SmartIT Services AG

# Managed Security Operations Center speziell für KMU

powered by SmartIT

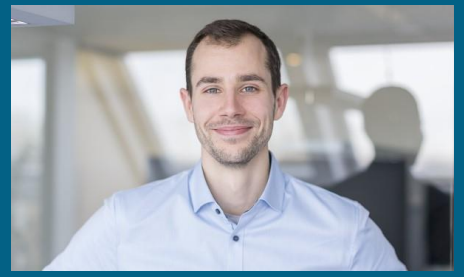
# Security Operations Center für KMU

**Kristian Hachen**
k.hachen@smartit.ch

**Head of Marketing + Communications**

**Aladin Steiner**
a.steiner@smartit.ch

**Head of Value Stream Azure & Datacenter**
**Service Owner Security Operations Center**



**Martin Schmidli**
m.schmidli@smartit.ch

**Senior System Engineer**
**Security Operations Center Analyst**

# Themenschwerpunkte

- **Bedrohungslage**
  Warum Cyber-Sicherheit wichtig ist
- **KMU Security Operations Center SmartIT**
  Welchen Mehrwert bieten wir mit KMU SOC
- **Praxisbeispiel**
  Adversary in the Middle Attack (AITM)
- **Angebot**
  Sicherheit als Managed Service zum monatlichen Preis

SmartIT

# Bedrohungslage 2024

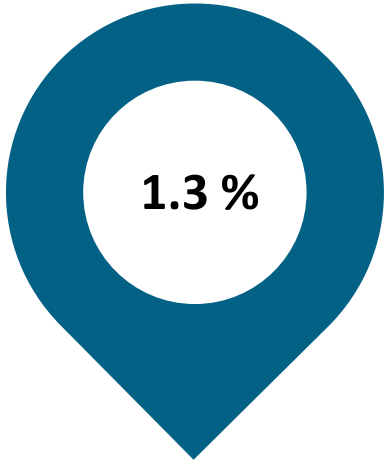
## Warum Cyber-Sicherheit wichtig ist

## Was hat sich in den letzten Jahren aus unserer Sicht verändert?


Registrierte Meldungen beim Bundesamt für Cybersicherheit (BACS) im Jahr 2023


Gemeldete (erfolgreiche) Cyberangriffe pro Woche KW44 2023 (BACS)


Finanzieller Schaden pro Jahr durch Cyberkriminalität in der Schweiz




Beträgt die Aufklärungsrate bei Ransomware-Fällen

Im Schnitt dauert es 23 Tage, den grundlegenden Betrieb nach einem weitreichenden Ransomware Angriff wiederherzustellen.

Die Wiederherstellung der gesamten IT-Systeme und vollen Funktionsumfangs kann Monate dauern.

# Die Phasen eines Cyberangriffs

SmartIT

# KMU Security Operations Center

## Welchen Mehrwert bieten wir mit KMU SOC

# Managed SOC Service Leistungen

Echtzeitüberwachung Ihrer Systeme*
durch SmartIT SOC rund um die Uhr

Vorbeugung, Erkennung, Analyse und
Beseitigung von Sicherheitsvorfällen

Erstreaktion auf Sicherheitsvorfälle durch SmartIT
Security Operation Center Analysten

Analysten „in Charge“ von Montag-Freitag
07.00-18.00 Uhr*

Zugang zu SOC-Dashboard für Kunde
(Servicenow & SOC Dashboard)

Regelmässige Reports und Besprechung der aktuellen
Incidents

Kalkulierbare Kosten durch monatlichen Fixpreis

# SmartIT Security Operations Center 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

Vs.

## 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 BACS**
- Managed Service zum monatlichen Preis
- **Gemeinsam im Team agieren**
- Technologisch vorne mit dabei
- Integration in bestehende Prozesse und Service NOW Anbindung

Extern

Nicht im Kundenteam

Nicht auf KMU ausgelegt

Betriebs- und Prozessnah

Proaktive Stärkung durch Sicherheits-experten

Wachsam und Verteidigungs-bereit

# Verantwortlichkeiten werden gemeinsam im Team Kunde-SmartIT definiert

## Kompetenzen

| Kompetenz | Verantwortung | | | Bemerkung |
|---|---|---|---|---|
| | SmartIT selbstständig | SmartIT in Absprache mit Kunde | Kunde | |
| Auf sämtliche öffentlichen IP Adressen des Kunden darf zum identifizieren von Schwachstellen regelmässig ein Attack Surface Scanner ausgeführt werden | ✓ | | | |
| Es darf eine Eicar-Datei (ungefährliche Datei, welche den Antivirus auslöst) auf der Umgebung vom Kunden verteilt werden. | ✓ | | | |
| Endbenutzer kontaktieren und nachfragen welche Tätigkeit ausgeführt wurde | | ✓ | | |
| Endbenutzer kontaktieren und via Teamviewer Analysen durchführen | | ✓ | | |
| Full Antivirus Scan auf einem Endgerät oder Server starten | ✓ | | | |
| Automation Investigation auf einem Endgerät oder Server starten | ✓ | | | |
| Live Response auf einem Endgerät oder Server selbständig durchführen | ✓ | | | |
| Compromised Scan mit Kostenloser Third Party Software durchführen | | ✓ | | |
| Isolierung von einem potenziell infizierten Endgerät | ✓ | | | |
| Isolierung von mehreren potenziell infizierten Endgeräten | ✓ | | | |
| Isolierung von allen Endgeräten | | | ✓ | |

# Technik
## Aufbau SOC & Komponenten

## SOC Komponenten

Endpoints
«Generieren
Logs»

