

Security Operations Center

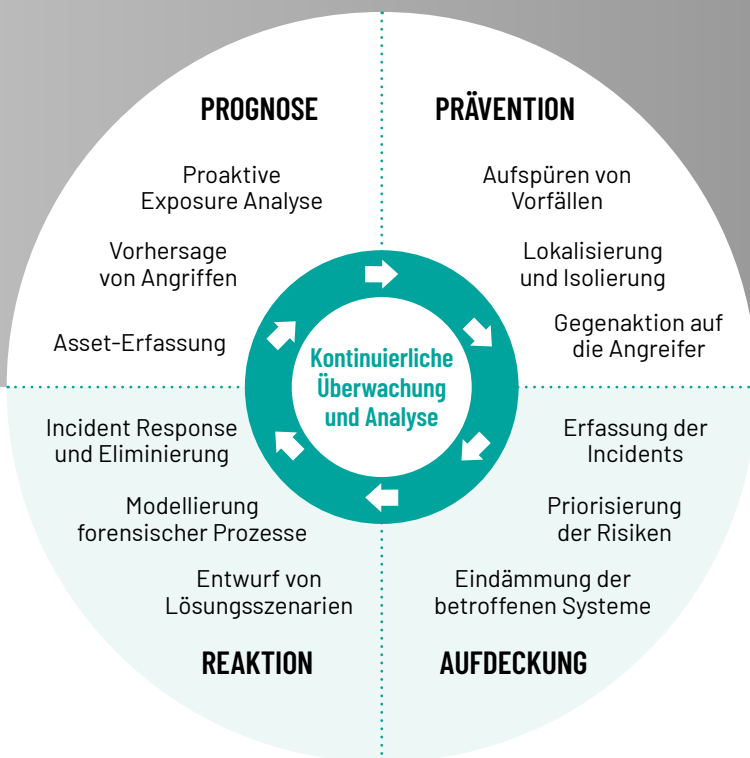
Ihre wirksame Verteidigungslinie
gegen Cyberangriffe



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 SOC's 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

Vorteile des Gravitare-Würth Phoenix SOC

Umfassende Bedrohungsanalyse

Das Gravitare-Würth Phoenix SOC nutzt die eigene SATAYO OSINT & Cyber Threat Intelligence Plattform, um Bedrohungen aus dem Deep und Dark Web in Echtzeit zu überwachen.

Nahtlose Technologie-Integration

Durch die Integration der NetEye-Plattform mit Tools wie SOC Prime und Greenbone Security Manager gewährleistet das SOC eine kontinuierliche und präzise Bedrohungserkennung.

Individuell anpassbar

Kein Standard-SOC – das Gravitare-Würth Phoenix SOC bietet eine flexible Infrastruktur, die genau auf die Bedürfnisse des Unternehmens abgestimmt wird und so maßgeschneiderten Schutz bietet.

Attacker Centric

Im Vergleich zu traditionellen SOC-Ansätzen deckt der Gravitare-Würth Phoenix SOC bereits die erste Phase eines Angriffs ab: die Aufklärungsphase (Reconnaissance). Dies wird durch die Integration der SATAYO® OSINT & Cyber Threat Intelligence Plattform ermöglicht.

Die Technologien im Einsatz

Durch den Einsatz fortschrittlicher Technologien und innovativer Tools gewährleisten wir, dass Ihre IT-Infrastruktur rund um die Uhr geschützt ist.

NetEye SIEM

NetEye SIEM ist eine leistungsfähige Plattform für IT-Monitoring, die die Elastic Stack-Technologie integriert. Sie ermöglicht eine präzise und schnelle Analyse von Log-Daten, um Sicherheitslücken frühzeitig zu identifizieren und zu beheben.

OpenCTI

Nutzen Sie OpenCTI, eine leistungsstarke Plattform, um Cyber Threat Intelligence zu verarbeiten und zu teilen. Durch die Integration mit NetEye SIEM haben Sie Zugriff auf die besten Bedrohungsdaten und können schnell reagieren.

