Cyber Threat Exchange Liechtenstein
26. September 2023

AVANTEC
Competence. Security. Trust.

Update Security Services

Christian Grob
Head of Security Services
grob@avantec.ch

Herausforderungen

AVANTEC
Competence. Security. Trust.

- Professionellere Cyber Angriffe
- Steigende Komplexität
- Fehlendes Knowhow
- Mangelnde Awareness
- Diskrepanz Risiken & Sicherheitsbudgets
- Fehlende Ressourcen

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Security Services Bereiche

AVANTEC
Competence. Security. Trust.

Cyber Defense

24/7 Managed Detection & Response Service durch AVANTEC Analysten & Responder - aus der Schweiz

Bereitstellung relevanter und qualitativ hochwertiger Threat Intelligence

Update

Technology Management

Professioneller Betrieb der AVANTEC Lösungen durch zertifizierte Experten - 24/7 Emergency Support

Übernahme Change Mgmt Incident Mgmt, Monitoring, Maintenance

Security Assurance

Überprüfung des Designs und Effektivität der Sicherheitsmassnahmen

Ausrichtung der Massnahmen auf die Exponierung und aktuelle Bedrohungslage

High Level Service Overview

AVANTEC
Competence. Security. Trust.

Cyber Defense Services

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

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

CROWDSTRIKE
Recorded Future

Threat Intelligence

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

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

tenable

Vulnerablity Scanning

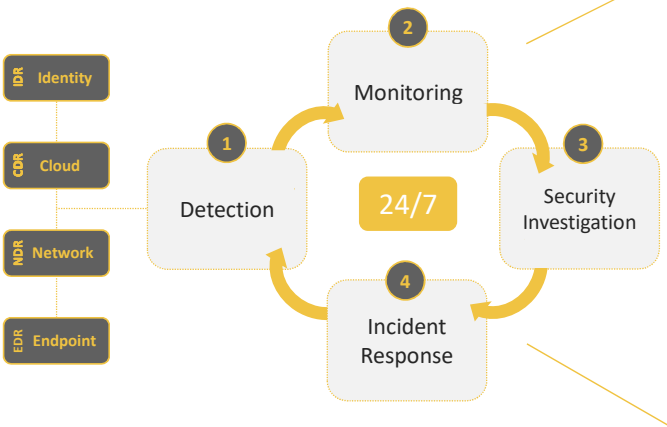
- Identifikation von Schwachstellen mit regelmässigen Scans von extern oder intern
- Verwaltung der Scan Policies
- Regelmässiges Reporting mit Empfehlungen
- Verwalten der False-Positives

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

MDR Service Übersicht

AVANTEC
Competence. Security. Trust.



Detection
Erkennung von abnormalem und maliziösem Verhalten mit State-of-the Art **Threat Detection Technologie**
Automatisierte Eröffnung eines Cases bei AVANTEC

Monitoring
Erstanalyse der generierten Security Events durch MDR Analysten und ggf. **Triage für weitere Investigation**
Automatisierte Response möglich

Security Investigation
Durchführung **tiefergehende Analyse** unter Einbezug von weiterem Kontext (Asset Information, Threat Intelligence, System Artefakten etc.)
Information an MDR Kunde bei Security Incident
Eskalation Incident Response Team (AVANTEC / Kunde)

Incident Response
Massnahmen werden in enger Zusammenarbeit mit dem Kunden gemäss definiertem **Szenario (Playbook)** ausgeführt sowie die **Recovery** begleitet
Abschluss Incident Report & lessons learned

AVANTEC CDC / MDR Module

AVANTEC
Competence. Security. Trust.