Microsoft
Defender for
Endpoint
«Erkennt»

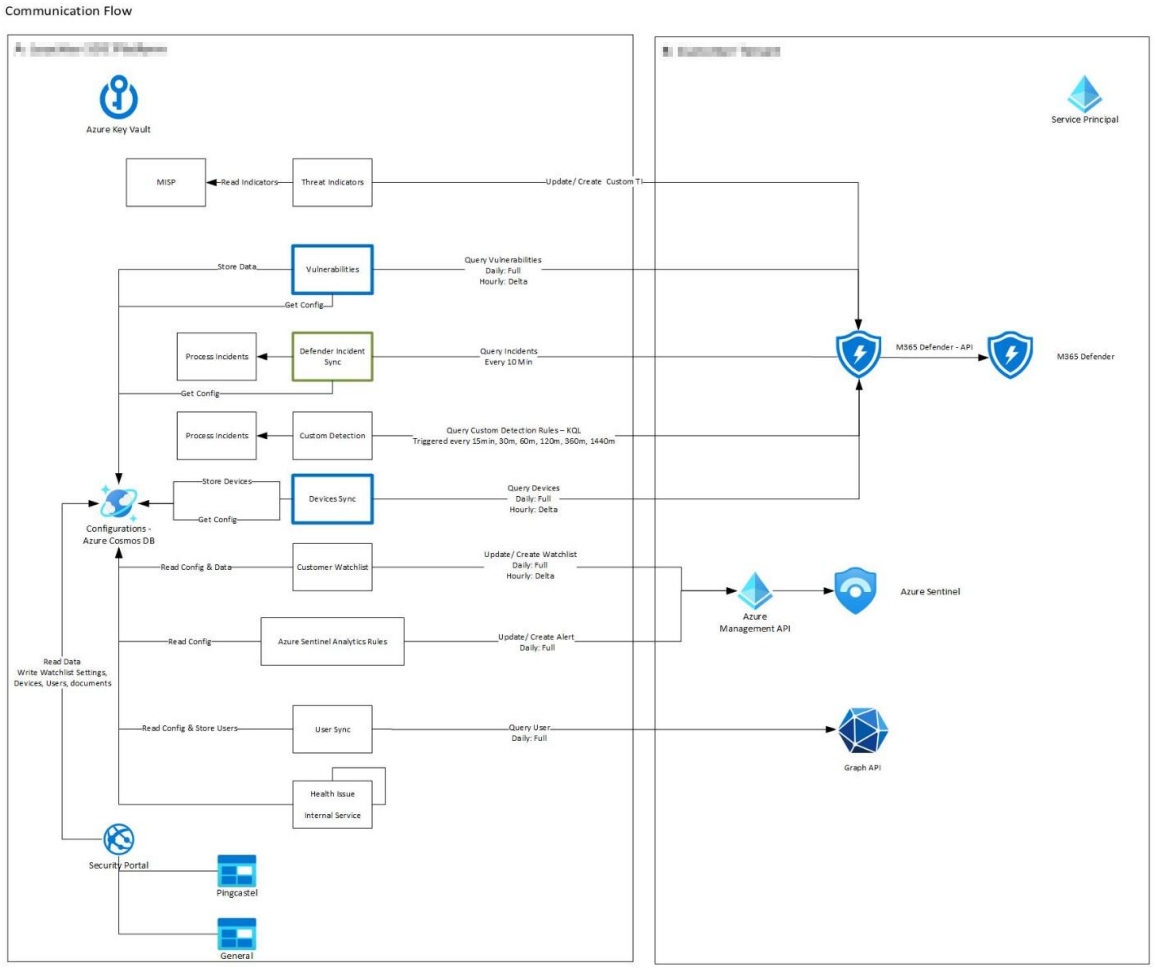
Microsoft
Sentinel
«Sammelt»