SATAYO

Unsere OSINT- und Cyber Threat Intelligence Plattform, SATAYO, überwacht kontinuierlich Ihre Exposition im Surface, Deep und Dark Web. Durch die direkte Integration in NetEye SIEM erhalten Sie sofort relevante Bedrohungsdaten, die Ihre Sicherheitsstrategie entscheidend stärken.

NetEye Master

Der NetEye Master verarbeitet alle sicherheitsrelevanten Daten und Logs, die von den NetEye Satelliten und SATAYO erfasst werden. Diese Daten werden sicher in der WÜRTH PHOENIX Cloud gespeichert, um die Vertraulichkeit und Integrität Ihrer Informationen zu gewährleisten.

SOC Prime

SOC Prime liefert Ihnen ständig aktualisierte Bedrohungserkennungsregeln. Durch unsere Partnerschaft haben Sie Zugriff auf die besten internationalen Threat Hunters, sodass Ihr Sicherheitsnetz immer auf dem neuesten Stand ist.

NetEye Satellite

Die Satelliten werden direkt in Ihrer Infrastruktur installiert und sammeln sicher alle relevanten Logs und Daten, die anschließend an den NetEye Master weitergeleitet werden.

Greenbone Security Manager

Schützen Sie Ihre Systeme vor bekannten Schwachstellen wie SUPERNova oder BlueKeep. Der Greenbone Security Manager bietet kontinuierliche Schwachstellenbewertung und ist vollständig in NetEye SIEM integriert.

Zugangskontrollen und Datenisolierung

Durch die Verwendung von RBAC (Role Based Access Control) stellen wir sicher, dass nur berechtigte Personen auf sensible Daten zugreifen können. Kunden erhalten einen isolierten Bereich, der ihre Daten schützt und eine transparente Verwaltung ermöglicht.

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?

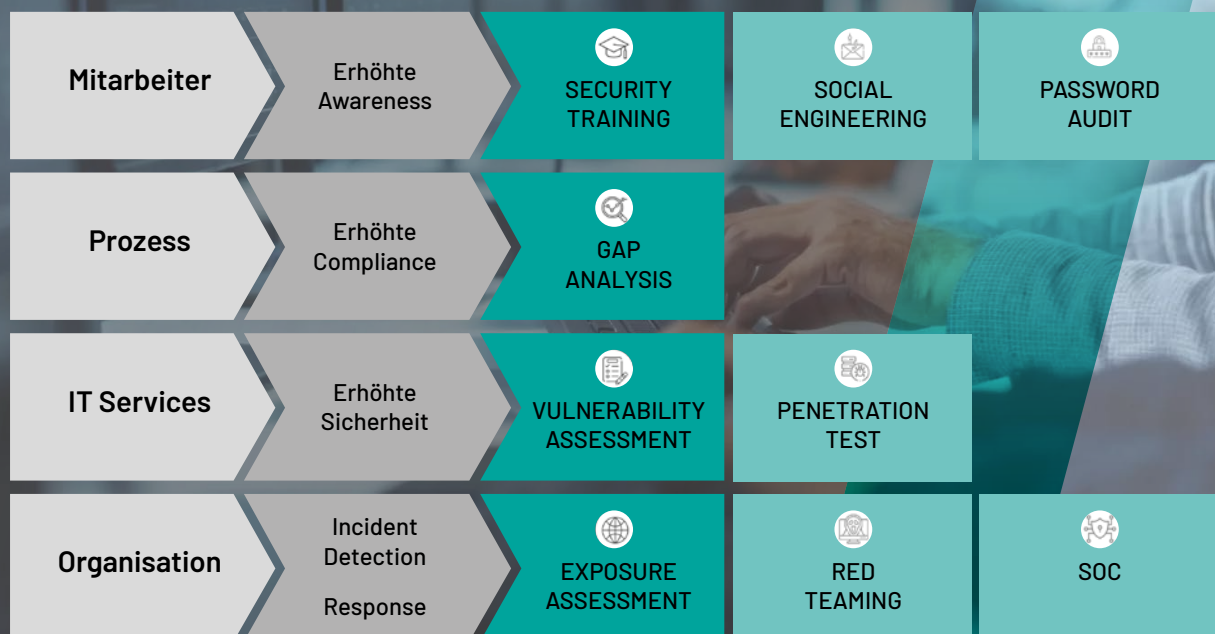
Wir orchestrieren die verschiedenen Rollen, Prozesse und Technologien, die für eine effiziente Erkennung, Analyse und Reaktion von Cyberangriffen notwendig sind.

