sepago
a PROACT company

SEPAGO SOC
GEBEN SIE IHRE IT SECURITY IN DIE RICHTIGEN HÄNDE

sepago. making people love it.

Eine Gemeinsamkeit, die wahrscheinlich die meisten IT-Abteilungen teilen, ist die notorische Personalknappheit. Die Suche nach Fachkräften ist aufwändig, und hat man sie gefunden, sind es immer zu wenig Fachkräfte für zu viele Lösungen, die überwacht (gemonitored) werden wollen. Zusätzlich folgt aus dem Wechsel von einer traditionellen Antivirus-Sicherheitslösung hin zu einer zeitgemäßen, geräteübergreifenden Endpoint Detection & Response (EDR)-Lösung eine Menge von neuen Alarmen, die eingeordnet und bearbeitet werden müssen. Unsere Antwort auf diese Herausforderung ist das sepagoSOC. sepagoSOC ist unser Angebot für Managed Security Services als Komplettlösung im Microsoft Ökosystem.

Unser Ziel ist es, den optimalen Schutz Ihrer Infrastruktur, Endpunkte, Identitäten, SaaS-Anwendungen und Daten zu gewährleisten. Dies gelingt uns durch das Zusammenspiel von permanenter Beratung in der sich ständig verändernden Cloud-Welt, unserer tiefgreifenden Expertise in der Absicherung mehrschichtiger Technologien und unserer zuverlässigen Leistung.

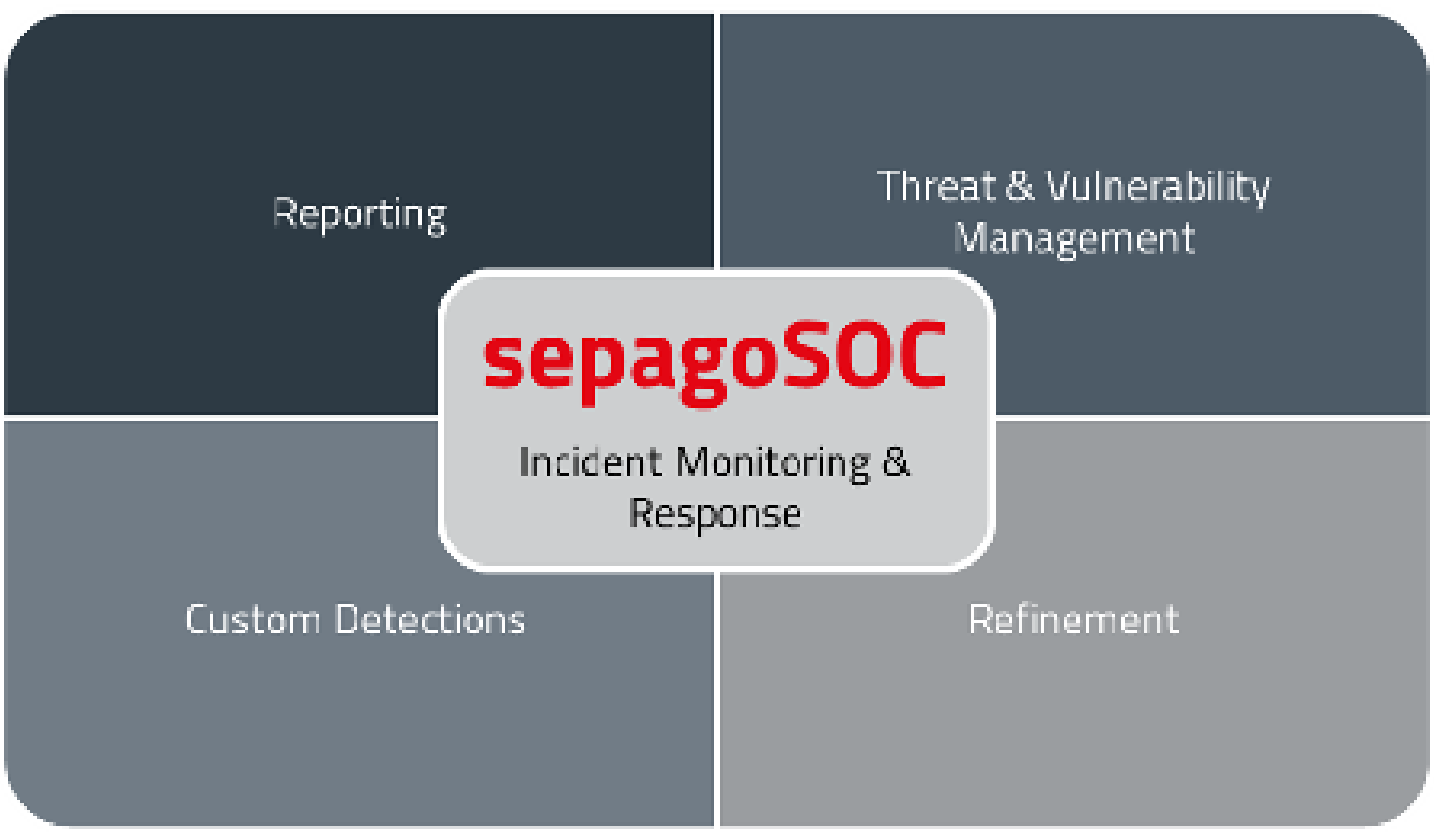
Das sepagoSOC ist modular aufgebaut und bietet verschiedene Services in verschiedenen Ausbaustufen an. Dadurch können wir auf die Anforderungen unserer Kunden flexibel eingehen und bieten genau das Servicelevel an, was gerade gebraucht wird.