servicenow

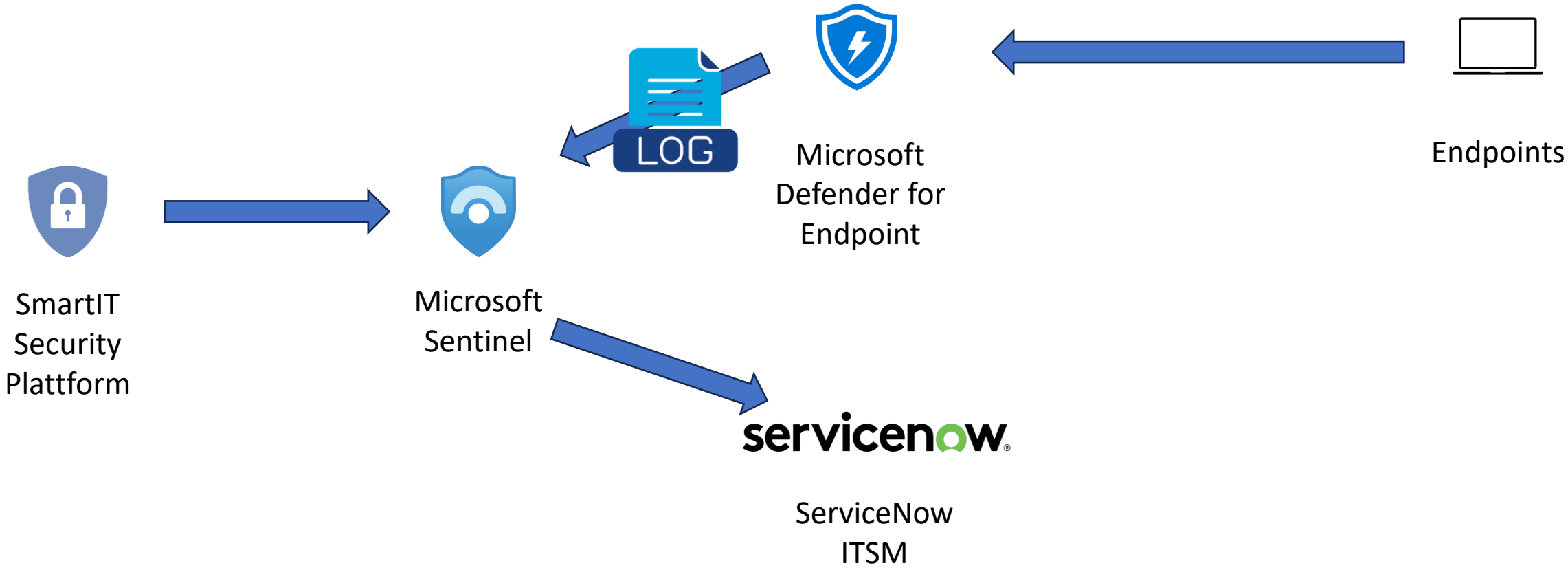
ServiceNow
ITSM

SmartIT
Security
Plattform

# SOC Komponenten – Flow 1



## SOC Komponenten – Flow 2



## Datenquellen

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

SmartIT

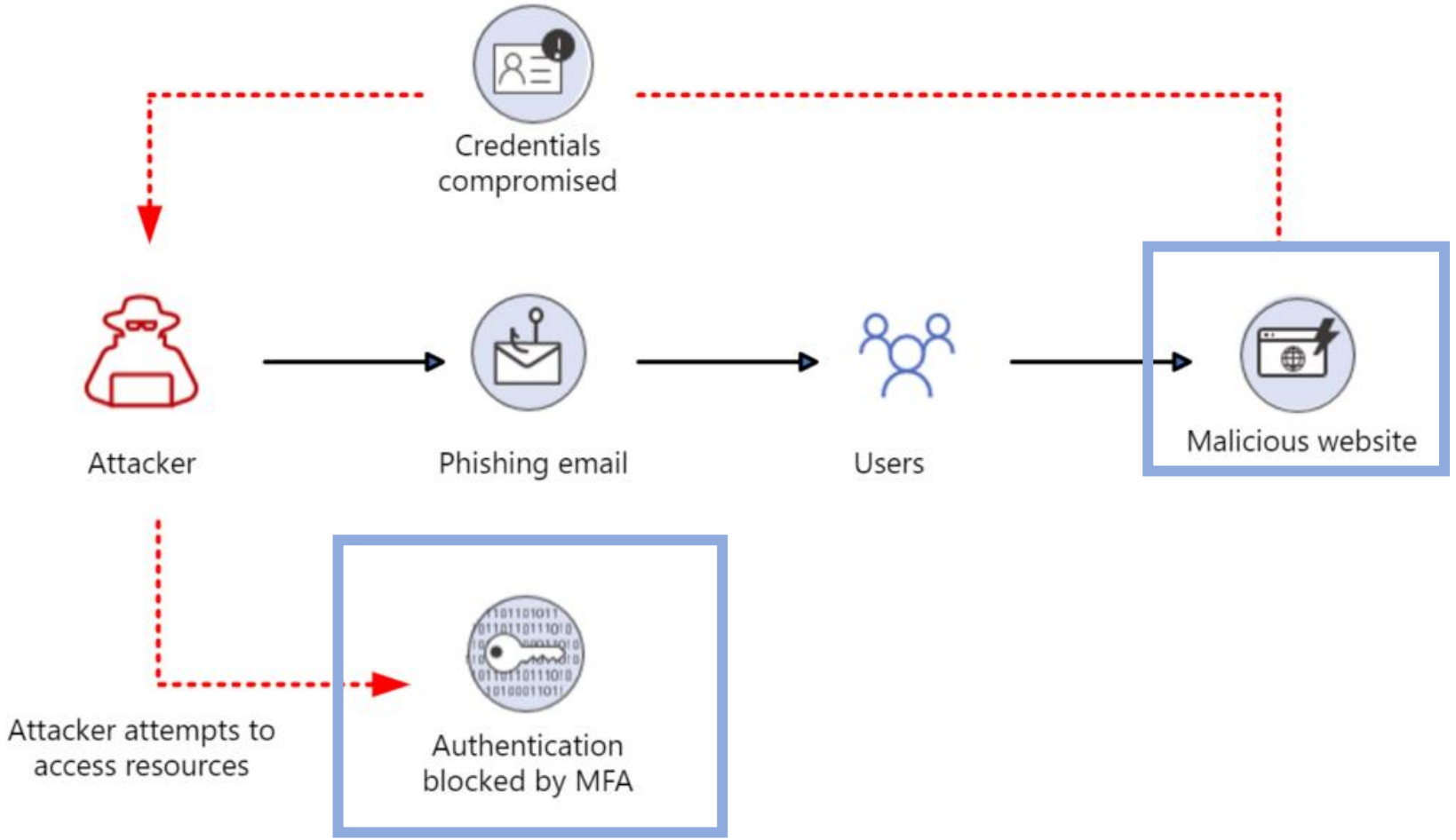
# Praxisbeispiel
## Adversary in the Middle Attack (AiTM)

