Unsere SIEM und SOC Dienstleistungen

Protect7
your application security experts

Ihre Unternehmensdaten und die betriebliche Verfügbarkeit sind wesentliche Aspekte, die es zu schützen gilt. Bei Protect7 verstehen wir die ständig wachsenden Herausforderungen der heutigen Cyberbedrohungen. Deshalb bieten wir Ihnen erstklassige Dienstleistungen im Bereich SIEM (Security Information and Event Management) und SOC (Security Operations Center) an, um Ihre digitale Welt zu schützen.

Unser Managed SIEM/SOC Service im Überblick

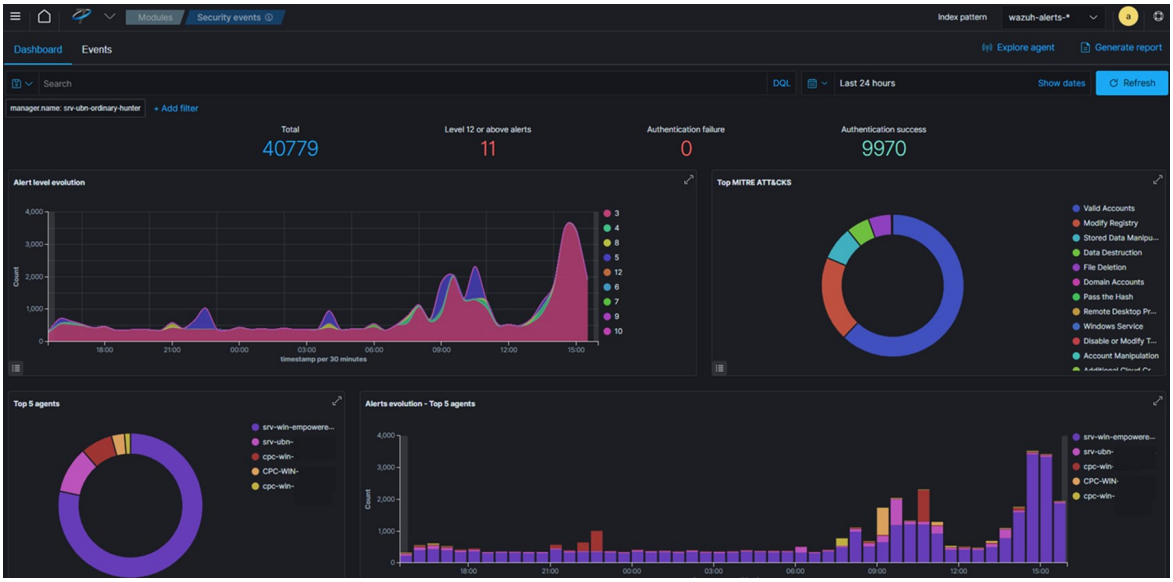
Echtzeitüberwachung: Unsere SIEM-Plattform analysiert die Logdaten Ihres Netzwerkes, Endpunkte und Applikationen rund um die Uhr und erkennt Unregelmässigkeiten.

Umfassende Bedrohungserkennung: Unsere fortschrittlichen Regeln & Algorithmen identifizieren nicht nur bekannte Bedrohungen, sondern erkennen auch unbekannte Angriffsmuster.

Schnelle Reaktion: Wenn eine Bedrohung erkannt wird, reagieren wir schnell. Unsere SOC-Analysten beobachten kritische Events im 5x9 Betrieb, um die Sicherheit Ihres Unternehmens zu gewährleisten.

Tiefgreifende Analyse: Wir gehen über die Oberfläche hinaus. Unsere Security-Analysten analysieren Bedrohungen im Detail, um ihre Herkunft und Absicht zu verstehen.

Kontinuierliche Optimierung: Wir passen unsere Sicherheitsstrategie kontinuierlich an die sich verändernde Bedrohungslage an und sorgen dafür, dass Sie immer zeitgemäss sind.



