Security Operations Center

Ihre wirksame Verteidigungslinie gegen Cyberangriffe

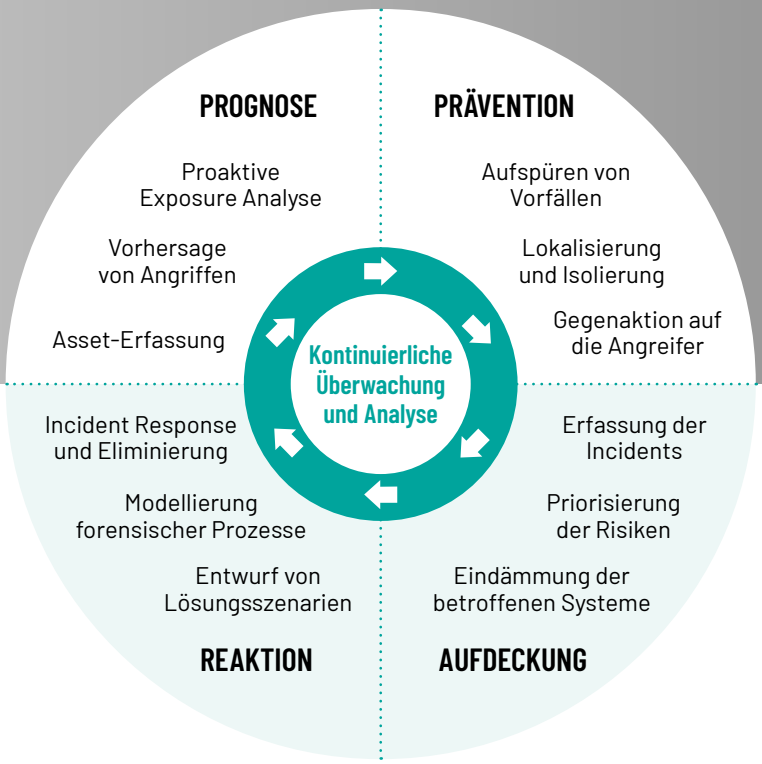
GRAVITATE

WÜRTHPHOENIX

Auf Ihre individuellen Bedürfnisse zugeschnittene Cybersecurity

Während Unternehmen lernen, sich besser zu schützen, entwickeln Angreifer immer ausgefeiltere Techniken, um Ihre Sicherheitsbarrieren zu durchbrechen. Eine stetig wachsende Anzahl von Bedrohungsakteuren suchen aktiv und gezielt nach unentdeckten Sicherheitslücken. In diesem Umfeld richten viele Unternehmen ein Security Operations Center (SOC) ein, um Sicherheitsprobleme aktiv zu bekämpfen und bereits im Vorfeld zu verhindern.

Das Gravitate-Würth Phoenix SOC ist Ihr zentrales Kontrollsystem für die kontinuierliche Bedrohungsüberwachung und -analyse sowie für die Prävention von Cybersicherheitsvorfällen. Unser Team von spezialisierten Experten ist in der Lage, Bedrohungen vorherzusehen, zu erkennen und effektiv darauf zu reagieren.



Traditionelles SOC – zu langsam, zu spät, selbst wenn es richtig gemacht wird?

- Herkömmliche SOCs erzeugen riesige Datenmengen. Laut jüngsten Studien von Gartner sind aber bis zu 95 % der Alarme Fehlalarme. Ernstzunehmende Risiken gehen dabei oft verloren. Das macht den ohnehin schon überforderten IT-Mitarbeitern noch mehr zu schaffen.

Das Gravitate-Würth Phoenix SOC bietet unumstrittene Vorteile:

- Kontinuierliche Netzwerküberwachung und Transparenz
- Ihre IT-Infrastruktur wird vor Ort und in der Cloud laufend auf Bedrohungen überwacht
- Im Falle einer Malware-Infektion wird die Verbreitungszeit auf ein Minimum reduziert
- KI-gesteuerte Sicherheitsautomatisierungen helfen, Angriffe schnell und präzise zu identifizieren und darauf zu reagieren

Vorbeugen, Erkennen und Reagieren

Ob ganz auf Ihre individuellen Bedürfnisse zugeschnitten oder als mandantenfähiges Managed Service bereitgestellt, unser SOC wird Sie mit den Technologien und Ressourcen ausstatten, die Sie benötigen.