## Glossar

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

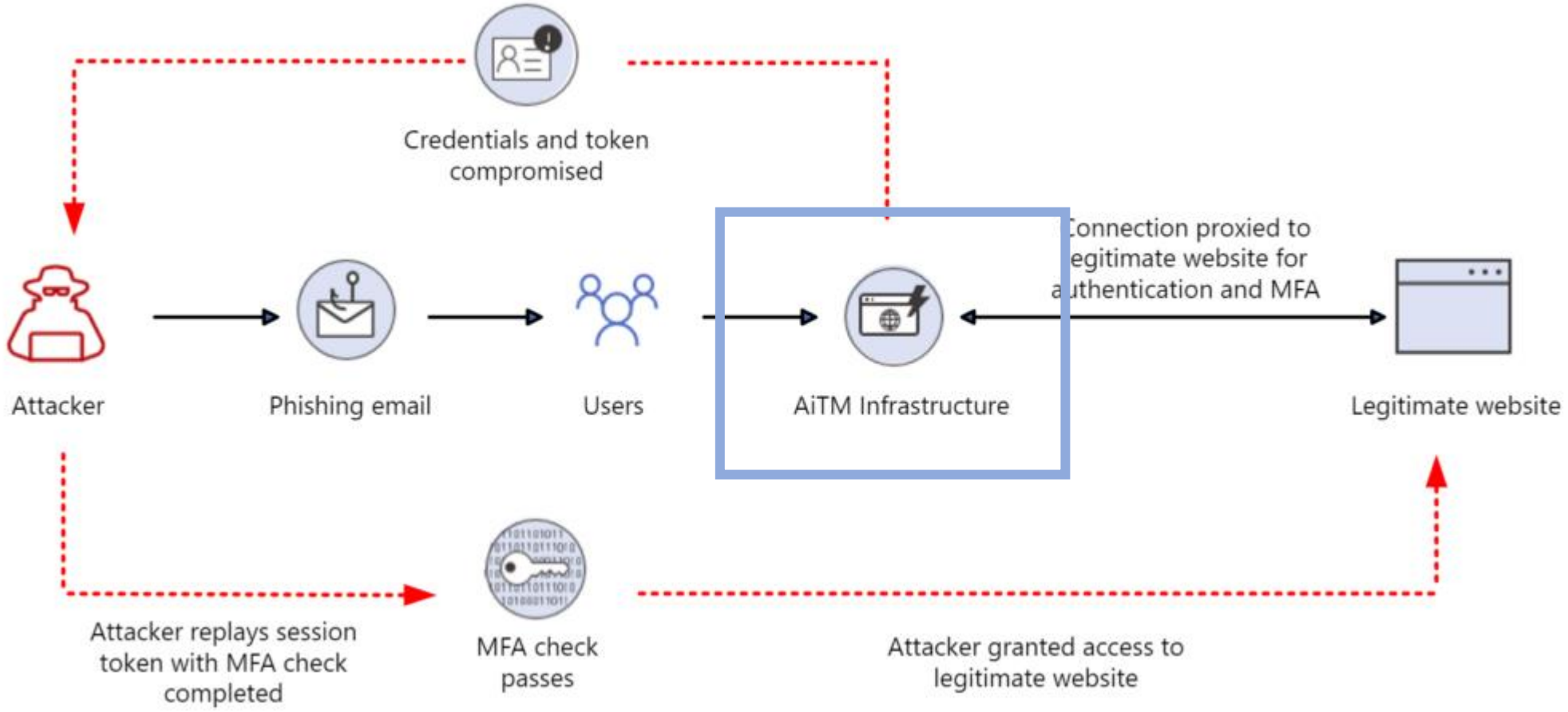
SmartIT

# Phishing – Alter Weg



SmartIT

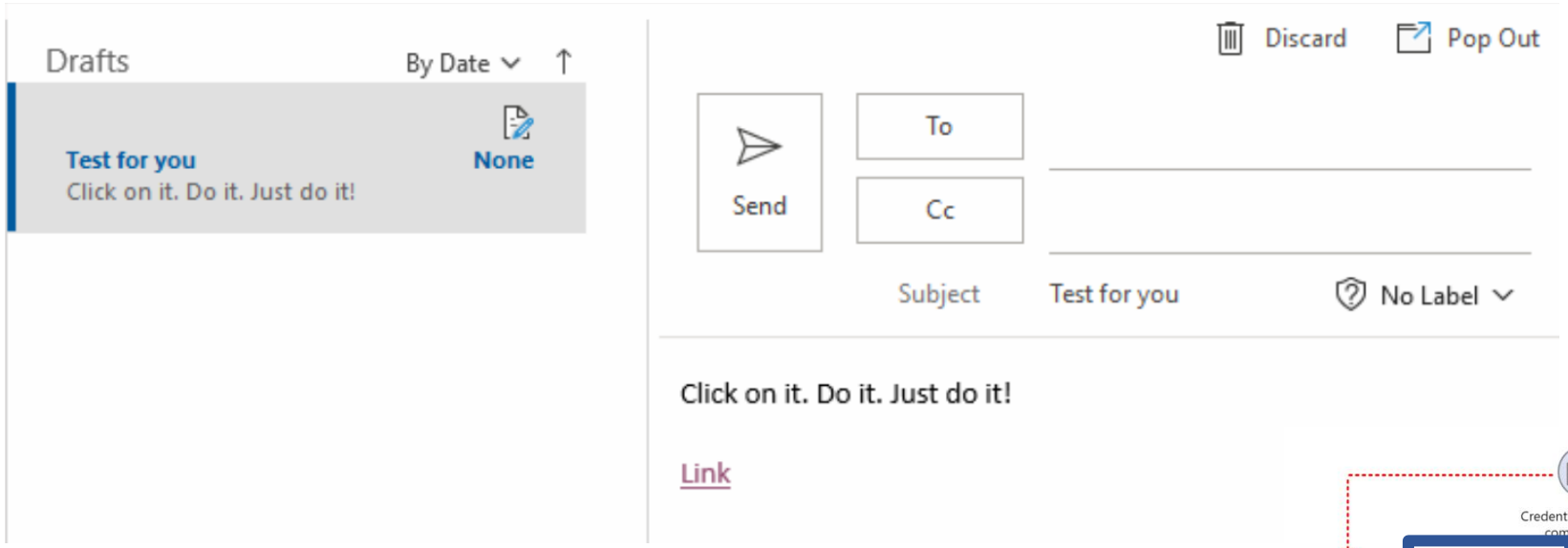
# Phishing – AiTM adversary-in-the-middle

