SmartIT Services AG

Azure Zmorge - Security Operations Center

Bern, Oktober 2023

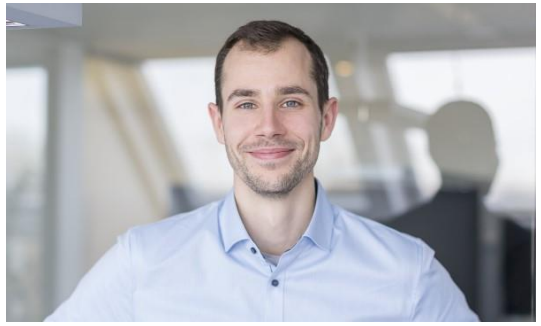
Ansprechpartner
SmartIT Services AG

Thomas Graf
t.graf@smartit.ch

Head of Sales | Account Manager

Aladin Steiner
a.steiner@smartit.ch

Head of Value Stream Azure | Service Owner SOC



Martin Schmidli
m.schmidli@smartit.ch

Senior System Engineer | Security Operations Center Analyst

Agenda

Eintreffen und Frühstück (30‘)

Geniessen Sie italienischen Spitzenkaffee und ein leckeres Frühstück zur Stärkung vor dem Event

08:00

Begrüssung

Begrüssung und Agenda durch Thomas Graf – Head of Sales

08:30

08:40

SmartIT Security Operations Center (30’)

Was ist ein SOC und was ist das SmartIT-SOC im Speziellen?
Aladin Steiner, Head of Value Stream Azure berichtet.

09:10

Kaffeepause (15’)

Kurze Biopause und Koffeinnachschub

09:30

Das SmartIT-SOC in der Praxis (45’)

Demonstration eines Angriffs, die Schwierigkeiten bei der Erkennung ohne ein SOC und wie das SOC im konkreten Fall hilft.

10:15

Abschluss

Diskussion, Fragen, Networking

SmartIT KMU Security Operations Center im Überblick

SmartIT

Themenschwerpunkte

Bedrohungslage
Warum Cyber-Sicherheit wichtig ist

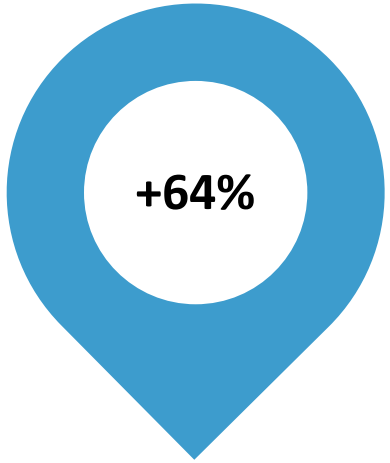
SOC im Überblick
Was ist ein Security Operations Center und was macht es

KMU Security Operations Center SmartIT
Welchen Mehrwert bieten wir mit KMU SOC

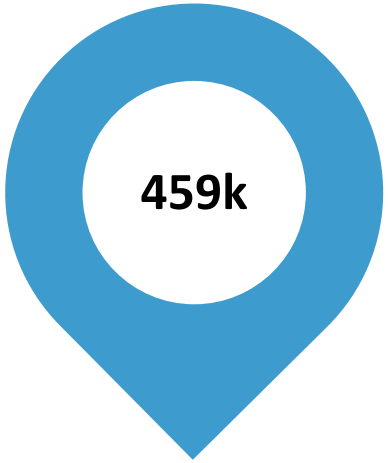
Angebot
Sicherheit als Managed Service zum monatlichen Preis

Was hat sich in den letzten Jahren aus meiner Sicht verändert?

Finanzieller Schaden pro Jahr durch Cyberkriminalität in der Schweiz



Anstieg von Ransomware-Angriffen auf Schweizer Unternehmen (RaaS)



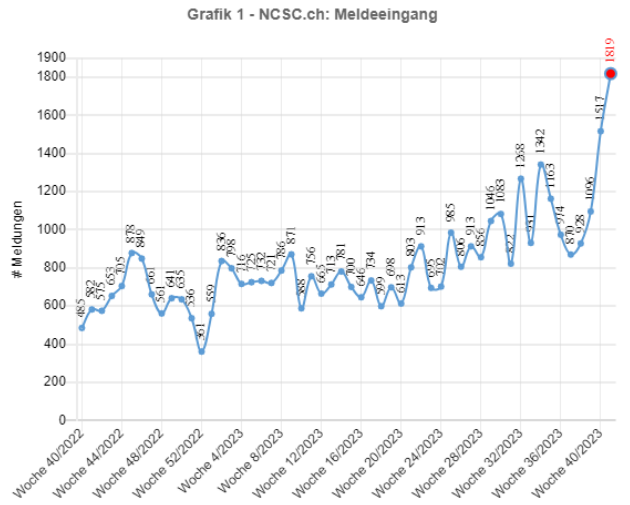
Entdeckte Phishing-Webseiten weltweit im 2023

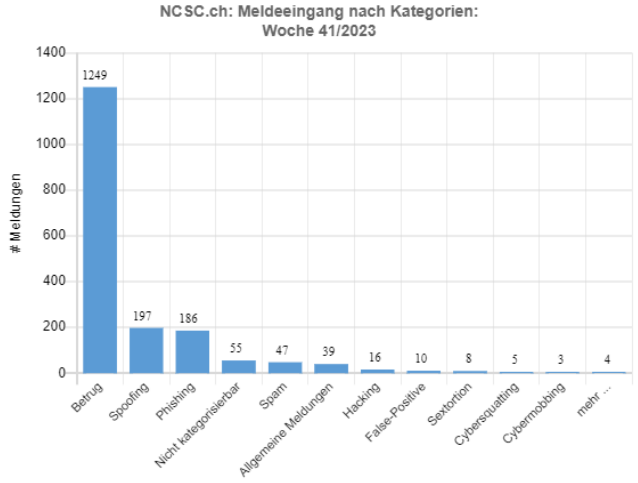
Gemeldete Cyberangriffe pro Woche KW41 2023 (NCSC).

Cyberattacken 2023 in Zahlen

Warum Cyber-Sicherheit wichtig ist - Statistiken 2023

- NCSC Meldeeingang KW41 2023: 1819 pro Woche / 260 pro Tag.
- Durchschnittlich werden 777 Angriffe pro Woche pro Unternehmen gemessen. Das entspricht einer Steigerung gegenüber dem Vorjahr um 61 Prozent.
- Aufklärungsrate Cyberkriminalität 2022: 34.3 %





SmartIT

Warum Cyber-Sicherheit wichtig ist

Der Verwaltungsrat hat gemäss Art 716a OR die unentziehbare und nicht delegierbare Aufgabe der Oberleitung und damit die Ausgestaltung eines angemessenen Risikomanagements, wozu auch Cybersecurity gehört

Cybersecurity Bedrohungslage auf Rekordniveau

Swatch Group shuts down some of its technology systems after detecting a cyberattack over the weekend.

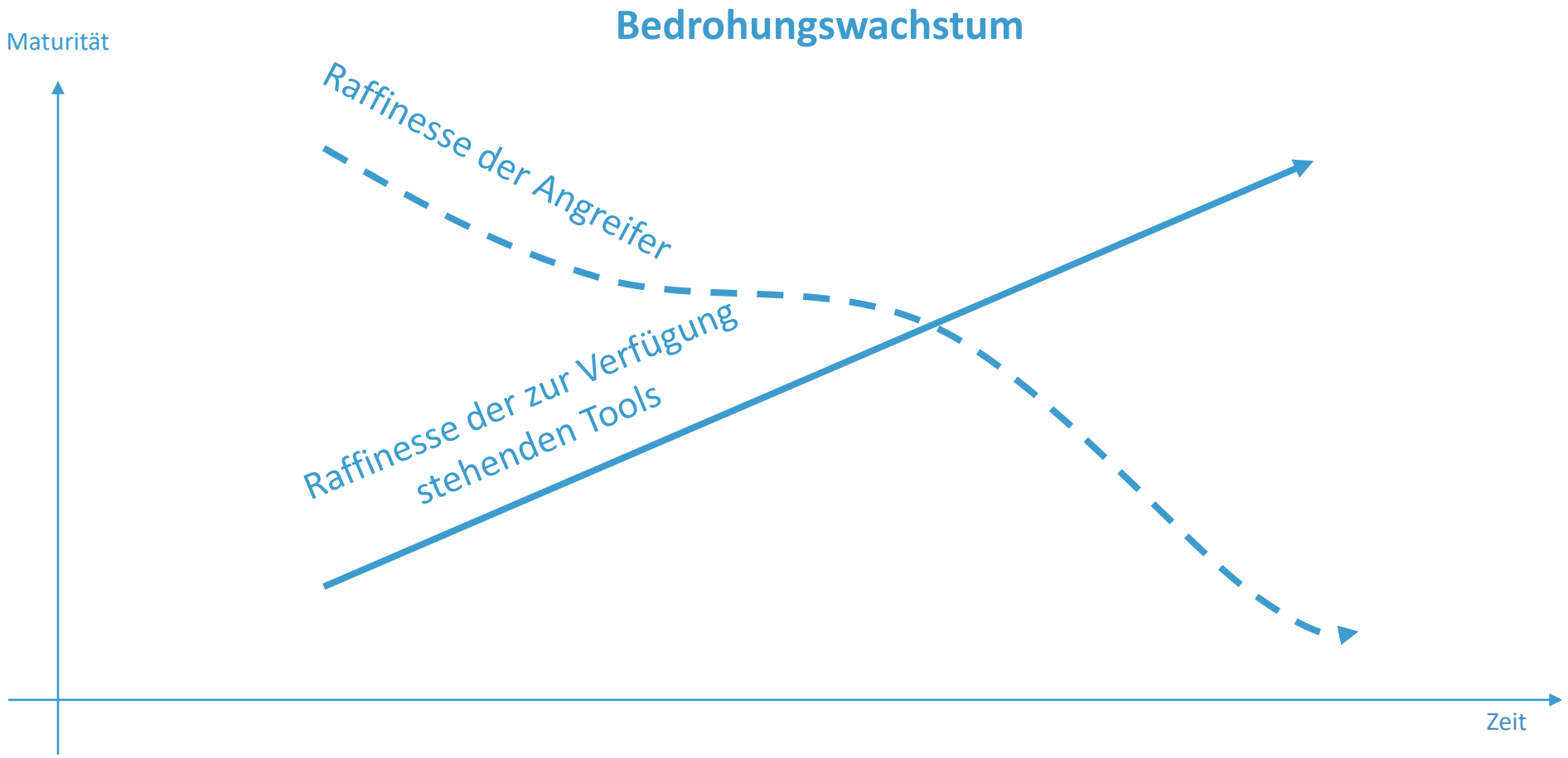
Target CEO Gregg Steinhafel resigns after massive securiy breach.