Unser Angebot beinhaltet:

- Erkennung von und Reaktion auf Bedrohungen
- Erfassung aller Assets
- Laufende Analyse und Schwachstellenbewertung
- Warnungseinstufung und -verwaltung
- Verwaltung von Schwachstellen in Infrastruktur und Anwendungen
- Sicheres Konfigurationsmanagement
- Digitales Identitäts- und Zugriffsmanagement
- Risikomanagement für Kunden / Drittanbieter
- Anwendungssicherheit durch einen zentralisierten Ansatz für Bedrohungserkennung und -reaktion
- Netzwerkmanagement und -sicherheit
- Cyber-Forensik
- Cyber-Resilienz

SOC-Eigenbetrieb versus Gravitate-Würth Phoenix Managed SOC

	SOC-EIGENBETRIEB	GRAVITATE MANAGED SOC
Keine Notwendigkeit für eine große IT-Infrastruktur	✗	✓
Keine Notwendigkeit für mehrere Lizenzen, Verträge, AMC, Support	✗	✓
Keine Notwendigkeit, Experten für Cybersicherheit einzustellen	✗	✓
Keine Notwendigkeit für Investitionsausgaben	✗	✓
Keine Notwendigkeit, Management-Bandbreite für IT-Sicherheit aufzuwenden	✗	✓
Keine Probleme mit Personalwechsel und Kündigungen	✗	✓
Keine Probleme mit Upgrades (je nach hinzugefügtem Gerät)	✗	✓
Keine Probleme mit Fusionen und Übernahmen	✗	✓
Von "Betrieb" zu "Sicherheit" übergehen	✗	✓

Unser SOC-Team arbeitet rund um die Uhr an 365 Tagen im Jahr und wird von einer Mannschaft von Cyberexperten mit umfassender Erfahrung mit vollständig ausgelagerten oder hybriden Dienstleistungsmodellen unterstützt.

Aus einer Hand von einem vertrauenswürdigen Partner

In unserem SOC inbegriffen

- Feste monatliche Gebühr auf Basis der zu überwachenden Services
- Minimale Vorabkosten
- 24/7 Security Ops Team
- Verwaltetes Cloud-basiertes SIEM
- Sicherheits- und Penetrationstests aus der Perspektive echter Angreifer (Red Teaming)
- Echtzeit-Benachrichtigungen und -Warnungen
- Online-Analysen/Berichts-Dashboard
- Integration mit führenden Reaktionstools
- Monatliche Überprüfung und Empfehlungen
- Einhaltung gesetzlicher Vorschriften / Compliance

Ihre Vorteile: Schnellere Erkennung und Reaktion *** Intelligente, automatisierte Systeme in Kombination mit menschlicher Expertise für ein sofortiges Reaktionsmanagement *** Sofort und zu niedrigen TCO-Gesamtbetriebskosten einsetzbar

SOC Features

	TRADITIONELLES SOC	UNSER ANGEBOT
Abdeckung aller Protokolle/Ereignisse	✓	✓
Verwendung von Indikatoren für Kompromisse (IOCs)	✓	✓
Sichtweise des Blue Teams	✓	✓
Verwendet Erkennungsregeln, die auf neuesten SIEM-Technologien basieren	✓	✓
Das Blue Team analysiert die an SIEM übermittelten Protokolle/Ereignisse	✓	✓
Verwendet IoCs auf der Grundlage des verwendeten SIEM-Produkts	✓	✓
Kontinuierliche Bewertung der Schwachstellen	✓	✓
Deckt exakt ab, was die Analyse vorgibt	✗	✓
IoPC (Indicators of Pre Compromise) verfügbar	✗	✓
Sichtweise des Red Teams	✗	✓
Verwendet exklusive Erkennungsregeln (SOC Prime)	✗	✓
Das Blue Team analysiert Informationen, die aktiv von den überwachten Hosts abgerufen werden	✗	✓
Nutzt SATAYO als OSINT / IoC (über 900k, täglich aktualisiert)	✗	✓
Kontinuierliches Vulnerability Assessment mit Business-Korrelation	✗	✓

Oft ist es einfach nicht praktikabel - und auch nicht finanzierbar - rund um die Uhr ein Sicherheitsmanagementteam zu beschäftigen.
Wir bieten eine zuverlässige, sichere, kosteneffiziente Alternative.

Effiziente Sicherheit ohne Kompromisse

Was macht ein SOC effektiv?

Wir orchestrieren die verschiedenen Rollen, Prozesse und Technologien, die für eine effiziente Erkennung, Analyse und Reaktion von Cyberangriffen notwendig sind.

„Level Up Your SOC" - Fokus auf Menschen, Prozesse und Technologie

Unabhängig davon, an welchem Punkt Ihres Sicherheitslebenszyklus Sie sich befinden, ist das Verständnis und das Interesse an Ihren Mitarbeitern, die Entwicklung von Prozessen und die Nutzung von Technologien der Schlüssel zu einem erfolgreichen Security Operations Center.

Damit ein SOC effektiv arbeiten kann, ist es unerlässlich, Prozesse zu definieren und zu dokumentieren, damit die Ausführung gemäß dem dokumentierten Plan gewährleistet werden kann. Für Sie heißt das: Früherkennung und Reaktionsfähigkeit verlaufen weitaus effektiver, strukturierter und rascher. Im Idealfall ermöglicht ein SOC, eine Bedrohung sogar in Echtzeit zu erkennen.