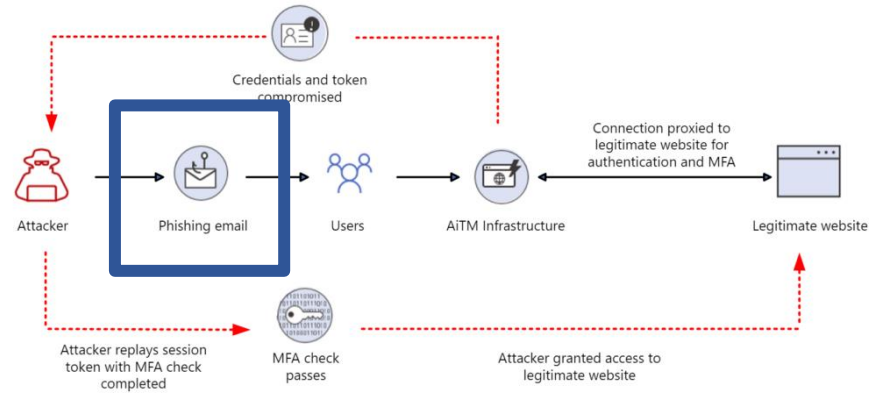


## Angriff – Was benötigt der Angreiffer?

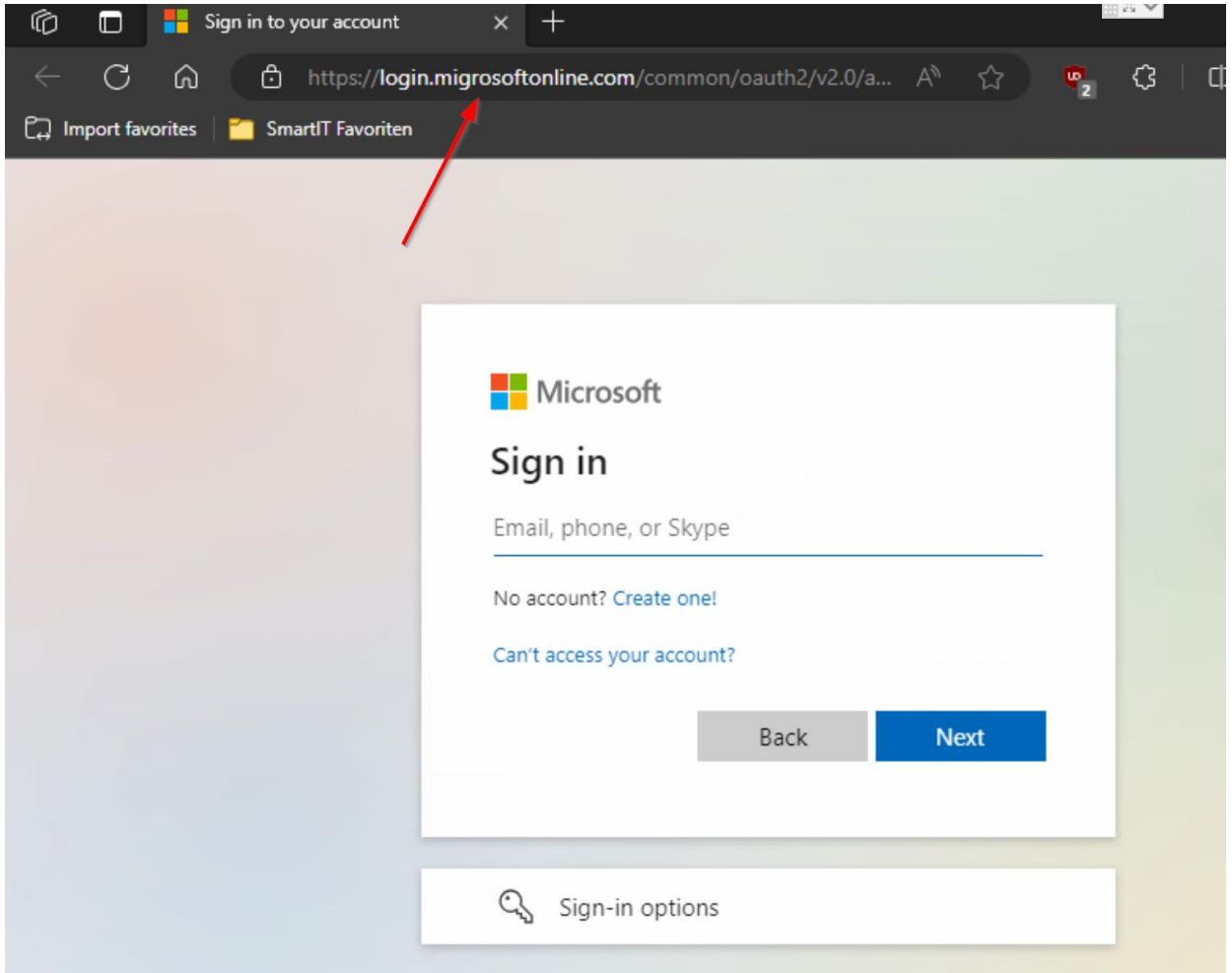
- Server = AiTM Infrastructure
- Tool: Evilginx
- Domänen Name: migrosoftonline.com
- Opfer
- Phishing Mail