77% aller KMUs werten LOG Daten nicht regelmässig und systematisch aus.

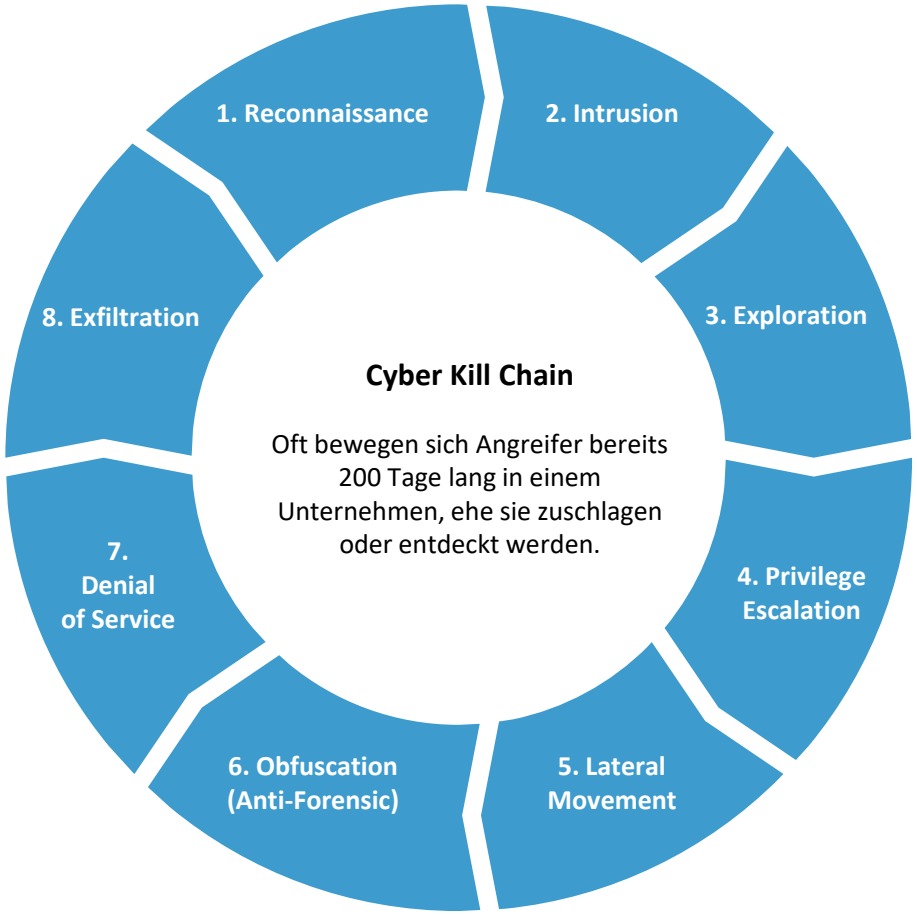
Bei einem Ransomware Angriff auf Comparis.ch wurden IT-Systeme blockiert und der Service war länger nicht verfügbar

SmartIT

Mensch gegen Maschine



Cyber Kill Chain – Phasen eines Cyberangriffs



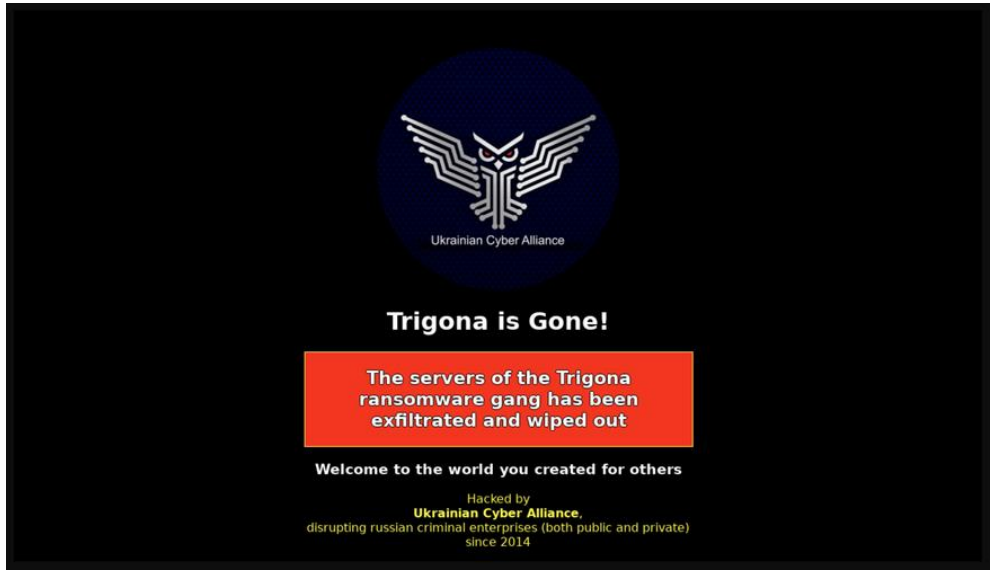
SmartIT

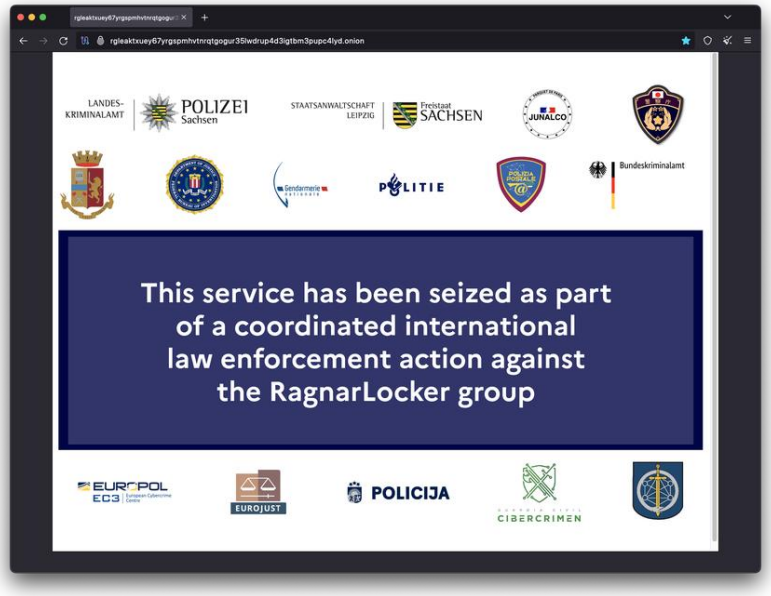
Jede 4. Unternehmung von Cybervorfall betroffen.

Die neusten Zahlen vom Nationalen Zentrum für Cybersicherheit (NCSC) lassen aufhorchen und zwingen Unternehmen zu handeln.

Egal wie der Cyberangriff ausgesehen hat, das Schadenpotenzial ist enorm gross.

