



Microsoft
Partner
 Microsoft

Azure
Expert
MSP



Microsoft Sentinel Checkup



Kunde hat Microsoft Sentinel aktiv im Einsatz, um die Erkennung von Anomalien, Sicherheitsbedrohungen und Angriffe über Tool- bzw. Applikationsgrenzen hinweg, zu ermöglichen. Dazu hat SoftwareOne folgendes Vorgehensmodell etabliert:

Kick-off Termin

Der KickOff Termin dient dazu alle Beteiligten über das Vorhaben zu informieren und den Scope des CheckUps darzulegen. Zusätzlich werden die Anforderungen an Berechtigungen sowie die Art und Weise des Reportings erläutert.

Microsoft Sentinel Checkup/Review

Während diesem Schritt wird der eigentliche Checkup durch die beteiligten Consultants durchgeführt. Hierbei wird die Microsoft Sentinel Umgebung des Kunden einem Review unterzogen, bei welchem die „Reife“ der Umgebung überprüft wird. Ziel ist es eventuelle Optimierungspotentiale festzustellen.

Der Checkup selbst orientiert sich an der gleichen Vorgehensweise, welche auch im Kontext eines Microsoft Sentinel POCs bzw. einer Microsoft Sentinel Migration verwendet wird. Diese besteht aus drei Phasen.

- Setup of Environment
 - Hier wird das „Fundament“ der Umgebung (Microsoft Azure Architektur) überprüft und entsprechend der gängigen BestPractices überprüft.
- Setup of Collection
 - Hier wird die Anbindung die Logging Strategie, die Log Quellen und das Parsing entsprechend der gängigen Best Practices überprüft.
- Detect/Investigate/Response
 - Hierbei wird die Verwendung der Gesammelten Logs zur Erkennung von Vorfällen, die Aufbereitung zu Untersuchung sowie die eingesetzten Möglichkeiten/Vorgehensweisen zur entsprechenden Reaktion (SOAR) untersucht.

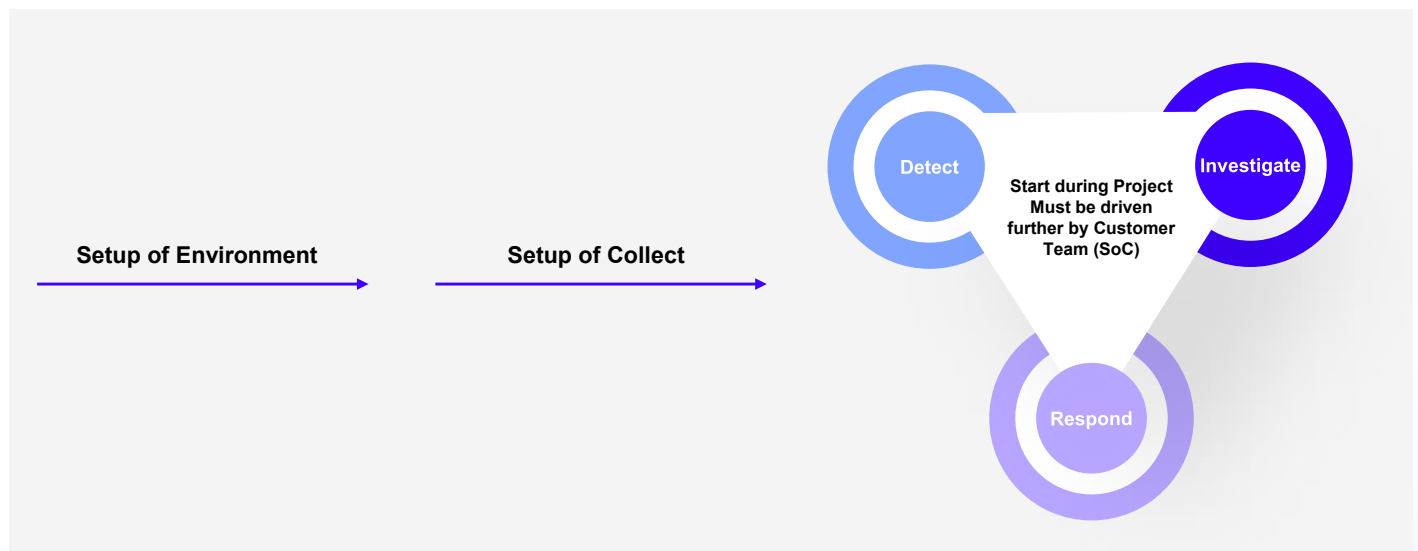


Abbildung 1, Microsoft Sentinel Approach

Ergebnispräsentation und Diskussion

Die Ergebnisse des Reviews werden entsprechend für diesen Punkt aufbereitet. In einem Gemeinsamen Termin mit den Ansprechpartnern des Kunden präsentiert und ggf. diskutiert. Das Ziel ist, das der Kunden einen Überblick über das Optimierungspotential erhält. Aus diesen Empfehlungen kann bei Bedarf eine Roadmap inkl. einer Priorisierung entwickelt werden.