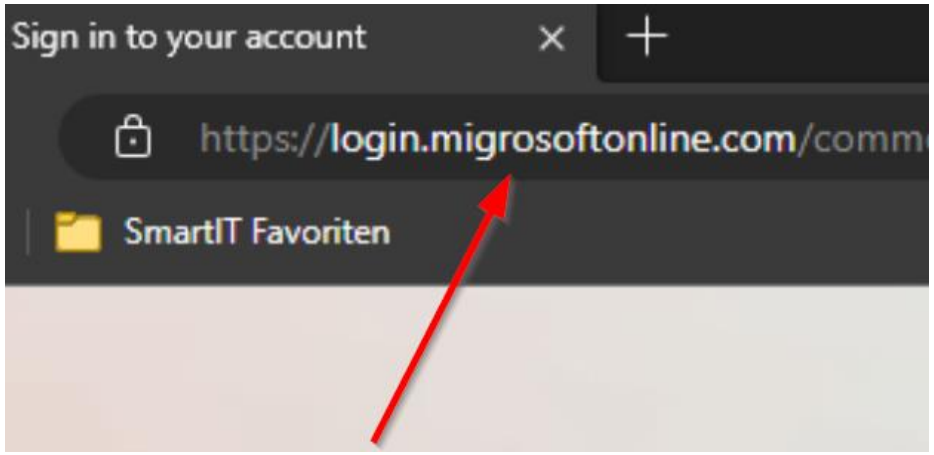
# Schritt 1 - Phishing Mail

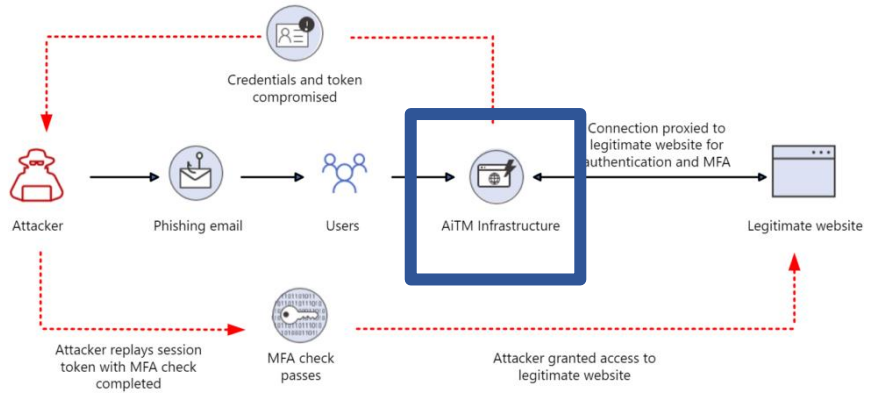


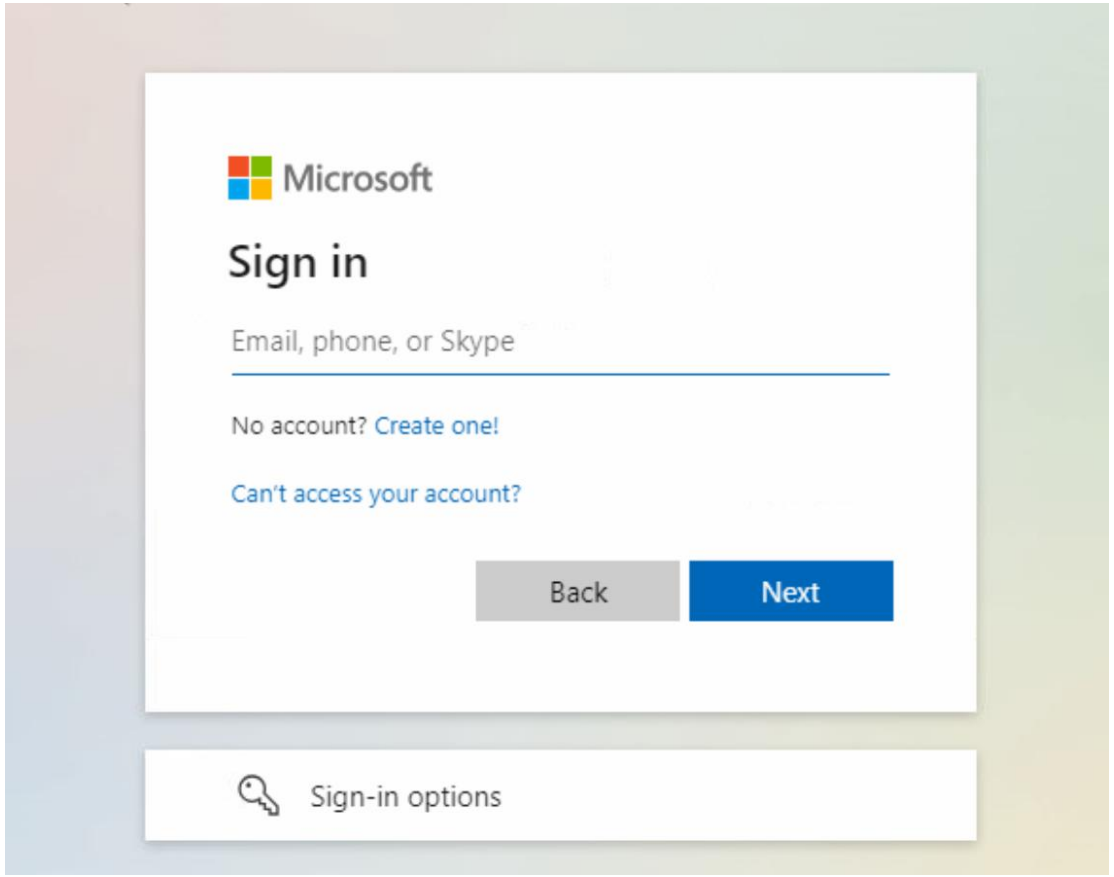
# Schritt 2 – “Fake Seite” – AiTM Infrastructure