Es gibt auch gute Neuigkeiten





SmartIT

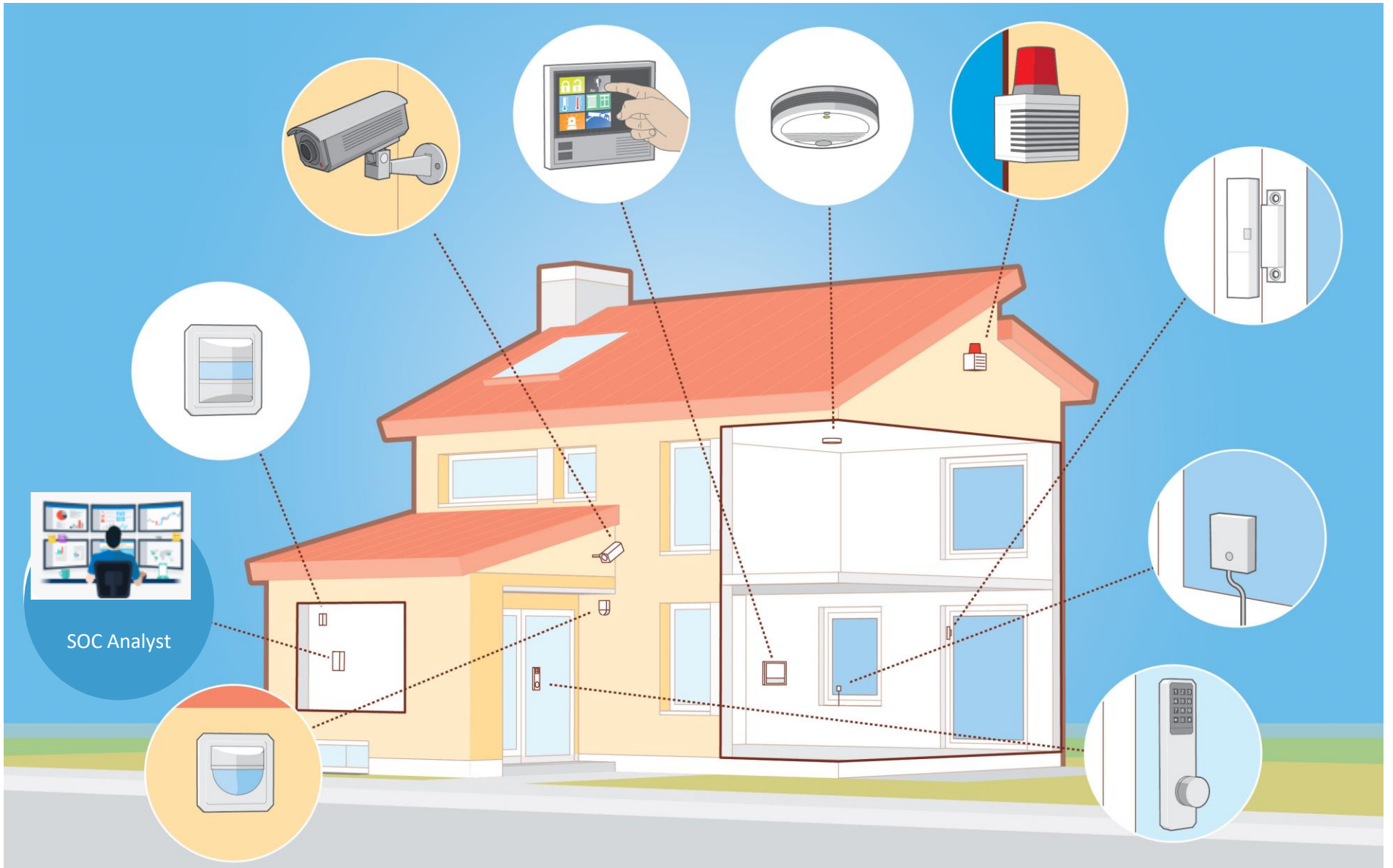
Was ist ein SOC?

- Ein SOC ist ein zentraler Punkt innerhalb oder ausserhalb eines Unternehmens, der sich auf die **Erkennung, Analyse und Abwehr von Cyberbedrohungen** spezialisiert hat.

- Ein SOC besteht aus einem **Team von Experten**, die Sicherheitswerkzeuge, Technologien, Methoden und Prozesse einsetzen, um Bedrohungen zu identifizieren, zu untersuchen und entsprechende Gegenmassnahmen zu ergreifen.

- Ein SOC wählt, betreibt und pflegt auch die Cybersicherheitstechnologien des Unternehmens und analysiert kontinuierlich Bedrohungsdaten, um Wege zu finden, das Sicherheitsniveau des Unternehmens zu verbessern.

SmartIT




AMS
EMEA
Security Operations & Management Center

SmartIT - KMU Security Operations Center

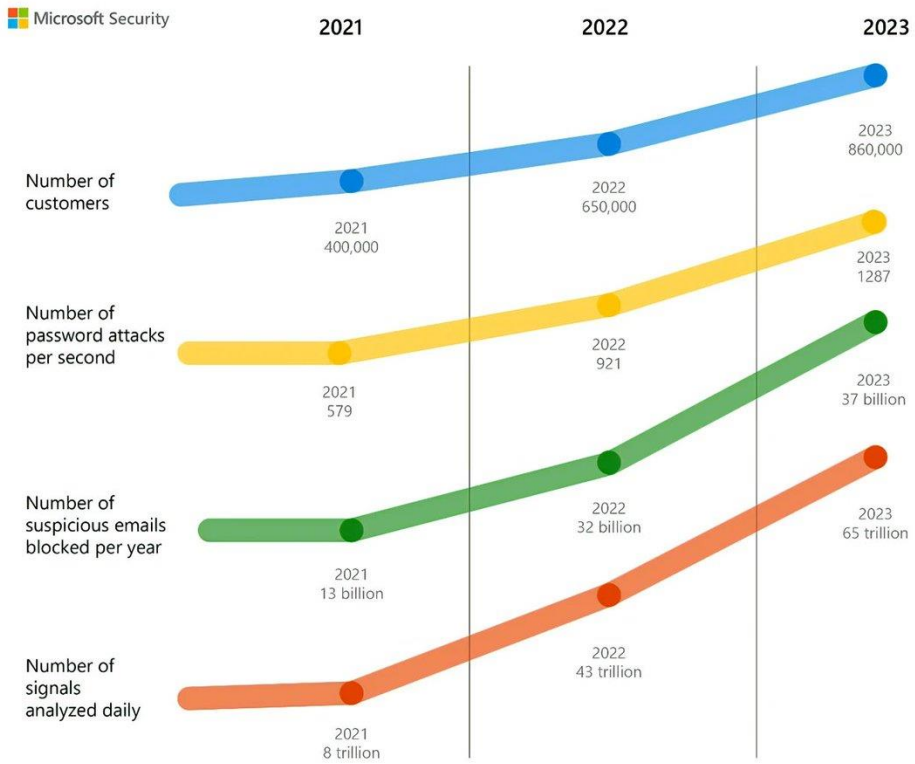
SmartIT - KMU Security Operations Center

Security-zentrale	▪ Team von IT-Experten mit Expertise in Informationssicherheit ▪ Kontinuierliches überwachen, analysieren und abwehren von Cyberangriffen
Endpoint Protection	▪ Internetverkehr, Netzwerke, Desktops, Server, Datenbanken, Anwendungen und andere Systeme werden kontinuierlich auf Anzeichen eines Sicherheitsvorfalls untersucht
Managed Service	▪ Übergabe der Sicherheitsüberwachung an ein Team von Sicherheitsspezialisten ▪ Kontinuierliche Verbesserung der Erkennungs- und Präventionsprozesse
Risiko Management	▪ Der Kunde ist nach wie vor verantwortlich für die Risikobewertung und Definition des Risikoappetits, wir unterstützen ihn bei der Risikominimierung ▪ Gemeinsame Definition der Cybersicherheitsstrategie und Ausrichtung an der aktuellen Geschäftszielen und -problemen

SmartIT - KMU Security Operations Center

Verbessertes Sicherheits-personal	▪ Fachkräftemangel im Bereich Cybersicherheit ▪ SmartIT SOC-as-a-Service Angebot ergänzt oder schliesst Lücken einer Unternehmung in bestehender Sicherheitsstrategie
Zugriff auf spezialisierte Sicherheits-expertise	▪ Unternehmen benötigen regelmässig Zugriff auf spezialisierte Sicherheitsexperten wie Incident Responder, Malware-Analysten und Cloud-Sicherheitsarchitekten ▪ SmartIT kann seinen Kunden bei Bedarf Zugang zu qualifizierten Cybersicherheitsspezialisten bieten.
Niedrigere Gesamt-betriebskosten	▪ Kein internes & teures Knowhow notwendig ▪ Planbare Kosten
Erhöhte Sicherheitsreife	▪ Der Aufbau von Lösungen und institutionellem Wissen für ein ausgereiftes Cybersicherheitsprogramm ist ein längerer Prozess ▪ Fixkosten für Ausrüstung, Lizenzen und Gehaltsabrechnung können mit den anderen Kunden geteilt werden, welche sowohl die Kapital- als auch die Betriebsausgaben (CapEx/OpEx) reduziert
Aktuelle Sicherheit	▪ SmartIT mit dem SOC-as-a-Service verfügt über die erforderliche Grösse und Expertise, um ihr Toolset auf dem neuesten Stand zu halten, und bietet seinen Kunden die Vorteile modernster Sicherheit.

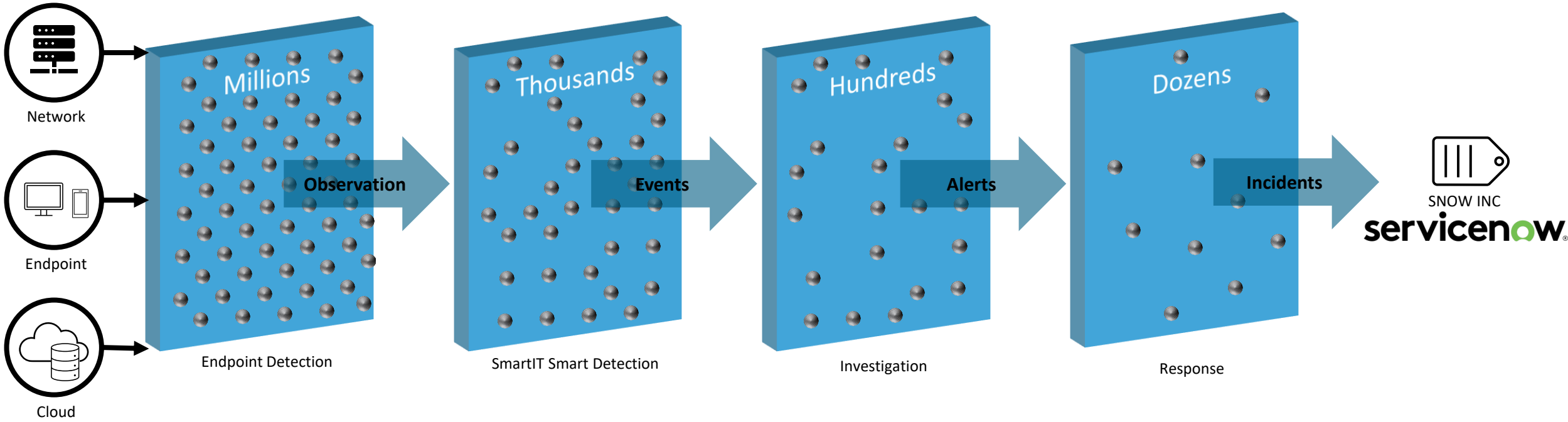
Wir setzen auf Microsoft Security



Im Bereich der Sicherheit verzeichnete Microsoft im Vergleich zum Vorjahr ein Wachstum von 32 % und wird weiterhin von Gartner als führende Lösung auf dem Markt eingestuft.