Ihre Sicherheit ist unsere Mission. Protect7 ist Ihr vertrauenswürdiger Partner im Kampf gegen Cyberbedrohungen. Lassen Sie uns zusammenarbeiten, um Ihr Unternehmen zu schützen, damit Sie sich auf das Wachstum und Ihre Geschäftsziele konzentrieren können.

Kontaktieren Sie uns noch heute, um mehr über unsere erstklassigen SIEM und SOC Dienstleistungen zu erfahren und wie wir Ihnen helfen können, Ihre Assets sicherer zu gestalten.

MANAGED SERVICES

Managed SIEM/SOC Service

Protect7
your application security experts

Unser Managed Service wurde speziell für Unternehmen entwickelt, die nach einer kosteneffizienten Lösung suchen, die sich zwischen einem vollständig verwalteten EDR und einem rund um die Uhr aktiven SOC (Security Operation Center) befindet. Unser Service kombiniert das Beste aus beiden Welten, ohne dabei auf wichtige Aspekte zu verzichten. Mit unserem Service haben Sie die Freiheit, den Umfang und das Intervall der explorativen Analyse von Sicherheitsereignissen selbst festzulegen, ganz nach den Bedürfnissen Ihrer Unternehmensgrösse und finanziellen Möglichkeiten.

Dadurch erhalten Sie erstklassige Qualität zu attraktiven Preisen. Sie haben die Gelegenheit, von unserem umfangreichen Fachwissen zu profitieren, um die Sicherheit und den Schutz Ihres Unternehmens zu stärken. Sie können potenzielle Sicherheitsverletzungen frühzeitig erkennen, bewerten und bei Bedarf angemessen darauf reagieren.

Unser Managed Service basiert auf folgenden Eckpfeilern:

Integration von Logdaten aus Endpoints, Infrastruktur, Applikationen und Cloud-APIs mithilfe von Open-Source-SIEM und XDR:

- Wir erfassen umfassend Daten von verschiedenen Quellen, darunter Endgeräte, Infrastrukturkomponenten und Cloud-Anwendungen, um eine ganzheitliche Sicherheitsüberwachung sicherzustellen.

Anwendung vordefinierter Regeln:

- Wir nutzen gut definierte Regeln, einschliesslich Sigma-Regeln, um verdächtige Aktivitäten zu identifizieren und potenzielle Bedrohungen frühzeitig zu erkennen.

Kontinuierliche Überwachung auf kritische Ereignisse:

- Wir sind ständig wachsam und überwachen Ihr System auf kritische Ereignisse, um unmittelbare Reaktionen auf Sicherheitsvorfälle zu ermöglichen.

Regelmässige Datenanalyse durch einen Sicherheitsanalysten von Protect7:

- Unsere hochqualifizierten Sicherheitsanalysten analysieren regelmässig die erfassten Daten, um sicherzustellen, dass keine Bedrohungen unbemerkt bleiben und um schnell auf neue Entwicklungen reagieren zu können.

Erweiterte Security Funktionen:

- Überprüfung der Systemintegrität und die Identifizierung von Schwachstellen in kritischen Systemen durch den Einsatz spezieller Agenten.

Diese Säulen bilden das Fundament unseres Services und gewährleisten, dass Ihr Unternehmen vor aktuellen und zukünftigen Cyberbedrohungen geschützt ist.

Sie erhalten

- 9x5 Überwachung & Analyse potentiell kritischer Events
- Integration aller relevanten Systeme inkl. Cloud-Infrastruktur wie M365, Azure, AWS als auch Custom Application Logs
- Regelmässige Analyse von Security Events und Logdaten durch einen Security Spezialisten
- Agentenbasierter Vulnerability und Integrity Check Ihrer kritischen Systeme

Ihr Vorteil

- Klar definiertes Security Operation
- Freie Wahl des Analyse-Intervalls
- Zeitlich und kostenmässig optimiertes Vorgehen
- Qualität, Aufwand und Preise wählbar
- Nutzen unseres Know-hows