„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



Ihre Sicherheit, Ihr Servicemodell, Ihre Wahl

Wählen Sie den Servicelevel, der am besten zu Ihren Geschäftsanforderungen passt - von Standard-diensten, 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) Vulnerability 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 SOC **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 Gravitare

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



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



Sicherheitsbedrohungen erkennen, untersuchen und bekämpfen

Im Rahmen unseres Security Operations Centers (SOC) gibt es einen klaren Prozessablauf, um Sicherheitsbedrohungen zu erkennen, zu untersuchen und zu bekämpfen.

1) Erkennung von Bedrohungen:

In dieser Phase suchen unsere Experten aktiv nach Anzeichen für Bedrohungen, um potenzielle Angriffe frühzeitig zu erkennen. Hierbei kommen Technologien wie Security Information and Event Management (SIEM), „Intrusion Detection and Prevention“ und Network Traffic Analysen zum Einsatz, um verdächtige Aktivitäten zu identifizieren.

2) Analyse und Klassifizierung:

Hierbei nutzen wir für die Reconnaissance-Phase das Cyber Kill Chain-Modell von Lockheed Martin, das den Angriffsprozess in mehrere Phasen unterteilt und sich auf die erste Phase des simulierten Angriffs bezieht, in der Angreifer Informationen über ihr Ziel sammeln, um eine erfolgreiche Attacke zu planen. Dies kann beispielsweise die Identifizierung von Schwachstellen in der Sicherheitsinfrastruktur, die Identifikation von Schlüsselpersonen oder -systemen oder die Erfassung von Netzwerktopologien umfassen. Wir arbeiten in dieser Phase mit Satayo als OSINT-Tool.



3) Reaktion:

Sobald die Bedrohung identifiziert und klassifiziert wurde, handelt unser Team um sie zu neutralisieren. Hierbei setzen wir auf den Einsatz von Red-Team-Blue-Team-Übungen, bei denen ein "Red Team" versucht, das System zu hacken, während ein "Blue Team" versucht, die Angriffe zu erkennen und zu stoppen. Unsere Experten sind darauf geschult, die Reconnaissance-Phase und OSINT-Aktivitäten von Angreifern zu erkennen und zu analysieren, um Bedrohungen frühzeitig zu erkennen und zu neutralisieren.

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.



Synergie mit den besten Quellen

Unsere Interaktion mit den wichtigsten internationalen Communities und Organisationen

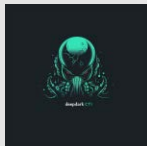
Sie erhalten Zugriff auf hochkarätige Informationen, von denen Sie nie gedacht hätten, dass sie zugänglich wären. Bleiben Sie einen Schritt voraus den Bedrohungsakteuren, um potenzielle Angriffe vorherzusehen.



FIRST ist die führende Organisation und anerkannter weltweiter Vorreiter im Bereich Incident Response. SATAYO wurde von FIRST für die Implementierung des EPSS-Index anerkannt, das die Bewertung der Ausnutzungswahrscheinlichkeit von Schwachstellen ermöglicht.



Curated Intelligence bringt eine private Gemeinschaft internationaler Forscher zusammen, die zusammenarbeiten, um das sich ständig verändernde Cyber-Bedrohungslandschaft zu verstehen. Unser Team ist mit 2 Mitgliedern vertreten.



deepdarkCTI ist ein von unserem Team gegründetes Projekt und wird heute weltweit von mehr als 3.500 Personen verfolgt. Es hat sich zu einem globalen Bezugspunkt für den Austausch von Threat Intelligence-Quellen entwickelt.