SmartIT

Security Operation in Practice



Security Operation ist betriebsnah

Standard SOC

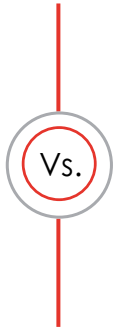
Externer SOC-Anbieter. Meist ausgerichtet auf Grossunternehmungen. Gruppe aus Sicherheitsspezialisten ohne KMU-Erfahrung.

- Standard SOC
- Phishing Simulation
- Social Engineering
- Known Vulnerability's
- Kennt den Schweizer Markt nicht
- Physische Sicherheit
- Penetrationstest
- Maschinell
- Sitzt irgendwo
- Kennt die Prozesse nicht

Extern

Nicht im Kundenteam

Nicht auf KMU ausgelegt



SmartIT KMU SOC

Blue Teams im Bereich Cybersicherheit bewerten und analysieren ständig Informationssysteme, um Systeme zu patchen, Sicherheitslücken und sicherheitsrelevante Konfigurationsprobleme zu ermitteln und die Auswirkungen von Sicherheitskontrollen zu überprüfen.

- Prävention
- Kundennah
- Betriebsnah
- Persönlich, in Bern
- Einsitz im NCSC
- Gesunder Produktemix
- Gemeinsam im Team agieren
- Technologisch vorne mit dabei
- Integration in bestehende Prozesse und Service NOW Anbindung

Betriebs- und Prozessnah

Proaktive Stärkung durch Sicherheits-experten

Wachsam und Verteidigungs-bereit

SmartIT SOC – wiederkehrende Kosten pro Monat

Leistung	Preis	Anzahl	Summe
Managed Security Operation Center Standard pro Unternehmen - Basispreis	CHF 350.00	1	CHF 350.00
Managed Security Operation Center pro Endpoint	CHF 19.00	50	CHF 950.00
Total wiederkehrende Kosten Benutzer			**CHF 26.00**

Lizenzen und Azure Consumption*	Preis	Anzahl	Summe
Microsoft Defender for Endpoint Plan 2	CHF 4.70	50	CHF 235.00
Microsoft Defender for Server P1	CHF 5.10	5	CHF 25.50
Microsoft Azure Consumption Verrechnung nach Aufwand	CHF 20.00	1	CHF 20.00

*Je nach Lizenzierungsmodell bereits im Einsatz

SmartIT SOC – einmalige Projektkosten

Leistung	Stunden	Summe
Projektleitung	8h	CHF 2000
Aufbau Azure Infrastruktur & SOC Software	18h	CHF 3’600.00
Microsoft Defender for Endpoint Plan 2	9h	CHF 1’800.00
Implementation Defender for Server Plan 1	9h	CHF 1’800.00
Dashboard Schulung	-	CHF 2’000
Nachbesprechung Go-Live	5	CHF 1’000
Total einmalige Kosten		**CHF 12’200.**
Total einmalige Kosten nach Rabatt		**CHF 9’600.**

20% Rabatt auf die einmaligen Projektkosten (Bestellungen bis Ende Jahr)

Kaffeepause (15’)

SmartIT KMU Security Operations Center in der Praxis Praxis (45')

SOC-Komponenten

Endpoints

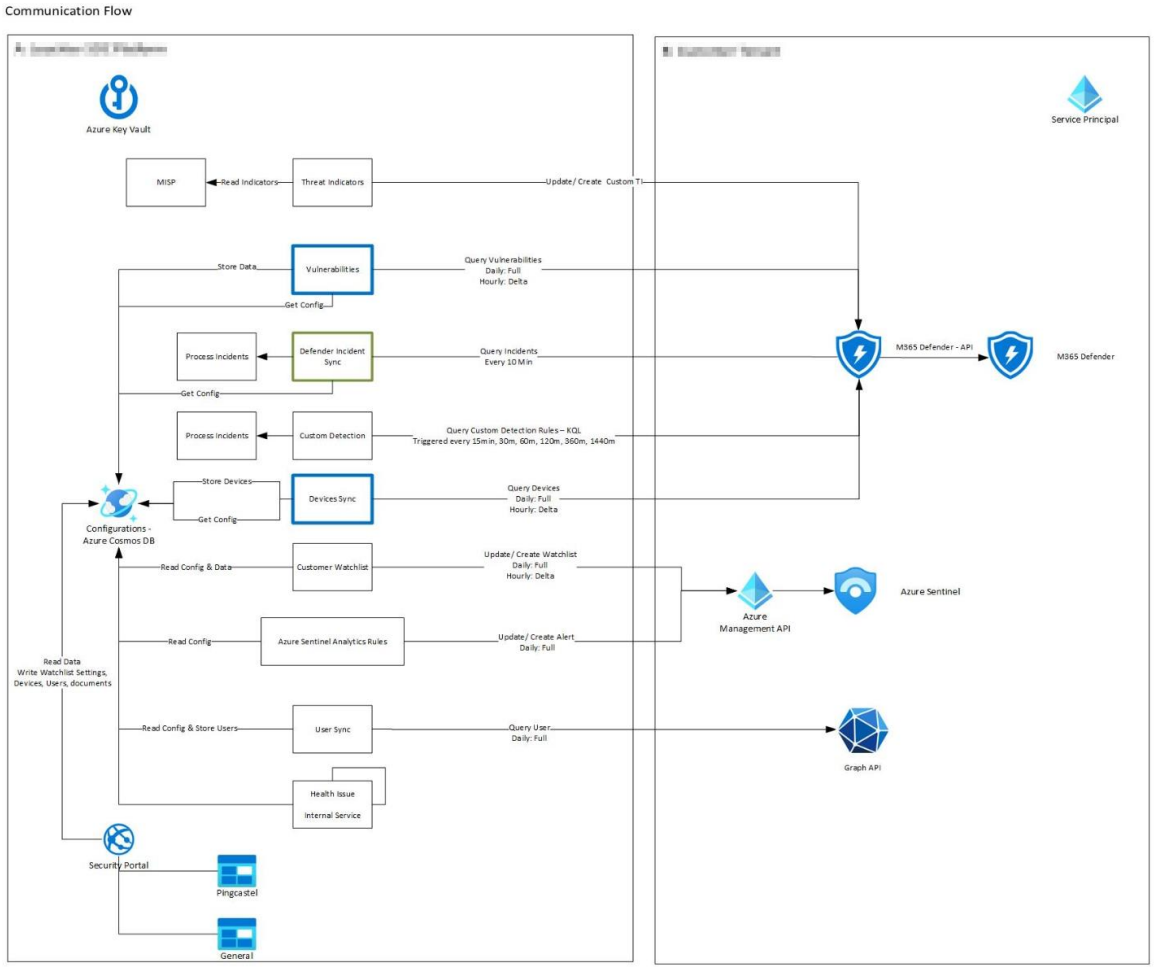
Microsoft Defender for Endpoint «Erkennt»

Microsoft Sentinel «Sammelt»