Incident Monitoring & Response

Das Kernstück des sepagoSOC bildet der Service „Incident Monitoring & Response". Im Rahmen dieses Service überwacht das sepagoSOC aktiv die IT-Umgebung unserer Kunden mit Hilfe der Microsoft 365 Defender-Lösungen (Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Office, Microsoft Defender for Cloud Apps und Microsoft Sentinel).
Neue Alarme werden bewertet und nach einem standardisierten Verfahren abgearbeitet, wiederkehrende Alarme und deren Lösungsweg werden in Playbooks festgehalten und künftig, wenn möglich, automatisiert abgearbeitet.
Angereichert wird das „Incident Monitoring & Response" durch umfangreiches Reporting und verschiedene Dashboards. Hier ist z.B. neben einem Dashboard, dass unsere Service Level Agreement Treue abbildet und einem Management Summary Dashboard auch ein ASR Dashboard Teil unseres Services. Dieses Dashboard erleichtert die Arbeit mit Attack Surface Reduction Rules. Die Visualisierung von geblockten oder auditierten Regelanwendung ermöglicht kontinuierliche Anpassung des Regelwerks, um so auch langfristig die Sicherheit zu erhöhen, ohne die User unnötig zu unterbrechen.

Threat & Vulnerability Management

Um die Möglichkeiten, die Microsoft Defender for Endpoint bietet, voll auszuschöpfen, bieten wir darüber hinaus auch Threat & Vulnerability Management als Service an. Je nach Ausprägung des Services unterstützen wir von der Einordnung bis zur Beseitigung von Schwachstellen.
Als erfahrener Managed Service Anbieter haben wir in den letzten Jahren Best Practices entwickelt, wie die Möglichkeit zur Custom Detection im Microsoft Security Center am besten genutzt werden können. Dies sind über Standardalarme hinausgehende, individuelle Alarmierungen, die im Rahmen des Monitorings ebenfalls überwacht werden. Diese Custom Detections erstellen wir individuell angepasst für Ihr Unternehmen.



Refinement-Service

Der Funktionsumfang der Microsoft Security Tools erweitert sich ständig. Um diese neuen Funktionen sinnvoll einsetzten zu können, ist das Verständnis für potentielle Auswirkungen auf Ihre Unternehmensumgebung unerlässlich. Im Rahmen von quartalsweise stattfindenden Meetings stellen wir Ihnen neue Funktionen vor und beschreiben, wie Ihr Unternehmen von den neuen Funktionen profitieren kann.
Im Rahmen unseres Refinement-Service ist in einigen Ausbaustufen bereits ein Kontingent an Beratungstagen enthalten, in deren Rahmen unser Consulting Team unsere Kunden bei der Einführung neuer Funktionen und Optimierung der vorhandenen Funktionen unterstützt.

Aller Anfang ist leicht! Ihr Onboarding im sepagoSOC

Das Onboarding in unser sepagoSOC erfolgt erst dann, wenn mehrere Voraussetzungen erfüllt sind. Anfangs unterstützen wir unsere Kunden bei der strukturierten Einführung der Microsoft Security Lösungen. Doch die besten Lösungen sind immer nur so stark wie die Prozesse, die sie anstoßen. Für sepago ist die Entwicklung der richtigen Prozesse und die Vorbereitung auf den Ernstfall ein wesentlicher Bestandteil dieser Projekte! Daher legen wir einen besonderen Schwerpunkt auf die Operationalisierung und Erstellung von Prozessen im Zusammenhang mit Ihren neuen Sicherheitslösungen. Basierend auf unseren Erfahrungen aus vorangegangenen Kundenprojekten und den Best Practices von Microsoft werden wir im Rahmen von sepago adapt gemeinsam mit Ihnen Prozesse aufbauen und etablieren, die es Ihrer Organisation ermöglichen, alle Funktionen von M365 Defender vollständig zu nutzen. Das Ziel der Konzeption und Definition der neuen Prozesse ist ein strukturierter "Incident Handling and Remediation Prozess" sowie die perspektivische Implementierung in ein ITSM oder die Dokumentation in einem "Process Warehouse" für gesetzliche Anforderungen. Das volle Potenzial der eingesetzten technischen Sicherheitslösungen wird in diesem Modul ausgeschöpft.

Für eine genaue Beschreibung der einzelnen Services und ein persönliches Beratungsgespräch stehen wir Ihnen gerne zur Verfügung und freuen uns über Ihren Kontakt!

IT-Sicherheit funktioniert nur, wenn man sie anwendet.

Microsoft Solutions Partner
Security

KONTAKTIEREN SIE UNS
ANJA KRUMKAMP
IT Security Sales

sales@sepago.de

sepago. making people love it.

sepago GmbH
Dillenburger Straße 83
51105 Köln

Tel.: +49 221-801 93 95 0
info@sepago.de
www.sepago.de

Partner
Microsoft
citrix

Always informed with sepago: