G DATA
CyberDefense

SecMon – Security Monitoring simplified

G DATA Advanced Analytics GmbH

Christian Landström

Head of Managed Security Services

Was betrachten wir ?

Relevanz von Schutzmaßnahmen

SecMon – Konzept und Umsetzung

Welche Vorteile hat der Kunde

Relevanz von Schutzmaßnahmen

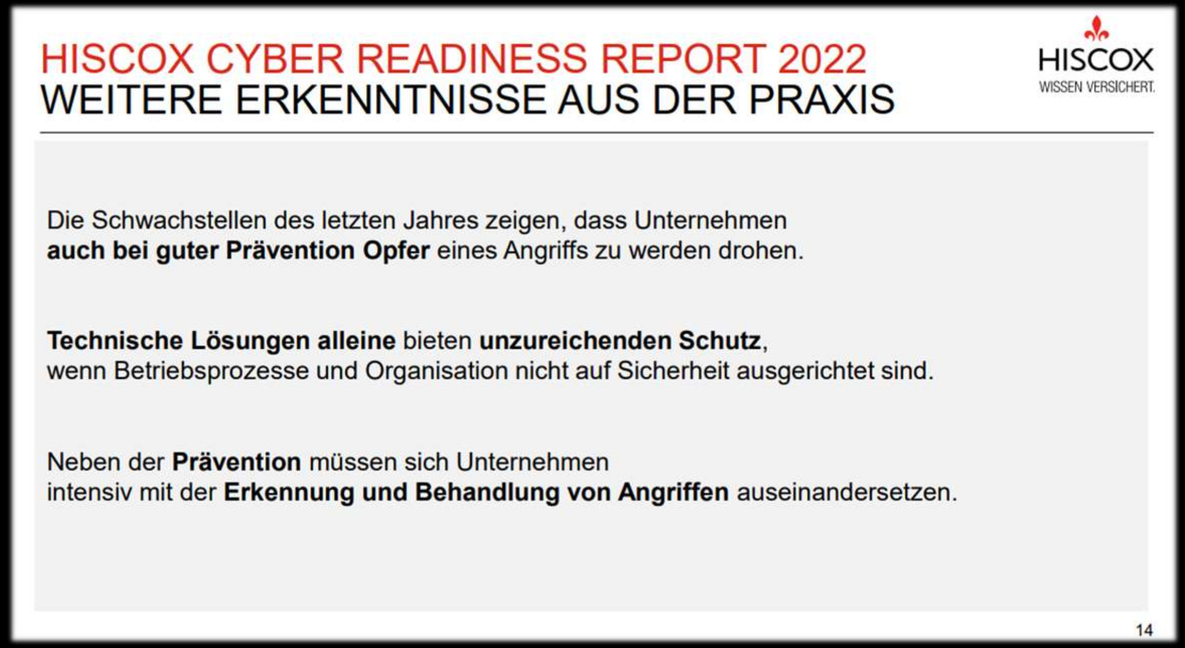
Penetration Test
Security Assessment
Red Teaming
Awareness
Threat Intelligence

Firewall
Endpoint Protection
Sandboxing
Email-/Web Protection

Incident Response
(Retainer)
Forensik
Malware Analyse

Managed Security
Services
LogManagement / SIEM
Security Monitoring

Realistischer Umgang mit Cybersicherheit



Aus dem Bericht „HISCOX CYBER READINESS REPORT 2022 Key Findings“ [1]

2022-cyber-readiness-report-key-findings.pdf

[1] https://www.hiscox.de/wp-content/uploads/2022/05/Hiscox-Cyber-Readiness-Report-2022-Key-Findings-DE.pdf

SecMon – Security Monitoring simplified

Warum SecMon ?
Sicht eines Incident Responders

Vorher:

Nachher:

G DATA CyberDefense

SecMon – Konzept und Umsetzung

Viel hilft viel…

- Wo liegen überall Logdaten?
- Welche davon sind für die Erkennung eines Cyberangriffes relevant?
- Wer sucht wie lange in den Daten?
- Wie weit in die Vergangenheit kann in den Logs gesucht werden?
- Was tun bei Alert Fatigue?