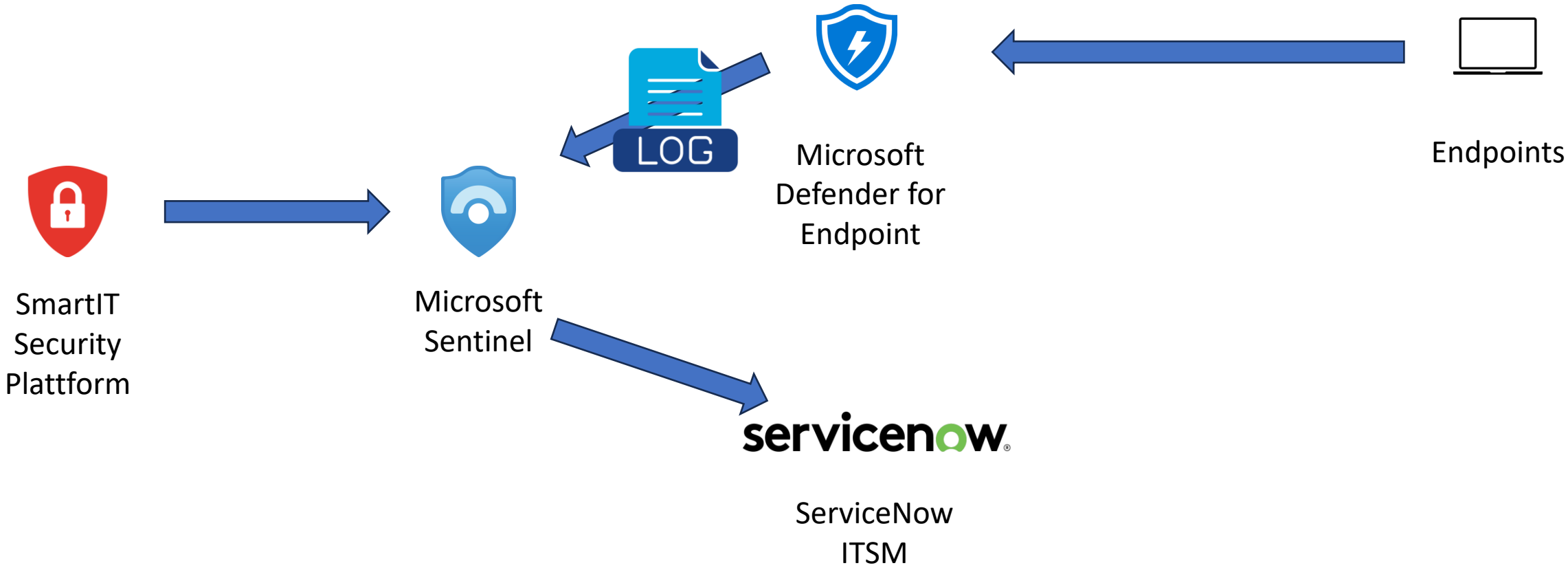
ServiceNow ITSM

SmartIT Security Plattform

SOC Komponenten – Flow 1



SOC Komponenten – Flow 2



Konnektoren

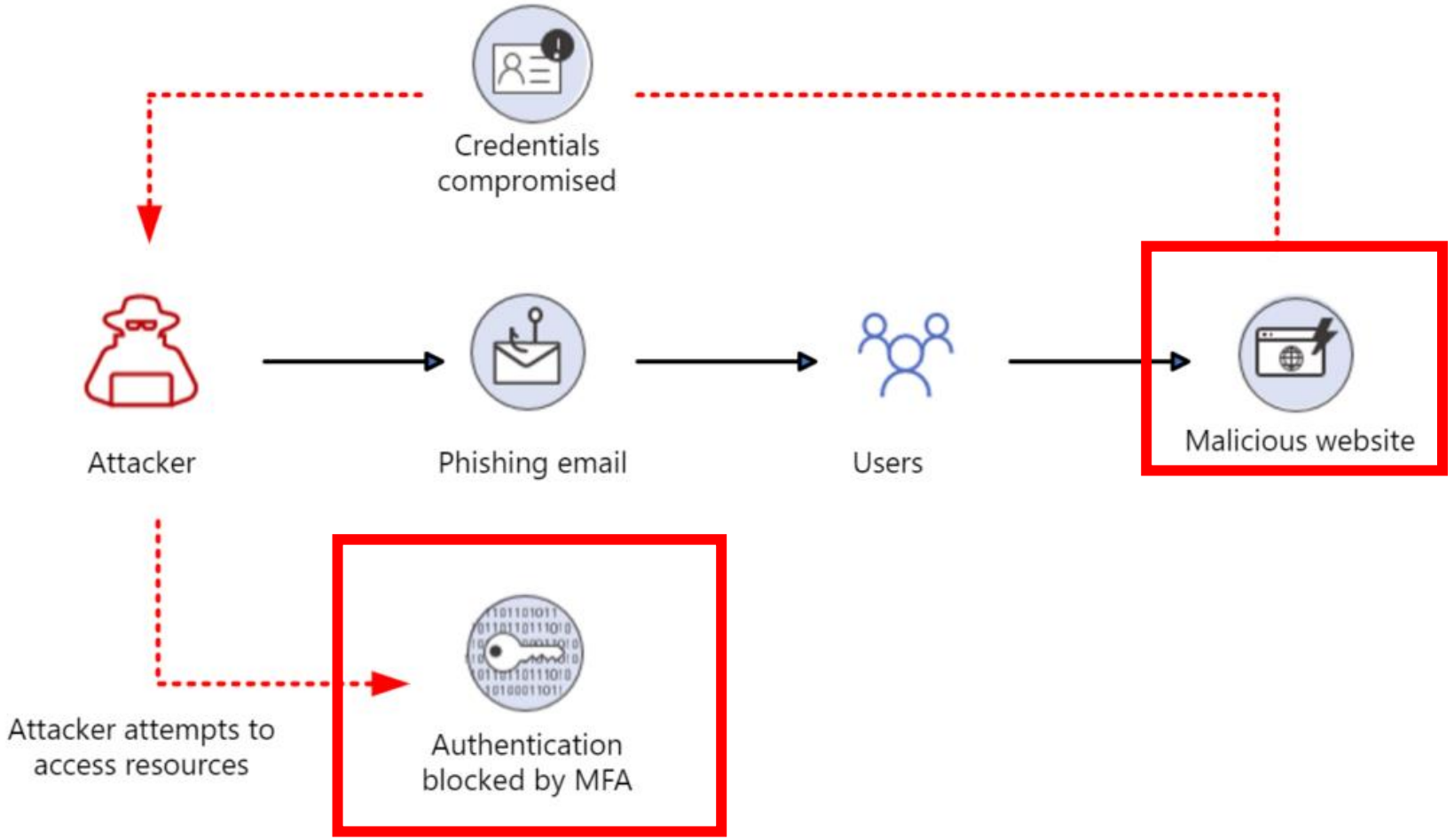
- Active Directory
- Windows Server Security Logs
- Entra ID (Azure AD)
- Microsoft 365 Defender
  - Endpoint
  - Office
  - Identity
  - Cloud Apps
- Azure (Defender for Cloud)
- Threat Intelligence