Der **Trusted Introducer Service** wurde im Jahr 2000 von der europäischen CERT-Community gegründet, um gemeinsame Bedürfnisse aller Sicherheits- und Incident-Response-Teams anzusprechen. Unser Team ist als akkreditiertes Mitglied vertreten.



Die **DCSO Community** ist ein Netzwerk von Fachleuten und Organisationen, die sich für die Optimierung von Software und die Weiterentwicklung von Lösungen für Rechenzentren engagieren. Diese Community bietet uns Raum für den Austausch von Wissen, Best Practices und Ressourcen im Bereich der Softwareoptimierung und der gemeinsamen Weiterentwicklung neuer Technologien für den Schutz unserer Infrastrukturen.



Unsere Fähigkeit, aufkommende Bedrohungen zu identifizieren, hat es uns ermöglicht, wiederholt den Verkauf des ersten Zugriffs an verschiedene nationale CERTs und Agenturen wie **BSI**, **ACN** und **NCA** zu kommunizieren, was eine schnelle Intervention durch die betroffenen Organisationen zur Folge hatte.



Eine starke Lösung

SATAYO hat sich im Rahmen der Cyber Threat Intelligence-Strategie innerhalb der Würth-Gruppe als unerlässliches Werkzeug etabliert, um eine proaktive Verteidigungsstrategie gegen Cyberangriffe dauerhaft zu unterstützen und auszubauen.

SATAYO bietet leistungsstarke Analysewerkzeuge, um die gesammelten Informationen zu verarbeiten,

Muster zu erkennen, Zusammenhänge aufzudecken und Erkenntnisse zu generieren. Die Erkenntnisse, die das Sicherheitsteam der Würth-Gruppe durch SATAYO gewonnen hat, werden nicht nur innerhalb der Würth-Gruppe genutzt, sondern stehen auch anderen Unternehmen zur Verfügung. Ziel ist es, die Gesamtsicherheit von Unternehmen im gemeinsamen Kampf gegen Cyberkriminalität zu unterstützen.

Die Arbeitsweise des Cyber-Defense-Teams mit SATAYO

Wenn es darum geht, sich anbahnende Bedrohungen oder Cyberattacken zu entdecken, ist es neben dem Einsatz von SATAYO von zentraler Bedeutung, diese laufend hinsichtlich Ihrer Zielabsicht, Ernsthaftigkeit und Relevanz zu bewerten. Deshalb wird innerhalb des Cyber-Defense-Teams der Würth-Gruppe laufend in die Entwicklung systematischer und transparenter Prozesse investiert, um die Erkenntnisse so schnell wie möglich in Abwehrmaßnahmen und Lösungsansätze für alle Würth-Gesellschaften umsetzen zu können. Für jedes erkannte Anzeichen wird dabei eine Priorität festgelegt und ein Ticket erstellt, das eine technische

Analyse und Empfehlungen enthält. Bei Bedarf wird das Ticket direkt mit den betroffenen Teams und Personen im Unternehmen geteilt.

Nach der ursprünglichen Implementierung zur Identifizierung potenzieller Schwachstellen haben sich diese Techniken und Prozesse längst auch als äußerst wirksam für eine umfassende präventive Abwehrstrategie erwiesen. Konkrete Ergebnisse wurden erzielt, die dazu beigetragen haben, die Sicherheit und Cyberresilienz der Würth-Gruppe nachhaltig zu stärken.

Sie möchten mehr über die Funktionsweise und den Einsatzbereich von SATAYO wissen?

Kontaktieren Sie unser Cyber-Defense-Team



info@wuerth-phoenix.com



www.wuerth-phoenix.com





Security Operations Center



Gravitate GmbH
Fürther Straße 27
D-90429 Nürnberg
Tel. + 49 911- 28 7070 78
info@gravitate.eu
www.gravitate.eu