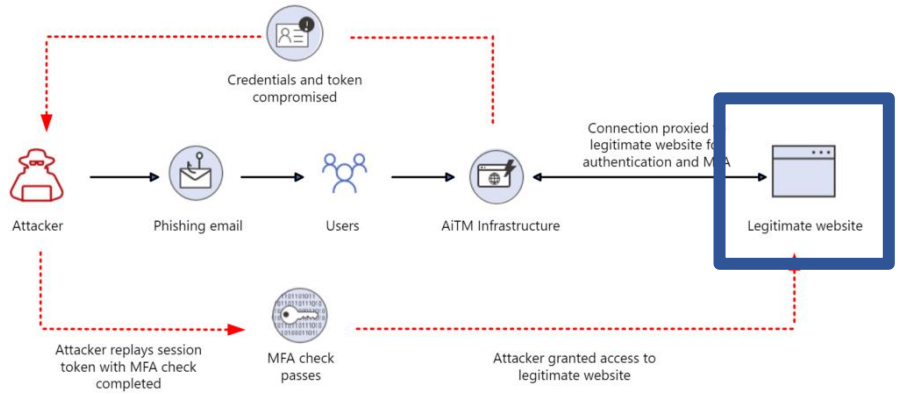


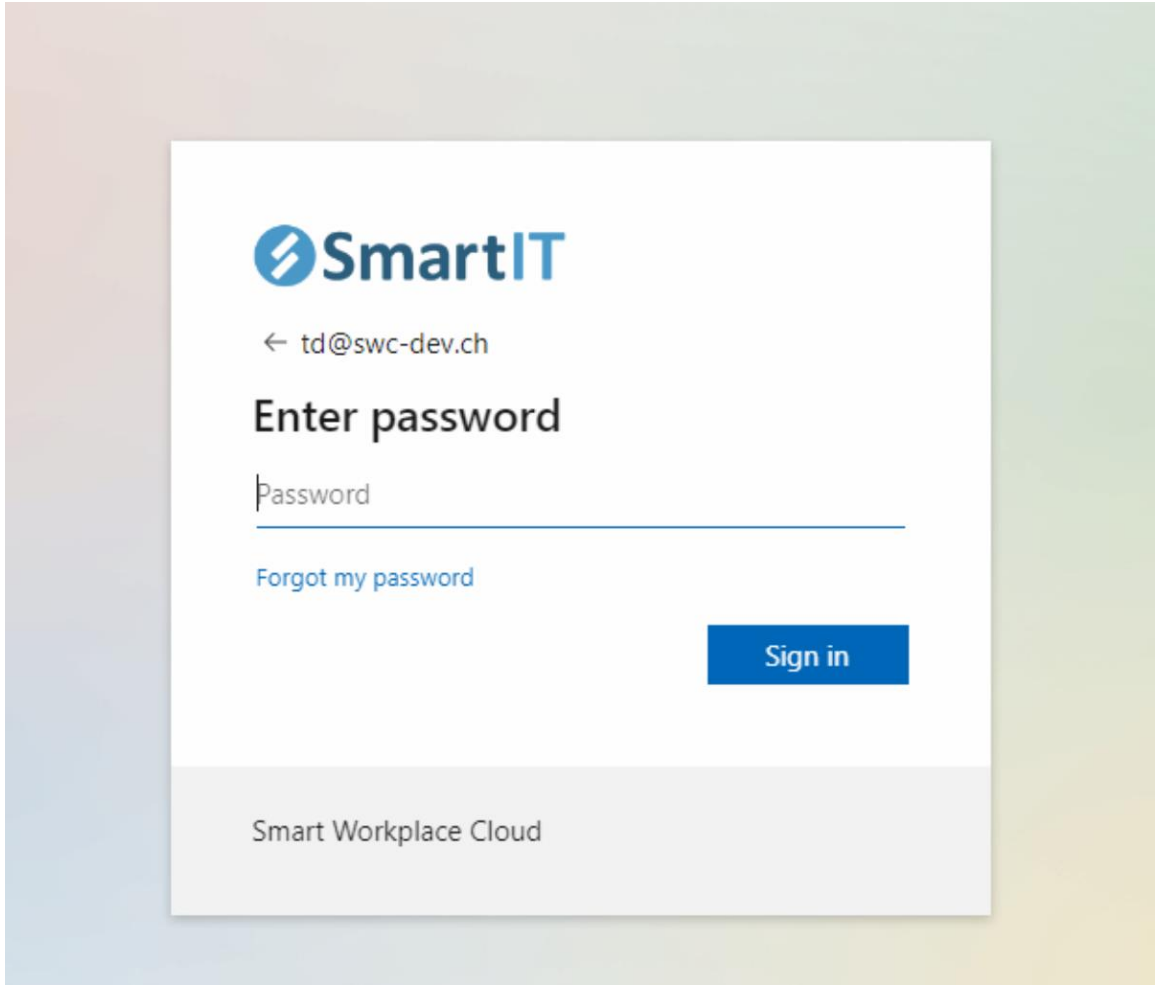



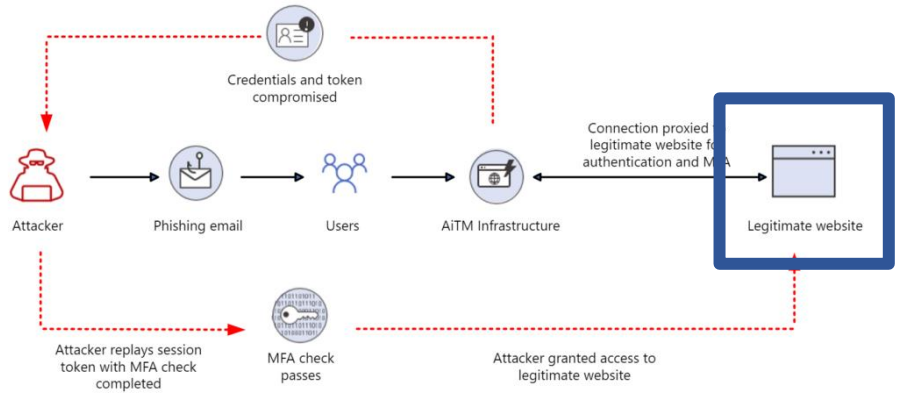