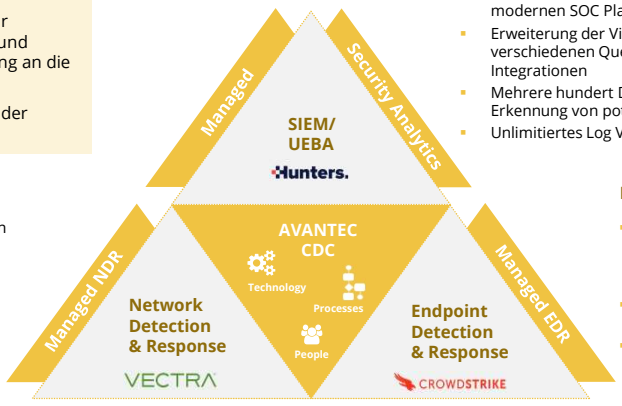
Modularer Aufbau der Services ermöglicht individuelle Zusammenstellung

Schrittweiser Ausbau zur Steigerung der Maturität und kontinuierlichen Anpassung an die Bedrohungslandschaft

Technologie wird als Teil der Services **bereitgestellt**

Managed NDR

- Überwachung des gesamten Netzwerkverkehrs mit der innovativen Technologie von Vectra
- Kombination verschiedener Analyse-Verfahren (u.a. Machine Learning/AI)
- Ohne Agent auf den Endpoints



Managed Security Analytics

- Korrelation und Analyse von sicherheitsrelevanten Daten auf Basis der modernen SOC Plattform von Hunters
- Erweiterung der Visibilität mit Daten aus verschiedenen Quellen – Umfangreiche Integrationen
- Mehrere hundert Detectors für zuverlässige Erkennung von potenziellen Cyber-Angriffen
- Unlimitiertes Log Volumen

Managed EDR

- Überwachung der Client und Server mittels Endpoint Sensor & cloud-basierter Management Technologie von CrowdStrike
- Next GEN AV, EDR und Threat Hunting inklusive
- Umfangreiche Handlungsoptionen und direkter Eingriff auf Endpoints bei Alerts

Source: Gartner, Applying Network-Centric Approaches for Threat Detection and Response
ID G0037346

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Managed Security Analytics mit Hunters

AVANTEC
Competence. Security. Trust.

Neuer Ansatz

Viele Kunde suchen Alternativen vom klassischen SIEM hin zu einer moderneren, stärker automatisierten und besser skalierbaren Lösung

- Steigende/zu hohe Kosten für die Log Ingestion
- False-Positives führen zur sogenannten «Alert Fatigue»
- Zeitaufwendiges Detection/Use Case Engineering, in vielen Fällen ohne die gewünschte Qualität zu erreichen

Top drei Use Cases

- XDR | Security Analytics: Vendor unabhängiges XDR mit umfangreichen Integrationen
- Ersatz SIEM: Ablösung SIEM durch eine moderne SOC Plattform mit «Detection Engineering als Service»
- Threat Hunting: Schnelle und optimierte Suche von Threats und IOCs über ihre gesamte Umgebung, egal ob in der Cloud oder on-premise aus einer zentralen Platform

Unterschied mit Hunters Plattform

- Keine Limiten für Log Ingestion und somit keine Einschränkungen bei der Anbindung von Log Sourcen
- 75-95% des Detection Engineerings wird durch Hunters in einer hohen Qualität sichergestellt, kontinuierlich weiterentwickelt und getestet
- Tiefe False-Positive Rates u.a. durch AI, ML und automatisierte Korrelation
- Hoher Automatisierungsgrad für Alert Korrelierung und Investigation