Servicequalität neu definiert

Mitarbeiter	Erhöhte Awareness	SECURITY TRAINING	SOCIAL ENGINEERING	PASSWORD AUDIT
Prozess	Erhöhte Compliance	GAP ANALYSIS		
IT Services	Erhöhte Sicherheit	VULNERABILITY ASSESSMENT	PENETRATION TEST	
Organisation	Incident Detection Response	EXPOSURE ASSESSMENT	RED TEAMING	SOC

Ihre Sicherheit, Ihr Servicemodell, Ihre Wahl

Wählen Sie den Servicelevel, der am besten zu Ihren Geschäftsanforderungen passt - von Standarddiensten, die die Grundlagen der Überwachung sicherstellen, Erkennung, Vorbeugung, Reaktion und Berichterstattung abdecken, bis hin zu bis hin zu erweiterten Servicelevels, welche die Grundlagen kombinieren - mit maßgeschneiderten Services, analytikbasierten Bedrohungsdaten und fortschrittlicher SOC-Automatisierung.

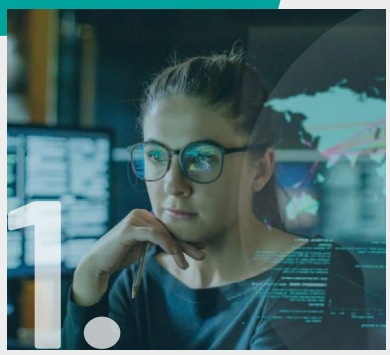
			STANDARD	PROFESSIONAL	ENTERPRISE
Servicelevel			Montag-Freitag 08:30 -12:30 13:30 – 17:30	Montag-Freitag 08:30 -12:30 13:30 – 17:30	0 - 24
Service Requests		IRT	1 Stunde	1 Stunde	1 Stunde
		PT	16 Stunden	16 Stunden	16 Stunden
Security Events	L1: Critical	IRT	30 Min	30 Min	30 Min
		PT	1 Stunde	1 Stunde	1 Stunde
	L2: High	IRT	30 Min	30 Min	30 min
		PT	3 Stunden	3 Stunden	3 Stunden
	L3: Medium	IRT	30 Min	30 Min	30 Min
		PT	8 Stunden	8 Stunden	8 Stunden
	L4: Low	IRT	30 Min	30 Min	30 Min
		PT	16 Stunden	16 Stunden	16 Stunden
Support über Web Tickets			Ja	Ja	Ja
Support telefonisch			Nein	Ja	Ja
Remote Support über TeamViewer			Ja	Ja	Ja
Remote Support über VPN			Nein	Ja	Ja
Support über MS Teams Chat			Nein	Ja	Ja
Exposure Assessment mit SATAYO			Ja	Ja	Ja
SATAYO IoC			Ja	Ja	Ja
(Wiederkehrendes) Vulnerabilty Assessment			Nein	Nein	Ja (max 32 public IPs) – 1 x monatl.
EDR Integration			frei abrufbar	frei abrufbar	frei abrufbar
Network based defense mit ntop Integration			projektbezogen	projektbezogen	projektbezogen
osquery Integration			frei abrufbar	frei abrufbar	frei abrufbar
Icinga Agent Integration			frei abrufbar	frei abrufbar	frei abrufbar
Individuelle Dashboards			Nein	projektbezogen	projektbezogen
Search in Log(s)			Ja	Ja	Ja
Digital Signed Logs – Blockchain			Ja	Ja	YES
Custom Detection Regeln			Nein	projektbezogen	projektbezogen
SOC Prime Regln			Nein	Nein	Ja
SIGMA Regeln			Nein	Ja	Ja
Elastic Regeln			Ja	Ja	Ja

Sicherheit auf höchstem Niveau: Das beste Team und fortschrittliche Technologien

Heutzutage verbringen viele Sicherheitsbeauftragte einen Großteil ihrer Zeit mit Routinearbeiten, die zwar notwendig und wichtig sind, die aber automatisiert werden können. Die Automatisierung dieser manuellen Aufgaben spart teure Arbeitsstunden und die daraus resultierende Arbeitsentlastung gibt mehr Zeit frei, um sich auf die Analyse und Reaktion auf wirklich komplexe Sicherheitsvorfälle zu konzentrieren.

Daten sind ein entscheidendes Element unserer SOC-Erfolgsgeschichte. Wir nutzen sie, um unsere Kunden von den Gejagten zu den Bedrohungsjägern zu machen. Unsere fortschrittlichen Datenanalysefunktionen vereinen SIEM, Netzwerksicherheitsüberwachung, OSINT-Technologien und Endpoint-Überwachung.