Was ist SecMon eigentlich genau ?

SecMon ist ein Managed Security Service der GDATA Advanced Analytics

SecMon verfolgt einen hybriden Ansatz mit Komponenten aus

- Managed SIEM
- SOC-as-a-service
- Managed Threat Response

SecMon arbeitet Stand heute auf Windows Servern ab Windows Server 2012/R2*

* Weitere Betriebssysteme siehe Roadmap

Welche Strategie verfolgt SecMon ?

- Assume Compromise – ihre Benutzer Endgeräte werden kompromittiert, immer !
- Detektion da, wo es wichtig wird -> beim Übergang in die zentrale Infrastruktur
- Manuelle Bearbeitung von erfahrenen Security Analysten anstatt reinem Machine Learning
- Direkte Kommunikation zwischen uns und den Kunden

Wie funktioniert SecMon ?

- Unsere Agent Software (Orchestrator) wird auf den zu überwachenden Systemen installiert.
- Die existierenden Logdaten werden an unser Incident Response Team übermittelt zur Überprüfung, ob bereits Systeme aktiv kompromittiert sind
- Neue Logdaten werden durch uns gefiltert an unser BackEnd übermittelt und dort ausgewertet.
- Unser Security Analysten Team in Bochum qualifiziert etwaige Anomalien, Fehlermeldungen und kritische Meldungen und kontaktiert den Kunden bei Bedarf

Wie funktioniert SecMon ?

Servertyp / Events pro Zeiteinheit	Events lokal	Events für Forensik	Events nach Filter
Kleiner Domain Controller	32.233	17.394	2.094 (6,5%)
Windows Server 2012 / 2016	5.669	1.857	776 (13,7%)
Windows Server 2019 / 2022	7.585	1.763	977 (12,9%)
Großer Domain Controller	108.845	58.530	3.988 (3,7%)

Welche Vorteile hat der Kunde

Wie unterscheidet sich SecMon von anderen Produkten und Services ?

- Leichtgewichtig: Der SecMon Orchestrator ist sehr schlank und braucht kaum Ressourcen
- Simpel: Einmal installieren – wir übernehmen den Rest
- Integrierbar: SecMon konkurriert nicht mit Schutzkomponenten, sondern komplettiert diese
- Erweiterbar: Spätere Produktiterationen einfach dazubuchen
- Kombinierbar: Mit unseren Incident Response Retainer Leistungen doppelt profitieren
- Flexibel: Sie bestimmen, wie viele Systeme Sie ins Monitoring nehmen
- Produktunabhängig: Wir arbeiten mit dem, was Sie einsetzen, nicht umgekehrt.

SecMon – Security Monitoring simplified

Das Stichwort ist „Konsumierbarkeit“

Do 02.09.2021 09:36

secmon-service@gdata-adan.de

Handlung erforderlich: SecMon Ticket Nr. SECMON-[redacted]

An [redacted]

Sehr geehrte Damen und Herren,

bei einem oder mehreren Systemen, die wir für Sie im Security Monitoring betreuen, ist ein Fall aufgetreten, der Ihre Aktion erfordert.