Glossar

- Phishing
- MFA
- Attacker
- Token = Pass, wer, wohin…
- Domäne

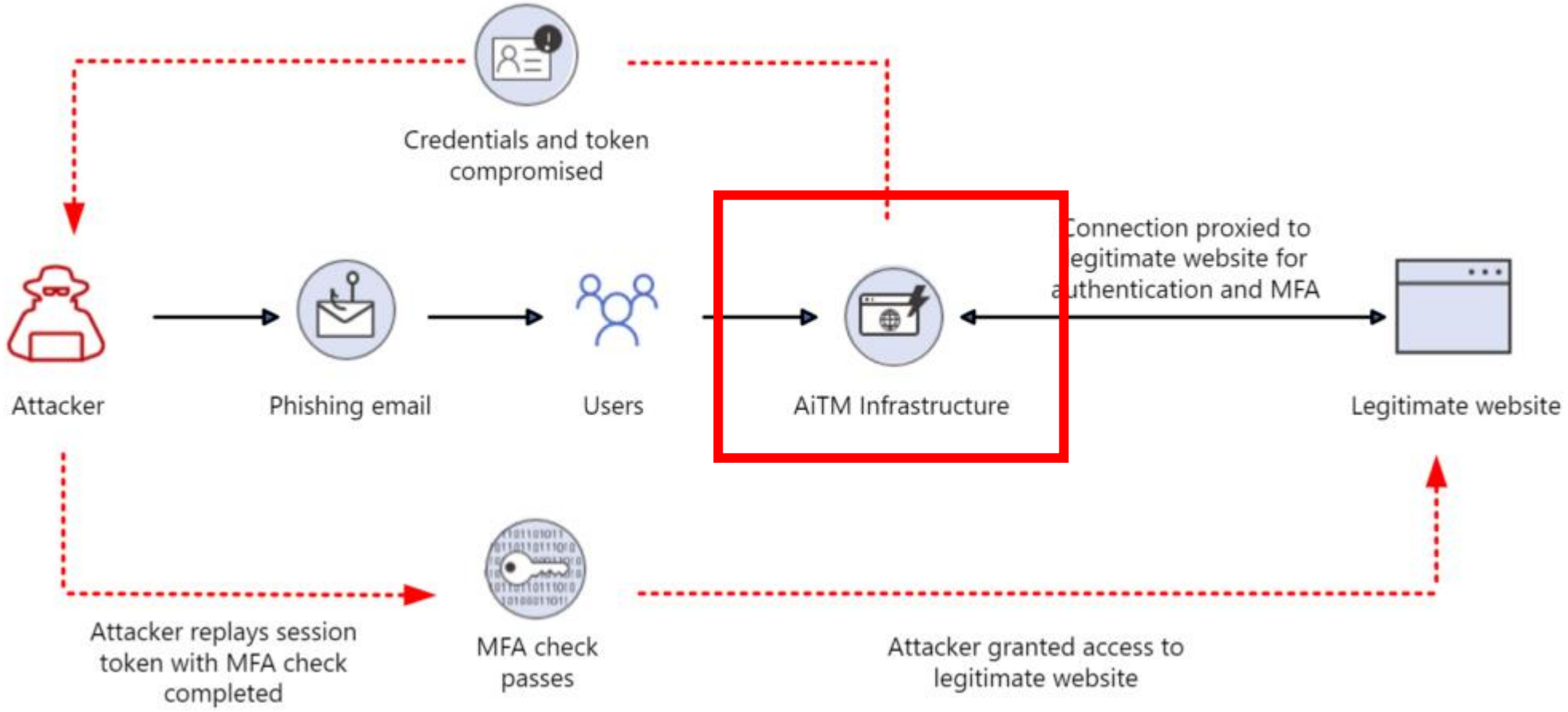
SmartIT

Phishing – Alter Weg



SmartIT

Phishing – adversary-in-the-middle

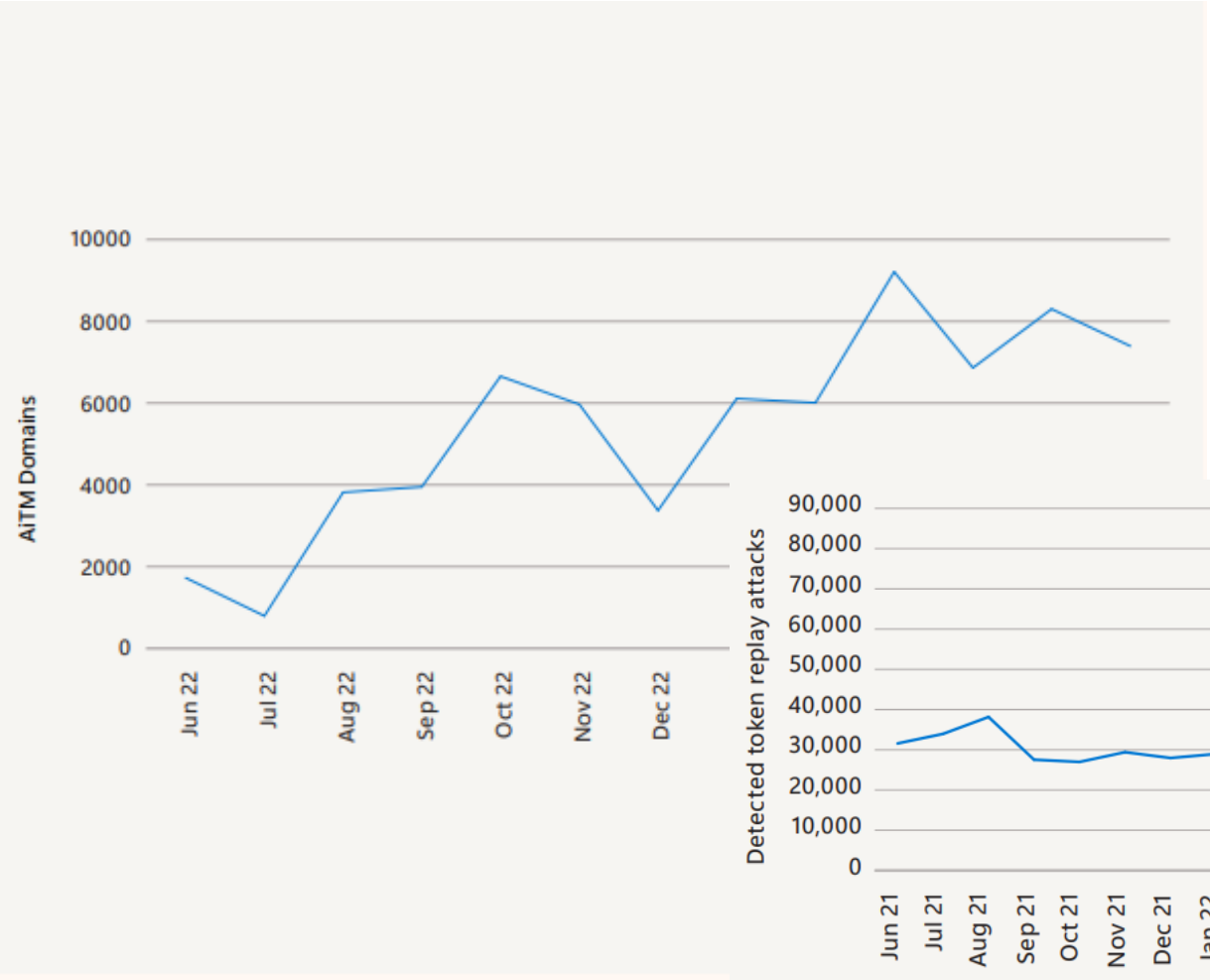


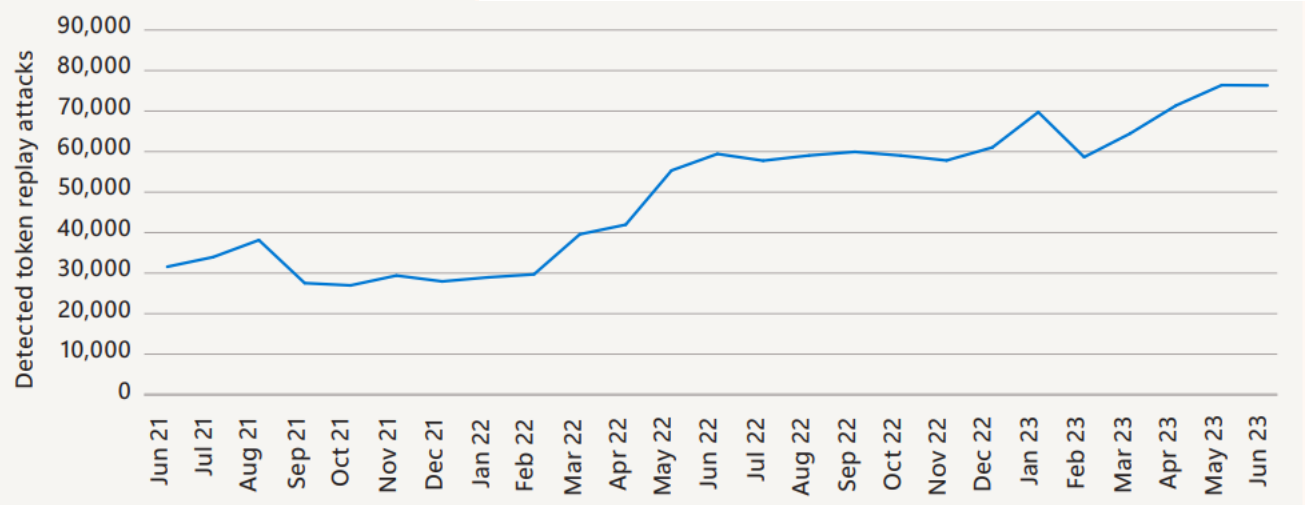
Angriff – Was benötigen wir

- Server = Aitm Infrastructure
- Domänen Name: migrosoftonline.com
- Tool: Evilginx
- Opfer
- Phishing Mail

Demo

Übersicht Microsoft – Digital Defense Report 2023

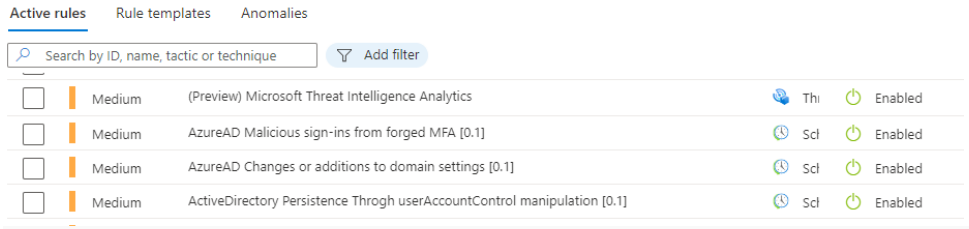


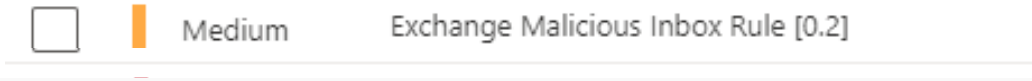


Ablauf SmartIT KMU SOC

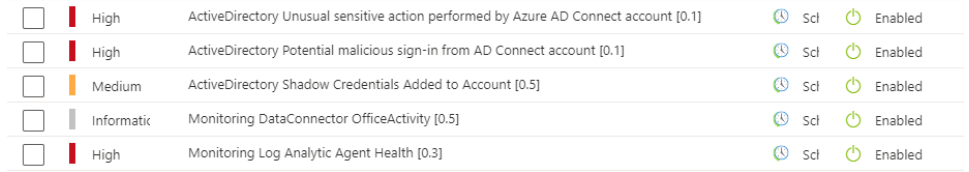
- Angriff wird erkannt
- Incident in Service-Now
- Analyst prüft Alert
- Erst-Massnahmen einleiten