Nachgefragt



Wenn Sie sich fragen, wie nützlich ein SOC für Ihr Unternehmen wäre, könnte die Antwort lauten, dass der Wert eines SOCs ***proportional zu dem Schaden*** *ist, den ein erfolgreicher Cybersicherheitsangriff verursachen könnte.*

Wenn Sie aktuell veraltete Sicherheitstechnologien verwenden, kann es je nach Studien von Gartner, IDC oder Forrester im Durchschnitt ***70 bis 150 Tage*** *dauern, bis Ihr Unternehmen eine Sicherheitslücke erkennt.*

Die Minimierung eines Cybersicherheitsrisikos erfordert in jedem Fall eine ***24/7-Überwachung der gesamten IT-Infrastruktur****. Dafür sollte Ihr Unternehmen in der Lage sein, ein Sicherheitsteam in mehreren Schichten zu besetzen und sicherstellen, dass interne Sicherheitsexperten rund um die Uhr verfügbar sind.*

Wir arbeiten partnerschaftlich mit Ihnen zusammen um den SOC-Service ständig zu aktualisieren und optimieren, um Ihre spezifische Bedürfnisse abzudecken und fortschreitenden Bedrohungen entgegenzutreten.

Die Zukunft der Cybersecurity: SIEM und OSINT

Von der umfassenden Überwachung zur punktgenauen Reaktion

SIEM (Security Information and Event Management) und **OSINT** (Open-Source Intelligence) sind zentrale Technologien für den Betrieb eines effektiven Security Operations Centers. Sie sorgen für eine umfassende Überwachung und Analyse von Sicherheitsereignissen und ermöglichen es, Bedrohungen frühzeitig zu erkennen und zu bekämpfen.

Unsere SIEM-Technologie sammelt und verarbeitet Daten aus verschiedenen Quellen, wie Firewalls, IDS/IPS und Netzwerkaktivitäten, um ein klares Bild der Sicherheitslage zu erhalten. Durch automatisierte Analyse-Tools kann das SOC schnell und effektiv auf Bedrohungen reagieren.

Satayo als OSINT hingegen nutzt offene Informationsquellen, wie Soziale Medien, News-Seiten und Datenbanken, um Informationen zu sammeln und zu analysieren, die für die Sicherheit von Bedeutung sind. So kann unser SOC ein umfassendes Bild über mögliche Bedrohungen und Angriffsvektoren erhalten.

„Unser erweitertes SOC-Angebot ermöglicht es Unternehmen jeder Größe, die Vorteile eines hochmodernen Sicherheitsteams in Anspruch zu nehmen. Durch die Verwendung von SIEM und OSINT-Technologien können wir sicherstellen, dass unsere Kunden jederzeit bestmöglich geschützt sind."

Claus Huber, Geschäftsführer Gravitate

Satayo ist unser eigenentwickletes Open-Source Intelligence-Tool (OSINT) und wichtiger Bestandteil moderner Cybersicherheitsstrategien.

Satayo ist eine wichtige Technologie, die für ein effektives Cybersicherheitsmanagement unverzichtbar ist.

Mit den Technologien SIEM und OSINT sind wir in der Lage, Ihnen einen klaren Überblick über die Sicherheit Ihrer IT-Infrastruktur zu geben und Sie gezielt vor Hackerangriffen zu schützen.

Real-Time Überwachung:
SIEM und OSINT bieten eine kontinuierliche Überwachung, die Echtzeitalarme bei Bedrohungen auslöst und eine rasche Reaktion ermöglicht.

Konsolidierte Datenanalyse:
SIEM konsolidiert Daten aus verschiedenen Quellen, einschließlich Netzwerkaktivitäten, Firewall-Protokollen und Anwendungsdaten.

Automatisierte Überwachung:
SIEM und OSINT automatisieren manuelle Überwachungsprozesse, was Zeit und Kosten spart und eine höhere Überwachungseffizienz gewährleistet.

Überwachung von kritischen Infrastrukturen:
OSINT ermöglicht die Überwachung von öffentlich zugänglichen Daten, um Bedrohungen für kritische Infrastrukturen zu erkennen und zu bewerten.

Verhinderung von Cyberangriffen:
SIEM und OSINT bieten eine frühzeitige Erkennung von Bedrohungen und geben Ihrem Unternehmen die Möglichkeit, Ihre Systeme und Netze vor Angriffen zu schützen.

Korrelation von Bedrohungen:
SIEM kann Bedrohungen über verschiedene Dienste hinweg korrelieren, um komplexe Bedrohungen schneller zu identifizieren und zu bewerten.

Security Operations Center

GRAVITATE

Gravitate GmbH
Fürther Straße 27
D-90429 Nürnberg

Tel. + 49 911- 28 7070 78
info@gravitate.eu

www.gravitate.eu

WÜRTHPHOENIX