Auf diesem System gab es am 01.07.2021 um 17:55 UTC eine Skriptausführung, die Klartextpasswörter enthält:

- [redacted]

Bei dem ausgeführten Skript handelt es sich um folgendes:

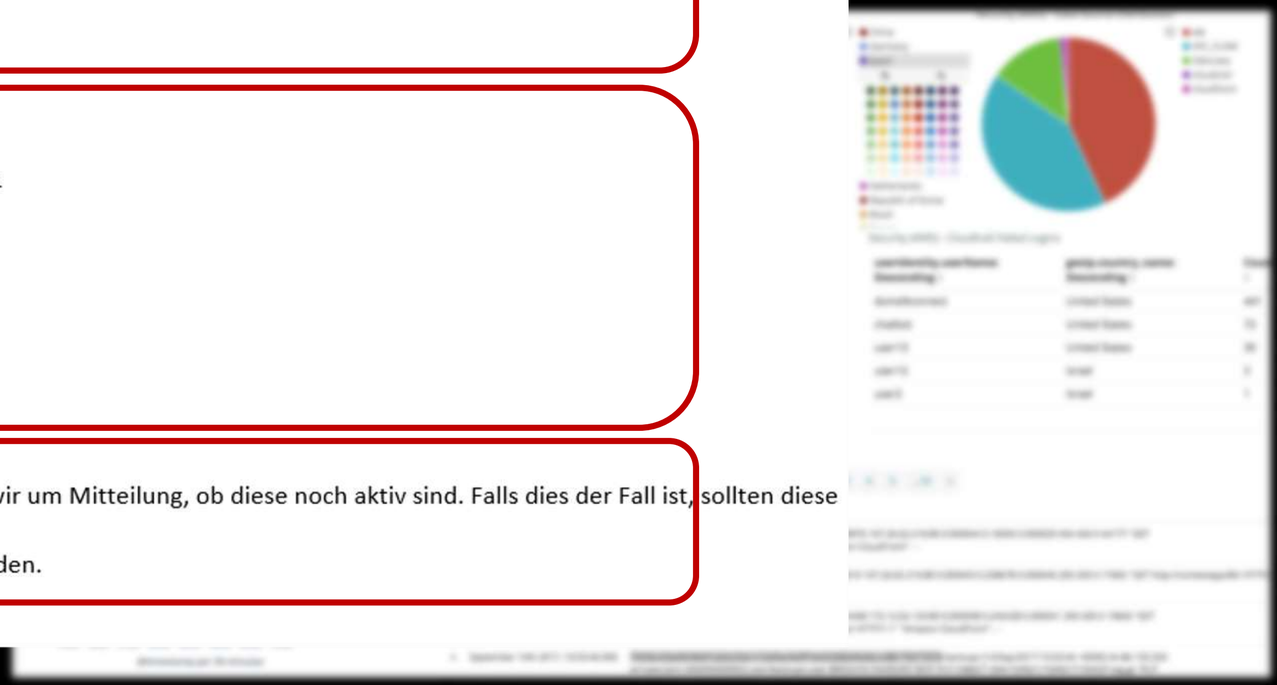
- E:\[redacted].ps1

Enthalten sind die Klartextpasswörter von folgenden Benutzern:

- [redacted]
- [redacted]
- [redacted]

Da die Passwörter der beiden lokalen Benutzer sehr schwach sind, bitten wir um Mitteilung, ob diese noch aktiv sind. Falls dies der Fall ist, sollten diese zeitnah durch starke Passwörter ersetzt werden.
Es ist generell davon abzuraten, Klartextkennwörter in Skripten zu verwenden.

Mit freundlichen Grüßen aus Bochum,



G DATA CyberDefense

Sie haben große Pläne ?

„Ich will aber mein eigenes SIEM haben und
ein SOC wollen wir auch aufbauen.“

Schließen Sie die zeitliche Lücke mit SecMon und profitieren Sie doppelt:

1. SecMon ist binnen Stunden einsatzbereit und läuft so lange, bis Sie soweit sind Ihr eigenes Monitoring in Betrieb zu nehmen

2. Viele relevante Informationen zur Definition Ihrer eigenen Use-Cases werden Sie bereits dank SecMon kennen und in der IT schon „bearbeitet“ haben

G DATA
CyberDefense

Sie wollen mehr erfahren?

Dann bleiben Sie mit uns in Kontakt.

G DATA
CyberDefense

Vielen Dank
für Ihre **Aufmerksamkeit**