Ablauf SmartIT SOC – Angriff wird erkannt

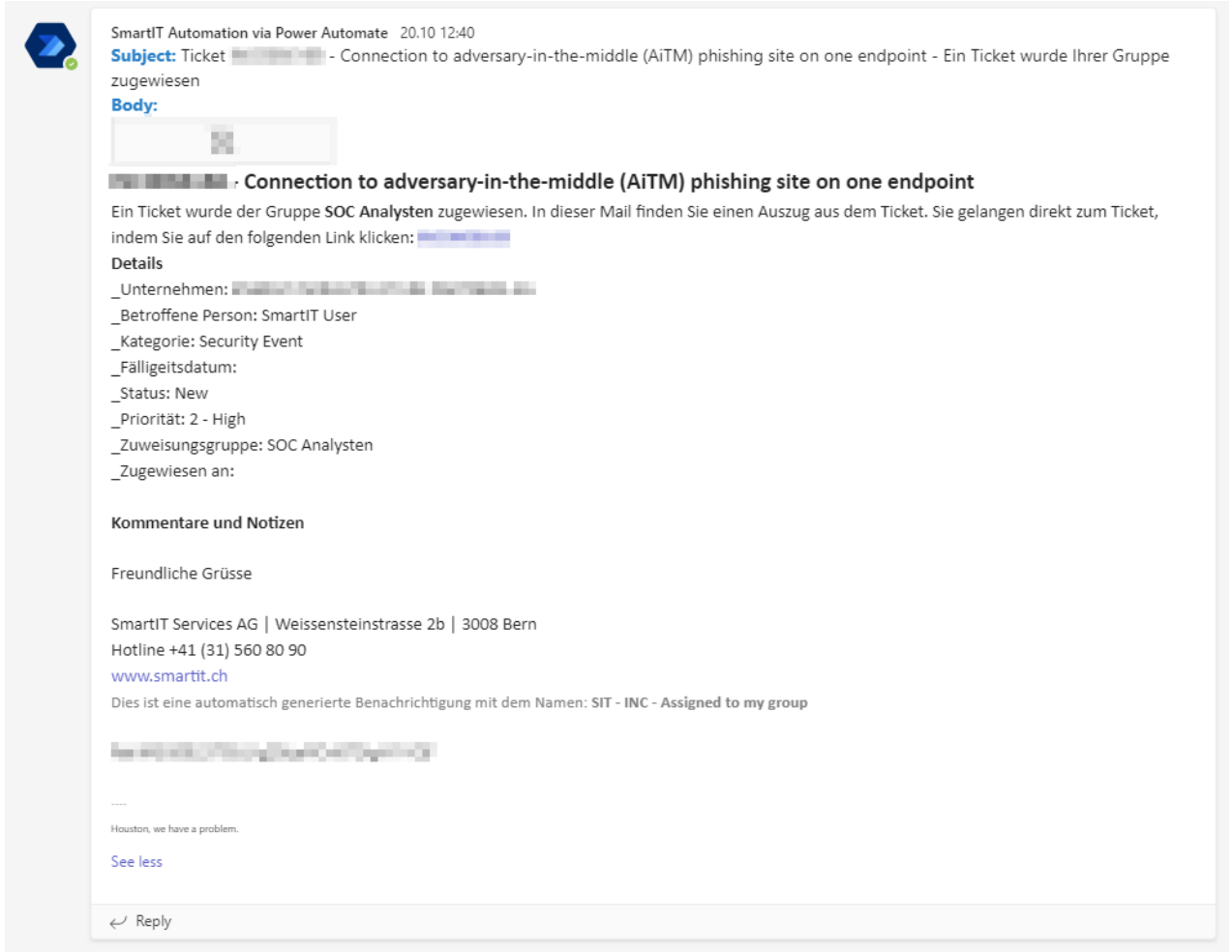





```
let timeframe=1d;
let lookback=0d;
let s_threshold = 20;
let lstring_threshold = 6;
let l_threshold = 3;
SigninLogs
| where TimeGenerated >= ago(timeframe+lookback)
| where OperationName =~ "Sign-in activity"
// Error codes that we want to look at as they are related to the use of incorrect password.
// Not included 50053 Account is locked because user tried to sign in too many times with an incorrect user ID or password.
| where ResultType in ("50126", "50055", "50056","50053")
| where not(ResultDescription contains "Sign-in was blocked because it came from an IP address with malicious activity")
| extend OS = DeviceDetail.operatingSystem, Browser = DeviceDetail.browser
| extend LocationString= strcat(tostring(LocationDetails["countryOrRegion"]), "/", tostring(LocationDetails["state"]), "/", tostring(LocationDetails["city"]))
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated),LocationStringCount=dcount(LocationString), LocationCount=dcount(Location),LocationSet = make_set(
make_set(LocationString),
IPAddress = make_set(IPAddress), IPAddressCount = dcount(IPAddress), AppDisplayName = make_set(AppDisplayName), ResultDescription = make_set(ResultDescription),
Browser = make_set(Browser), OS = make_set(OS), SigninCount = count() by UserPrincipalName
// Setting a generic threshold - Can be different for different environment
| where SigninCount > s_threshold and LocationStringCount >= lstring_threshold and LocationCount >= l_threshold
| extend tostring(LocationSet),tostring(LocationStringSet), tostring(IPAddress), tostring(AppDisplayName), tostring(ResultDescription), tostring(Browser), tostring(OS)
| extend timestamp = StartTime, AccountCustomEntity = UserPrincipalName, IPCustomEntity = IPAddress
```



Ablauf SmartIT SOC – Incident in Service-Now



SmartIT Automation via Power Automate 20.10 12:40

Subject: Ticket [redacted] - Connection to adversary-in-the-middle (AiTM) phishing site on one endpoint - Ein Ticket wurde Ihrer Gruppe zugewiesen

Body:

[redacted] - **Connection to adversary-in-the-middle (AiTM) phishing site on one endpoint**

Ein Ticket wurde der Gruppe **SOC Analysten** zugewiesen. In dieser Mail finden Sie einen Auszug aus dem Ticket. Sie gelangen direkt zum Ticket, indem Sie auf den folgenden Link klicken: [redacted]

Details

_Unternehmen: [redacted]
_Betroffene Person: SmartIT User
_Kategorie: Security Event
_Fälligeitsdatum:
_Status: New
_Priorität: 2 - High
_Zuweisungsgruppe: SOC Analysten
_Zugewiesen an:

Kommentare und Notizen

Freundliche Grüsse

SmartIT Services AG | Weissensteinstrasse 2b | 3008 Bern
Hotline +41 (31) 560 80 90
www.smartit.ch
Dies ist eine automatisch generierte Benachrichtigung mit dem Namen: **SIT - INC - Assigned to my group**

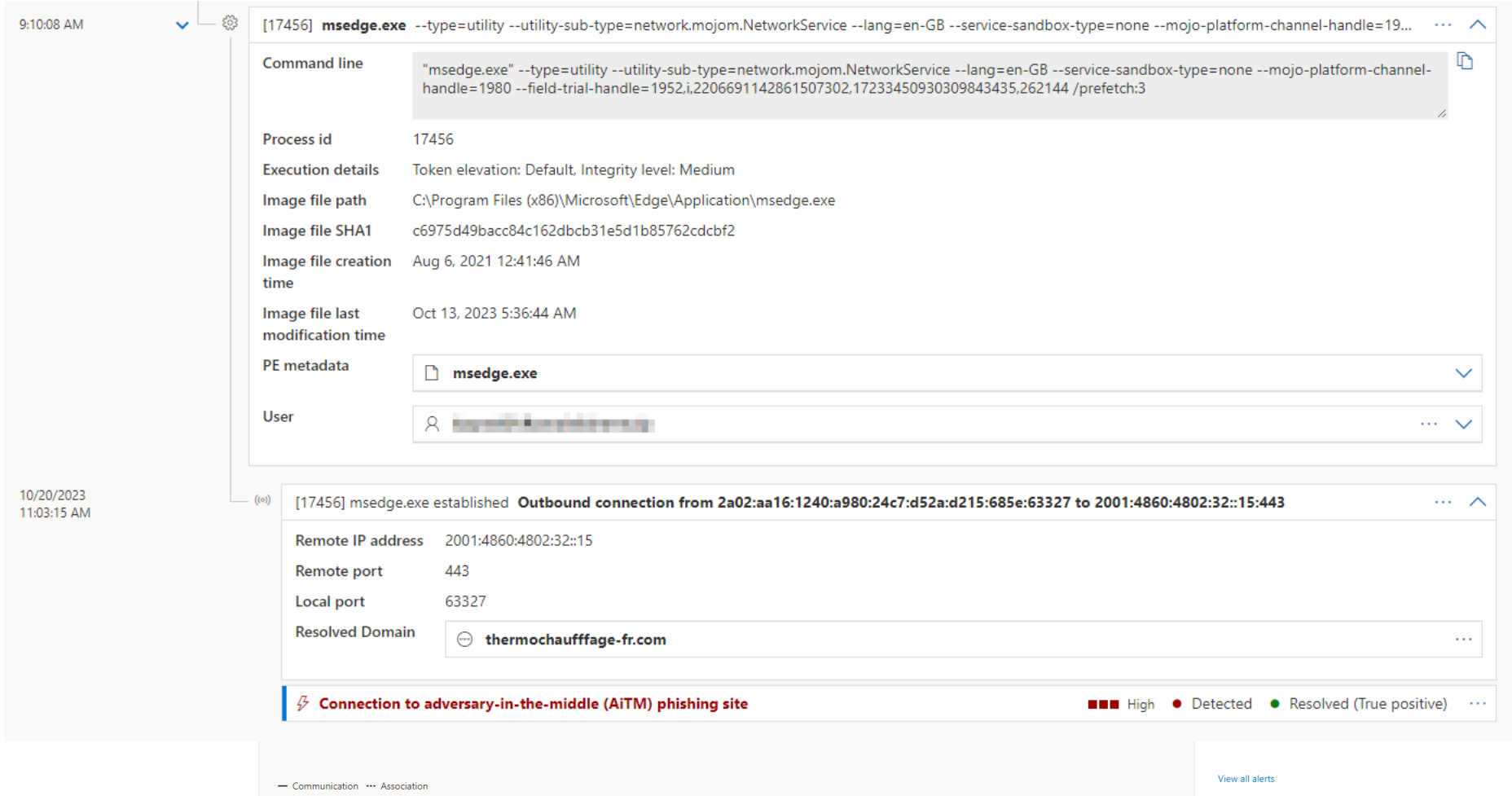
[redacted]

Houston, we have a problem.