Im Folgenden finden sie die Inhalte und Leistungsbeschreibung:

Leistungsbeschreibung

Arbeitspaket 1	Microsoft Sentinel Checkup
Leistungsumfang	<ul style="list-style-type: none"> • Durchführung eines KickOff Termins zur Definierung des Scopes sowie Erläuterung der Vorgehensweise. Weitere Inhalte des KickOff Termins beinhalten u.a <ul style="list-style-type: none"> • Abstimmung der Voraussetzungen (Berechtigungen) • Definition der beteiligten Ansprechpartner (APs für Rückfragen) • Grobe Zeitplanung • Durchführung des Microsoft Sentinel Checkups auf Basis der folgenden Bereiche: <ul style="list-style-type: none"> • Setup of Environment • Setup of Collection • Detect/Investigate/Response • Result Präsentation and Discussion <ul style="list-style-type: none"> • Hier werden die Erkenntnisse des zuvor durchgeführten Reviews aufgearbeitet und in einem gemeinsamen Termin mit dem Kunden durchgesprochen. • Ziel ist es dem Kunden zusammengefasst (PPTX und EXCEL) Optimierungsmöglichkeiten bzw. den aktuellen Status der Microsoft Sentinel Umgebung aufzuzeigen.
Sonstiges	
Annahmen / Abgrenzungen	<ul style="list-style-type: none"> • Die Umsetzung der identifizierten Optimierungsmöglichkeiten der Microsoft Sentinel ist nicht Bestandteil dieses Projektes. • Die Integration von Microsoft Sentinel in ein anderes SIEM Produkt, ist nicht Teil des Projekts. • Alle zusätzlichen Ressourcen oder Anwendungen werden als außerhalb des Bereichs liegend betrachtet. • Es wird nicht erwartet, dass SoftwareOne Sentinel während des Projekts aktiv überwacht. • SoftwareOne führt im Rahmen dieses Auftrags keine reaktiven Tätigkeiten auf Sicherheitsvorfälle durch. • Der Umfang des Microsoft Sentinel-CheckUP umfasst keine, nicht im Angebot definierten Tätigkeiten bzw. Scopes. • Microsoft Sentinel Checkup umfasst keine Bereitstellung einer Microsoft Sentinel Umgebung. • Infrastrukturkonfigurationen sind nicht im Umfang enthalten. • Jedes Thema, das nicht ausdrücklich als Bestandteil erwähnt wird, gilt als ausgeschlossen und außerhalb des Geltungsbereichs. • SoftwareOne garantiert nicht die Einhaltung von NIST-, CIS-, PCI- oder anderen regulatorischen oder branchenspezifischen Anforderungen. • Das Thema der richtigen Lizenzierung für den Produktiveinsatz ist in diesem PoC nicht Bestandteil. • Das Review von IaC Templates zur Bereitstellung der Microsoft Sentinel Umgebung, ist nicht Bestandteil des Microsoft Sentinel CheckUPs
Voraussetzungen / Mitwirkungspflichten	<ul style="list-style-type: none"> • Für die Projektteilnehmer muss ein Gast-Account erstellt werden und alle notwendigen Rechte zum Durchführen des CheckUPs müssen gegeben sein. • Bereitstellung technischer Ansprechpartner um etwaige Abhängigkeiten und Aufgaben zu klären bzw. durchzuführen.
Ergebnis	<ul style="list-style-type: none"> • Ergebnis des Microsoft Sentinel Checkups in Form einer Excel Datei sowie einer PDF Datei. • Durchgeführte Präsentation der Erkenntnisse aus dem Review

Aufwand und Kosten

Der Aufwand für die beschriebene Leistung basiert auf den uns vom Kunden zur Verfügung gestellten Daten, und ist auf Basis eines Tagessatzes kalkuliert. Der genaue Zeitplan wird nach Beauftragung erstellt.

Kostenübersicht

Pos.	Anzahl	Einheit	Beschreibung	Währung	Einzelpreis	Gesamtpreis
1	18	PT	Microsoft Sentinel PoC Azure Senior Consultant	EUR	1,550	27,900
	Nettobetrag zzgl. gesetzlicher MwSt. via remote					27,900

KONTAKTIEREN SIE UNS

Besuchen Sie uns auf
www.softwareone.com

DE
phone: +49 341 2568 000
email: info.de@softwareone.com

AT
phone: +43 1878 100
email: info.at@softwareone.com

CH
phone: +41 844 44 55 44
email: info.ch@softwareone.com



Copyright © 2025 by SoftwareOne AG, Riedenmatt 4, CH-6370 Stans. Alle Rechte vorbehalten. SoftwareOne ist eine eingetragene Marke der SoftwareOne AG. Alle anderen Marken sind Eigentum der jeweiligen Inhaber. SoftwareOne übernimmt für die Aktualität, Vollständigkeit und Richtigkeit keine Gewähr. © Bildmaterial von: Adobe Stock und Getty Images.