Managed Security Service SIEM

Angriffe entwickeln sich stetig weiter

Nicht nur IT-Tools zum Verhindern und Erkennen von Angriffen entwickeln sich kontinuierlich weiter auch die Angriffe selbst werden immer ausgeklügelter.
Oft reicht schon eine Phishing-Mail an einen unaufmerksamen Mitarbeiter für den Angreifer aus, um Zugriff auf Infrastruktur zu erhalten und so im Unternehmen hohen Schaden anzurichten, insbesondere Kritische Infrastrukturen wie Energieversorger oder Unternehmen im Gesundheitswesen haben eine erweiterte Pflicht ihre Kundendaten und Infrastruktur vor Angriffen zu schützen.
Aus diesem Grund sind Firewall und Malwareschutz nur noch ein Teil einer funktionieren IT-Sicherheitsstrategie. **Um volles Potential und kompletten Schutz zu gewährleisten sind daher drei Bestandteile maßgeblich.**

1. **PROTECT**
Absicherung durch Prozessuale und Funktionale Safeguards, wie Firewalls, IPS/IDS und Whitelisting von Anwendungen.

2. **DETECT**
Kontinuierlicher Schutz Ihrer Umgebung mit verhaltensbasierten Regeln. SIEM as a Service überwacht hier Ihr Netzwerk und Protokollierungsdateien anderer Anwendungen um schon im Ansatz verdächtige Aktivität festzustellen.

3. **RESPOND**
Unser Team aus SOC-Spezialisten analysieren den Sicherheitsvorfall so das schnell eine Behebung möglicher Schwachstellen erfolgen kann. Potentielle Bedrohungen werden durch eine rund um die Uhr überwachung schnellst möglich erkannt, automatisierung, Technologie unserer Plattform und entsprechende Expertise hilft uns potentielle Bedrohungen zu Klassifizieren, so das Sie sich auf das wesentliche Konzentrieren können.

Der zentrale Blick auf Ihre Infrastruktur

Für einen vollumfänglichen Überblick des Zustands Ihrer IT integrieren wir diese in unserer Security-Plattform, dabei sind kaum Grenzen gesetzt. Durch Unterstützung der eingesetztzen Tools unserer Partner integrieren wir Logquellen out of the box von hunderten Produkten und Protokollierungstypen, somit sind Integrationen der beispielhaft genannten Systeme kein Problem:

- Betriebssysteme
- EDR und NGAV
- Router und Switche
- Firewalls, IDS, IPS undNGFW
- Webserver und Datenbanken

Alleinstellungsmerkmal

Unsere Alleinstellungsmerkmal ist unser **Hybrider Ansatz auch ihre Cloud Dienste wie**

- Office 365
- Microsoft Azure AD
- SaaS Dienste
- Identity + Access Management Services

an unsere Managed SIEM anzubinden.

Darüber hinaus sind wir nicht auf unsere eigenen Security Lösungen beschränkt, sondern können Ihre schon vorhandenen Security Lösungen gleich mit integrieren und daraus abgeleitete Sicherheitsvorfälle durch unsere Experten auswerten lassen.
Bei Bedarf integrieren wir auch **Ihre KRITIS Komponenten aus der Operatianal Technologie (OT)** durch spezielle Logadapter.

Abgerundet wird dies um die Nutzung von zentralen Cybersecurity Frameworks wie dem MITRE ATT&CK, um Ihnen und unseren SOC Analysten direkte Informationen aus der Security Community zur Verfügung zu stellen und so verwendete Taktiken und Techniken der Angreifer verfügbar zu machen.

Individueller Service und Preisstrategie

Kein Unternehmen hat die gleichen Anforderungen, ganz nach diesem Motto gestalten wir unseren Service für Sie und finden das passende Modell, incl. einem übersichtlichen und transparenten Pricing.
Grundsätzlich unterscheiden wir bei unserem Managed Security Service zwischen den **Betriebsarten** WIE das SIEM betrieben wird und in **welchem Modell sie einen Service wünschen.**

Hierbei kann aus den folgenden drei Varianten für den Betrieb gewählt werden:

ON PREMISE

- Die Installation und Bereitstellung erfolgt in ihrem eigenen Rechenzentrum auf Hardware von Ihnen
- Logdaten verlassen Ihr Haus nicht, Computing On-Premise
- Optional subskribieren Sie auch die entsprechenden Lizenzen des von uns genutzen SIEM Herstellers

evoila ECP

- Die evoila betreibt einen für SIEM zugeschnitten Elasticsearch Stack in der evoila Cloud Plattform
- Skalierbarkeit nach ihren Bedürfnissen
- Transparente Kosten durch zentrales Reporting
- Übertragung Ihrer Logdaten über gesicherten Kanal (VPN)

Elestic Cloud

- Elasticsearch stellt einen skalierbaren Elastic SIEM Stack zur Verfügung
- Betrieb in Amazon AWS oder Google Cloud (AZ Frankfurt möglich)
- Transparente Kosten per GB/Tag Logvolumen
- Übertragung per HTTPS gesichertem Kanal (cloud.id)

Je nach Bedarf bieten wir unseren Managed Service, mit einem entsprechende Service Level Agreements (SLA), in wahlweise zwei Varianten an:

- 24 x 7
- 8 x 5 + Rufbereitschaf als Option

Hierbei können Sie wiederum aus den Varianten:

1. Nur Betrieb

Ihr SIEM steht in ihrem Rechenzentrum On-Premise, wir übernehmen für Sie den Betrieb (Verfügbarkeit, Updates, Patch- und Changemanagement) Die Loganalyse / Alerting liegt in Ihren Händen durch Ihr Team.

2. Security Analytics

Sie Betreiben den SIEM Stack selbst. Wir übernehmen die Log und Eventanalyse durch unsere Erfahrenen SIEM Analysten und das Incident Management nach abgestimmten Vorgaben mit Ihnen.

3. Full Managed

Dies ist die Kombination aus den ersten beiden Varianten: Wir betreiben den SIEM Stack für Sie und übernehmen die Log- und Eventanalyse sowie das Incident Management. Kein eigener Personaleinsatz – voller SOC / SIEM Service für Sie.

Ein **wöchentliches Reporting** zum Security Zustand ihrer IT-Umgebung incl. Aussagen über die Anzahl der Incidents nach Priorität und den ergriffenen Maßnahmen runden unseren Service ab.

Warum ein SIEM als Managed Service?

PERSONELLE VERSTÄRKUNG DER IT-SECURITY

Viele Unternehmen haben Schwierigkeiten Fachkräfte im Bereich der IT-Sicherheit zu finden und zu halten. Genau dort knüpft der Evoila Managed-Service an, wir kümmern uns um ausreichend SOC-Analysten um Ihr SIEM zu erfolgreich zu betreiben.

SPEZIALISIERTES FACHWISSEN

Grade spezialisierte Fachkräfte wie Incident Responder und Cloud Security Architekten oder Personal mit Expertise im Umgang mit kritischen Infrastrukturen sind oft ein Mangel im Security Team. Die Evoila betreut unter anderem auch Kunden im KRITIS Bereich sowie in vielen weiteren Geschäftsbereichen, somit können wir Ihnen diese Expertise „as a Service“ anbieten.

NIEDRIGERE OWNERSHIP-KOSTEN

Der Betrieb eines SIEM und das Etablieren eines SOC-Teams im Unternehmen kann oftmals kostspielig werden. Diese Resourcen müssen sie nicht selbst vorhalten, zusätzlich profitieren Sie durch die Erfahrungen und Probleme, die unsere Analysten bei anderen Projekten haben. Dadurch werden hohe Anschaffungskosten (CapEx) und Betriebskosten (OpEx) für ein eigenes SIEM und SOC-Team stark reduziert.

AUSGEFEILTES SIEM / SOC

Durch den Evoila Managed Security Service erhalten Sie Zugriff auf ein Ausgereiftes SIEM was stetig verbessert wird. Denn wird bei anderen Kunden ein Vorfall erkannt, profitieren alle weiteren von diesem Informationsfluss gleich mit. Zudem integrieren wir verschiedene Threat Intelligence Feeds zur Anreicherung Ihrer Logdaten um extern verfügbare Informationen.

CUTTING-EDGE SECURITY

Produkte und Lösungen werden rasch weiterentwickelt, mithalten mit neuen Updates und immer auf dem neusten Stand sein benötigt viel Manpower und ein großes Budget was bekanntermaßen häufig eher knapp in der IT-Security ausfällt ist. Uns als Managed Service Provider ist es essentiell unseren Kunden neuste Technologien und Produkte anzubieten.

Zertifizierungen

Datenverarbeitung

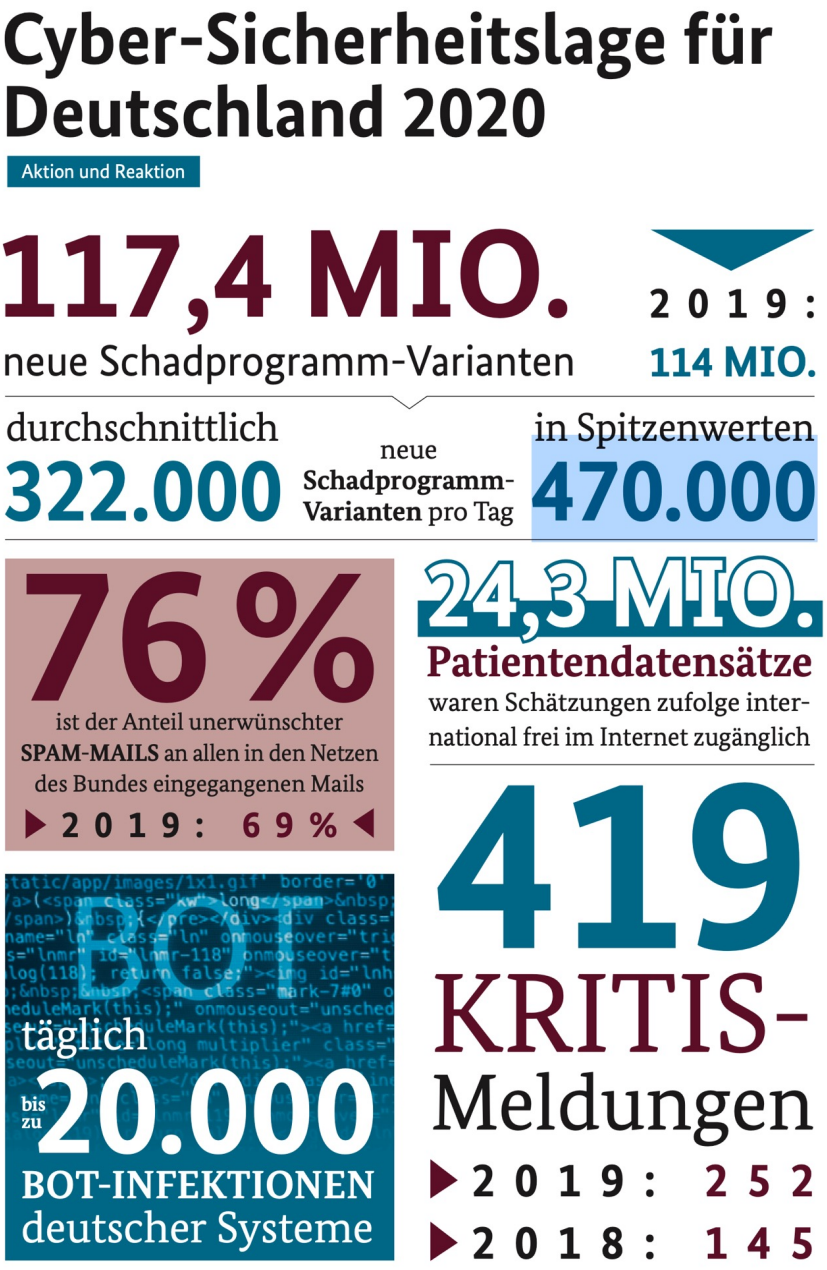
Besonders stolz sind wir darauf unserern Kunden eine

- ISO 27001 und
- BSI C5

zertifizierte Plattform zur Verarbeitung der Daten anbieten zu können. Neben unserer zentralen Plattform, der s.g. Evoila Cloud Plattform, ist unsere ISO27001 auch unternehmensweit für alle angeschlossenen Standort der evoila Group gültig.

Mitarbeiter

Die Schulung und Zertifizierung ist unser Hauptaugenmerk im Bereich Managed Service Security. Nur gut ausgebildete und erfahrene Mitarbeiter, wissen aktuelle Bedrohung korrekt einzuschätzen und die entsprechende Folgeschritte einzuleiten. Snsere Mitarbeiter halten unterschiedlichste Produktbezogener, als auch Herstellerneutrale Zertifizierungen.
Zudem ermöglichen wir unseren Mitarbeitern regelmäßig an Red und Blue Team Challenges teilzunehmen, um neue Impulse aus der Security Community mit in die tägliche Arbeit integrieren zu können.



Sprechen Sie uns an – jederzeit!