential Lists

Recorded Future Modules

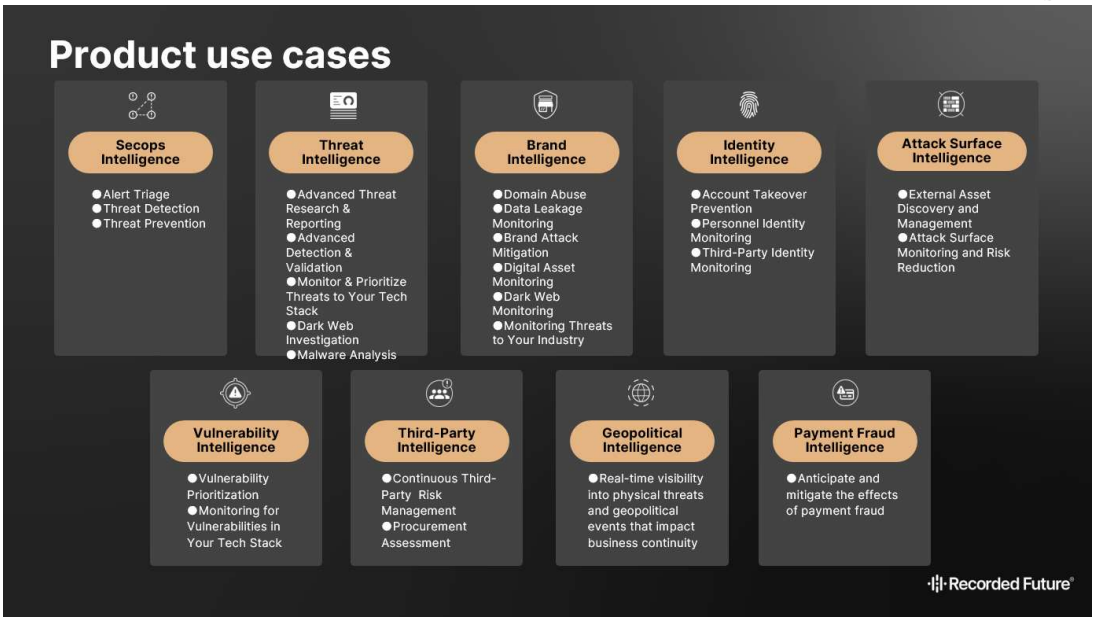
AVANTEC
Competence. Security. Trust.



AVANTEC
Competence. Security. Trust.

Alternativen zu einem SIEM Webinar
09. & 15. November 2023

Recorded Future Use Cases



Threat Intelligence Module

- Identify, investigate, and prioritize relevant threats to your organization
  - Outcomes
    - Faster, more confident identification and prioritization of threats
    - Complete investigations and proactively take action to reduce downtime, reputational damage and costs
    - Reductions of operational risk
  - Key Features
    - Conduct deep investigations of threats with full access to world's largest intelligence repository
    - Utilize data visualizations to gain more context and identify thrends from your threat landscape
    - Use pre-built threat hunting packages, sandbox results and more to protect your organizations assets

AVANTEC
Competence. Security. Trust.

Alternativen zu einem SIEM Webinar
09. & 15. November 2023

Vulnerability Intelligence Module

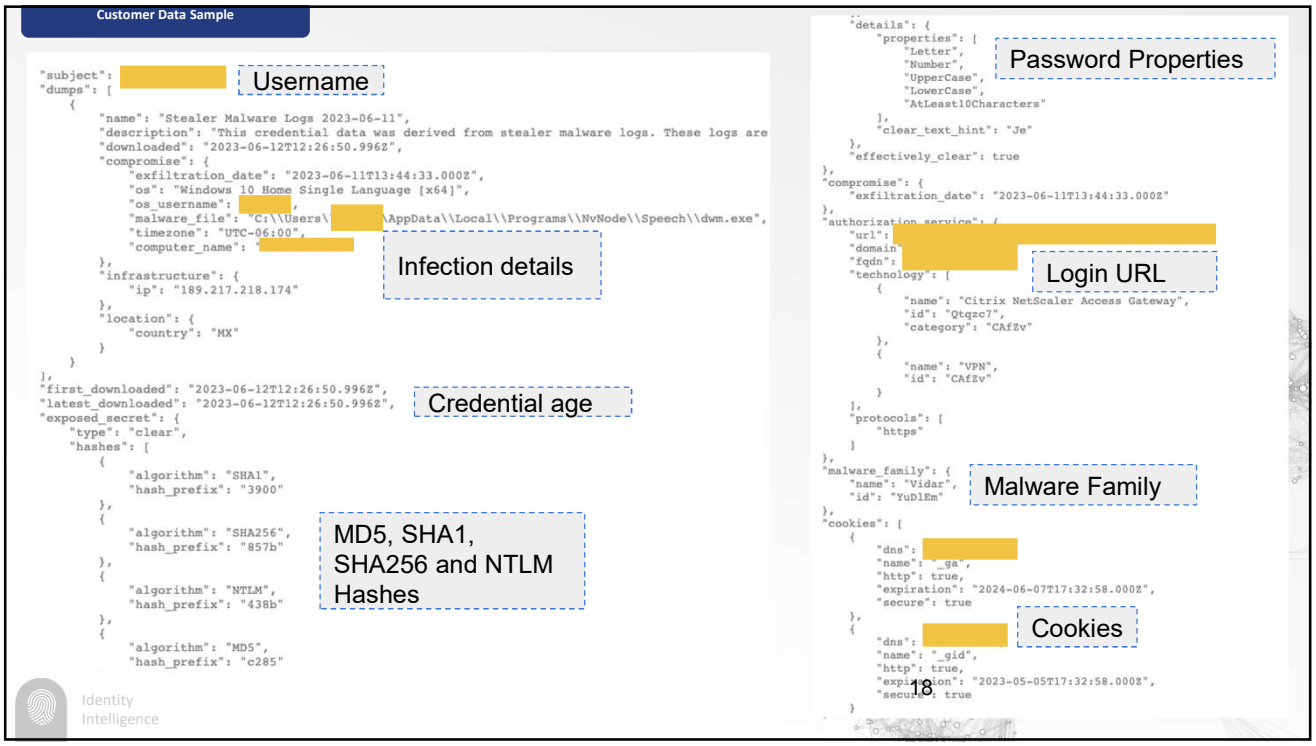
- Identify and prioritize critical vulnerabilities before they impact the business
  - Outcomes
    - Reduce operational risk
    - Prioritize vulnerabilities based on exploitation
    - Identify newly disclosed CVEs
  - Key Features
    - Real-time vulnerability risk scoring
    - Detailed research and analysis
    - Integrations and browser extension for CVE enrichment

Identity Intelligence Module

- Prevent identity compromises that impact your employees, partners or customers
  - Outcomes
    - Reduce operational and financial risk
    - Secure your attack surface, including the identities of employees and customers
    - Automated risk checks during critical events
  - Key Features
    - Visibility across hacker, criminal, and invitation-only dark web sites
    - Automated lookups and remediation of exposed credentials with detailed context
    - Integrations with leading IAM and SOAR solutions
  - 15+ Billion leaked credentials collected

AVANTEC
Competence. Security. Trust.

Alternativen zu einem SIEM Webinar
09. & 15. November 2023



AVANTEC
Competence. Security. Trust.

Alternativen zu einem SIEM Webinar
09. & 15. November 2023

AVANTEC
Competence. Security. Trust.

Threat Intelligence by Recorded Future Demo

AVANTEC
Competence. Security. Trust.