See less

Reply

Ablauf SOC – Analyst prüft Alert



Ablauf SOC – Erste Massnahmen

- PlayBooks
  - Critical CVE
  - Ransomware
  - Malicious or Unwanted Software
  - Malware detected
  - Impossible travel activity
  - Unknown Threat
  - Phising / Malware Mail
  - Identity Anonymous Login
  - Identity Compromised
  - Privileged Identity Compromised
  - Token theft [draft]
  - Container Compromised
  - Client or Other Device Compromised
  - Server Compromised
  - Appliance Compromised
  - IP on Blacklist
  - Website on Blacklist
  - Supicious File o. Proccess
  - Suspicious IoC (DNS oder IP)
  - Malicious URL oder Domain

🔥 Containment

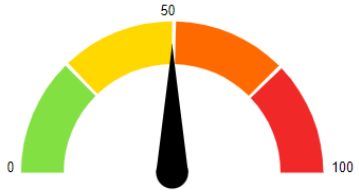
- [ ] Passwort zweimal zurücksetzen. Zuerst mit einem Zufallspasswort, dann mit dem eigentlichen Passwort. `The reason for changing a user's password twice is to mitigate the risk of pass-the-hash, especially if there are delays in on-premises password replication.`
- [ ] Revoke Token *(IIS Reset (Exchange OnPrem oder Azure AD Revoke-AzureADUserAllRefreshToken)* - Zusätzlich im Azure AD Portal unter "Authentication methods" MFA Token revoken
- [ ] Ist VPN / LDAP VPN Konfiguriert müssen diese Logs ebenfalls geprüft werden
- [ ] Prüfen was der Angreifer mit dem Account gemacht hat (Mail Forwarding, Mailbox permission).
  - [ ] im Exchange Weiterleitungen Prüfen `Get-InboxRule -Mailbox examle@example.com | fl`
- [ ] Im Azure AD Portal Authentication methods prüfen und gegeben falls zurücksetzen (wurde eine Mail oder Gerät erfasst das nicht dem Benutzer gehört?)
- [ ] Im Azure AD Portal prüfen in den Audit Logs ob es Änderungen am User Objekt gab
- [ ] Prüfen ob der User App-Registrationen vorgenommen hat.

Prevention - Active Directory Security

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators



Domain Risk Level: 50 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Stale Object : 6 /100 — 2 rules matched

It is about operations related to user or computer objects

Trusts : 0 /100 — 0 rules matched

It is about links between two Active Directories

Privileged Accounts : 45 /100 — 3 rules matched

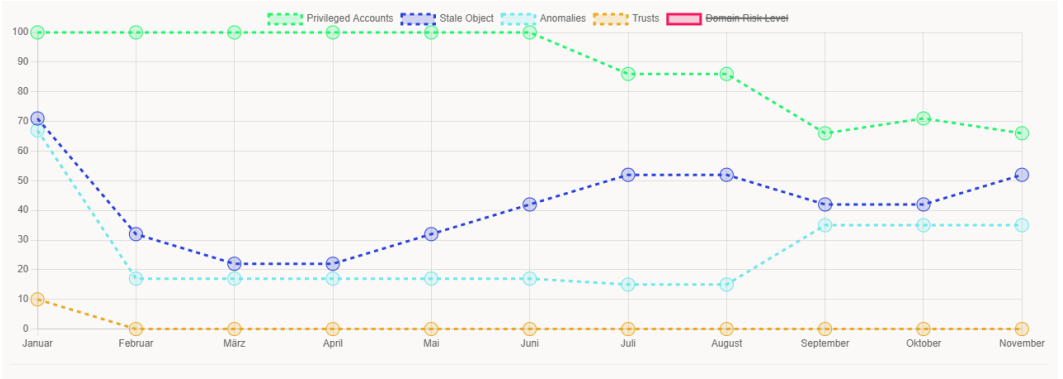
It is about administrators of the Active Directory

Anomalies : 50 /100 — 9 rules matched

It is about specific security control points

Risk model

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket



Prevention - Security Audit

- Übersicht zum aktuellen Stand
- Massnahmenkatalog zur Verbesserung

4.1 Azure AD Security

Azure Active Directory (Azure AD) ist ein cloudbasierter Dienst zur Identitäts- und Zugriffsverwaltung. Mit diesem Dienst können Personen auf externe Ressourcen wie beispielsweise Microsoft 365 zugreifen.

Komponente	Referenz-nummer	Befund	Schweregrad	Massnahmenvorschlag
*Azure MFA Admin*accounts	SEC1291	Aktuell ist für sämtliche Benutzerkonten MFA nicht aktiviert. Für die Anmeldung ist einzig Benutzername und Passwort notwendig.		MFA muss bei sämtlichen administrativen Benutzerkonten aktiviert werden, um ein Missbrauch der Berechtigungen vorbeugen zu können.
Azure MFA User	SEC1028	Aktuell ist für sämtliche Benutzerkonten MFA nicht aktiviert. Für die Anmeldung ist einzig Benutzername und Passwort notwendig.		MFA muss an sinnvollen, öffentlich erreichbaren Stellen (bspw. Exchange online) für sämtliche Benutzerkonten aktiviert werden.
Limit endpoint access to privileged AD accounts	SEC1015	Aktuell ist eine Anmeldung mit einem Global-Administrator auch auf einen gewöhnlichen Client möglich. Entsprechende Vorkehrungen wurden keine getroffen.		Der Zugriff auf ungeschützte Endpunkte (Clients) muss durch entsprechende Richtlinien (GPO / Intune) verhindert werden.
Azure AD Security Basis	SEC1030	Die aktuelle Konfiguration entspricht nicht dem aktuellen Sicherheitsstandard. Beispielsweise können alle Benutzer Geräte in Azure AD hinzufügen, MFA ist nicht aktiviert usw.		Sicherheitseinstellungen im Azure AD gemäss dem Standard vornehmen und umsetzen.

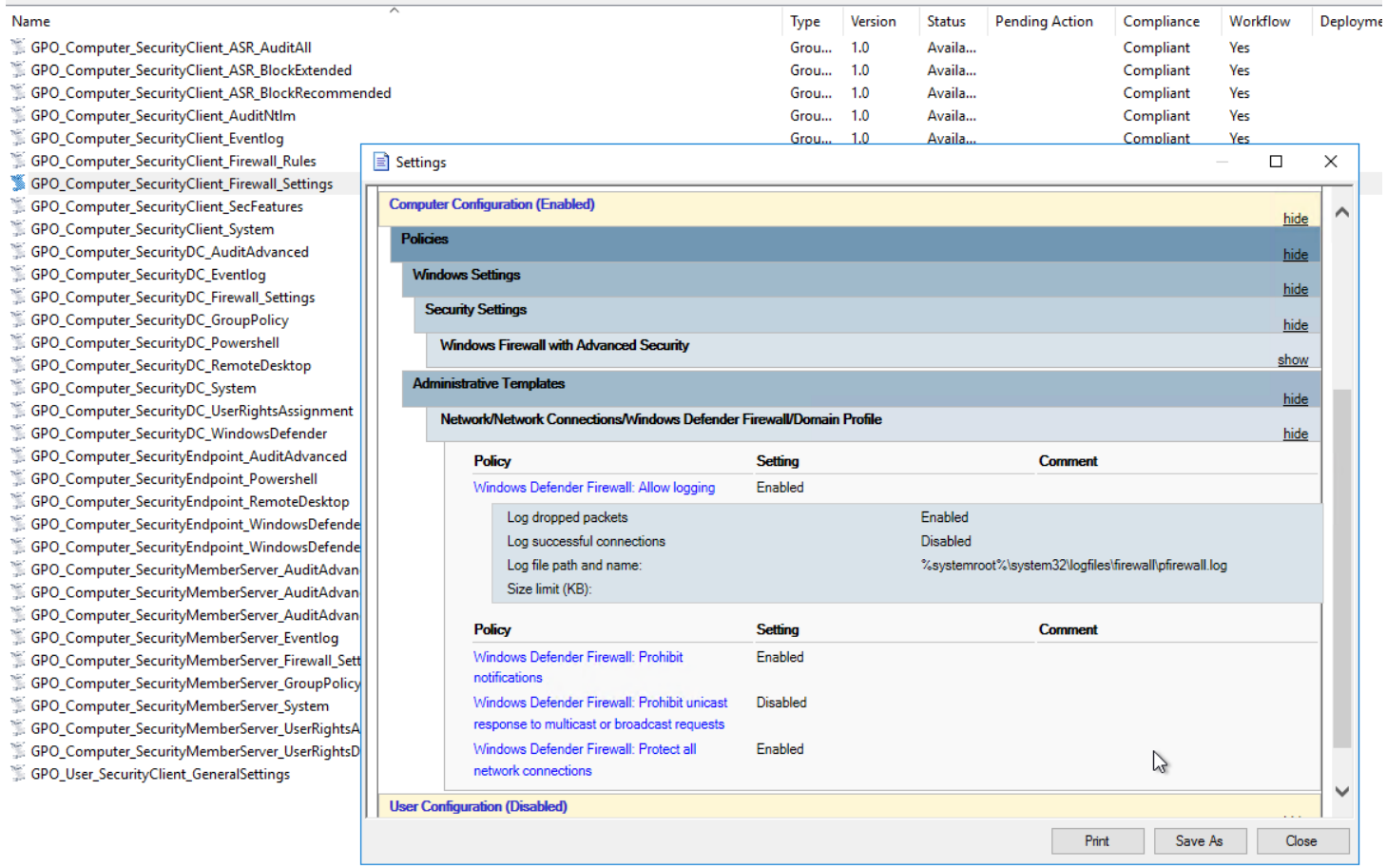
4.2 Windows Client

Windows Client bezieht sich auf sicherheitsrelevante Themen im Zusammenhang mit Windows Clients (Notebook/Desktop). Windows Clients werden von den Mitarbeitenden für die alltägliche Arbeit verwendet.

Komponente	Referenz-nummer	Befund	Schweregrad	Massnahmenvorschlag
Restricing priviledged ac-	SEC1280	Aktuell nicht gegeben, da Benutzer mit administrativen Rechten die		Getrennte Accounts erstellen und verwenden. Im Alltag "normale" Benut-

Prevention - Hardening

- Settings (Onprem + Cloud)
- Basierend auf Microsoft und CIS Baselines



Fragen & Diskussion