MANAGED SERVICES

Managed SIEM/SOC

Protect7
your application security experts

Service Übersicht

Übersicht	S1-Managed
Integration von Security Logquellen	✓
Integration von Endpoints & Infrastruktur Komponenten	✓
Integration von Syslog basierten Komponenten	✓
Integration von Applikationslogs	✓
Integration von Cloud Providern (M365, Azure, AWS, Google, Github)	✓
Integration von individuellen API Services	✓
Top Features	
9x5 Monitoring kritischer Events und Alarmierung	✓
Security Event und Logfile Analyse pro Woche (Intervall nach Wunsch)	1 –5 mal pro Woche
Vulnerability, Hardening & Integritäts-Check der kritischen Systeme[1]	✓
Integrierung Alarmierung in Teams, Webex etc. möglich	✓
Zugang zum Analyse Dashboard für Kunden	✓
Anpassen der Regeln[2]	✓
Optimierte Architektur zur Kostenoptimierung	✓
Einfacher Zugriff auf weitere unserer Skills	✓
Abruf für technische Security Prüfung	✓

Preise

Die Kosten sind abhängig von der generierten Datenmenge (basierend der Anzahl der Logquellen) und dem gewählten Analyseintervall. Die Preise beginnen monatlich bei etwa CHF 2'200.– für kleine Umgebungen bis etwa CHF 4'500.– für mittelgrosse Umgebungen.

Setzen Sie sich mit uns in Verbindung, um ein individuelles Angebot oder eine Produktpräsentation zu erhalten.

Hinweis: Abhängig vom Analyse Intervall, werden pro Tätigkeit unterschiedliche Aufwände investiert.

1. Systeme welche mittels Agenten integriert werden, können aktiv auf Schwachstellen überprüft werden
2. Die Regeln, falls nötig, werden angepasst oder durch neue erweitert
3. Support nur während regulären Bürozeiten
4. Der initiale Aufwand für den Aufbau des OpenSource SIEM/SOC und der Integration relevanter Systeme sind nicht im Preis enthalten

MANAGED SERVICES

Managed SIEM/SOC

Protect7
your application security experts

Technische Features

Feature	S1-Managed
Integration Firewalls, Appliances & Security Quellen	via Syslog
Integration von Clients, Servern und Applikationen	mittels Monitoring Agent
Unterstütze Betriebssysteme	Alle gängigen inkl. macOS
Integration von Cloud Services	via API
Hardening Policy Check (SCA)	HIPAA, PCI DSS, CIS
Security Event Retention Time - Hot Storage	90 Tage
Eventdaten Cold Storage	360 Tage
Integration von Wazuh Security Rules	✓
Integration von Sigma Security Rules	✓
Integration von Protect7 Security Rules	✓
Integration von kundenspezifischen Security Rules	möglich

Use Case Beispiele	Bereich	Kategorie
Netzwerkverbindungen aus Zonen werden aufgebaut, wo keine Verbindungen erlaubt sind	Firewall	Outgoing traffic
Traffic aus DMZ zu internen Netzen wird aufgebaut, welche nicht explizit erlaubt sind	Firewall	DMZ to Internal
Traffic aus einem internen Netz zu einem anderen internen Netz wird aufgebaut, welche nicht explizit erlaubt sind	Firewall	Internal to Internal
DNS Abfragen werden auf nicht erlaubte überprüft	Firewall	Abnormal DNS
Spezifische Ports aus dem Internet wurden erfolgreich aufgebaut (ssh, RDP, Database)	Firewall	Compliance
Berechtigungen auf dem NAS werden geändert	NAS	Permission Change
Anzahl der Failed Logins werden im definiertem Zeitraum überschritten	Server	Failed Logins
Mehrere erfolgreiche Logins auf Server von der gleichen Source in kurzen Zeitabständen	Server	Successful Logins
Kritische Applikationen erzeugen eine hohe Anzahl Fehler	Application	Error
Azure App Granted Privileged Delegated Or App Permissions	Cloud	Sigma Rules
Cisco Clear Logs	Network	Sigma Rules
Password Dumper Remote Thread in LSASS	Server	Sigma Rules
WannaCry Ransomware Activity	Malware	Sigma Rules

MANAGED SERVICES