Umfangreiche Integrationen

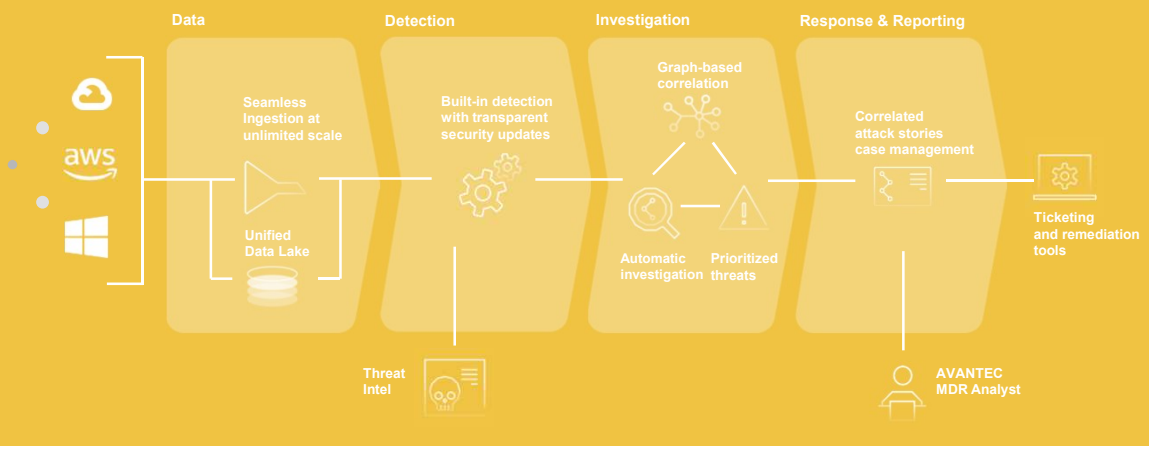
- Umfangreiche Integrationen out-of-the-box
- Custom Log Sources & Use Cases möglich

Microsoft · zscaler · aws · Office 365 · CROWDSTRIKE · Google Workspace · Azure · paloalto · Cisco Umbrella

MDR mit HUNTERS

AVANTEC
Competence. Security. Trust.

From data through detection, investigation and into response



AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Mehrwert unserer Cyber Defense Services

AVANTEC
Competence. Security. Trust.

Service Inbetriebnahme
- Erfahrenes Team leitet durch das Onboarding
- Vorkonfiguration der eingesetzten Technologie nach Best Practices
- Rollout in kürzester Zeit

Security Monitoring
- Analyse & Triage der Security Events gemäss definierten SLA
- Tiefergehende Security Investigation - rund um die Uhr 24/7

Incident Response
- Standard Playbooks werden auf Kunden angepasst
- Sofortige Einleitung von Eindämmungsmassnahmen gemäss Playbooks (z.B. Isolation von Endpoints)

Modernste Technologie
- State-of-the-Art Threat Detection der führenden Anbieter inklusive
- Module optimal aufeinander abgestimmt, integriert & konfiguriert

Kostentransparenz
- Hohe Kostentransparenz & Planbarkeit durch pauschale Preise – Endpoint basiert
- Attraktive Preise durch MSSP Skalierungseffekt

Zertifizierte Experten
- Zugriff auf zertifizierte Experten (u.a. GIAC Certified Forensic Analyst (GCFA), GIAC Continuous Monitoring (GMON)
- 24/7 Tel. Erreichbarkeit

AVANTEC
Competence. Security. Trust.

Backup Slides

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

AVANTEC
Competence. Security. Trust.

Sind Ihre Daten im Dark Web?

Als MSS Kunde profitieren Sie von Vorteilspreisen auf unseren Dark Web Monitoring Service

Kontinuierliche Überwachung des Dark Web auf Data Leaks, Account Leaks sowie auffällige Erwähnungen in Dark Web Foren

- Kontinuierliche Suche nach kompromittierten Accounts mit Bezug zum Kunden
- Kontinuierliche Suche nach gestohlenen Daten z.B. von Ransomware Gruppen
- Monitoring von Domains mit Bezug zum Kunden (Hinweis Phishing Kampagne)
- Überwachung von Paste Sites, Onion Sites, Git etc.
- Spezifisches Monitoring von Kredit Karten
- Überwachung Ransomware Data Leak Sites (auch von Herstellern/Vendoren/Partnerfirmen)
- Alarmierung bei kritischen Feststellungen

Dark Web – High Level View [Firma XY]

AVANTEC
Competence. Security. Trust.

Search Filter; Company Name XY, Domain www.cxz.ch

xx.xx.2023

Accounts 297	Leaks 96
Botnet Logs 2	Ransomware Extortion 0
Paste Sites 8	Forum Discussions 5

CTRL +C

Sample

AVANTEC
Competence. Security. Trust.