# Schritt 3 – Legitime Webseite



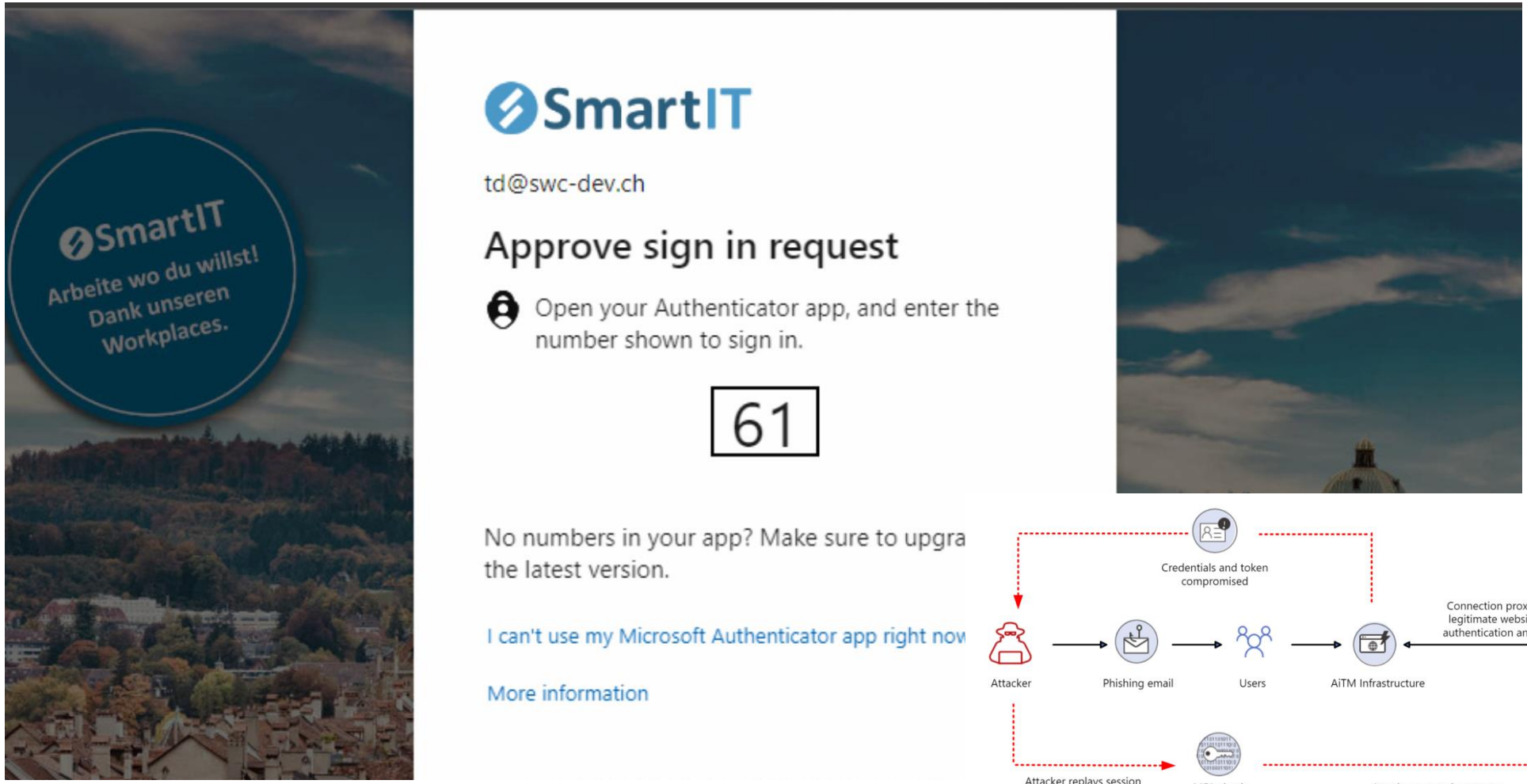



# Schritt 3 – Legitime Webseite

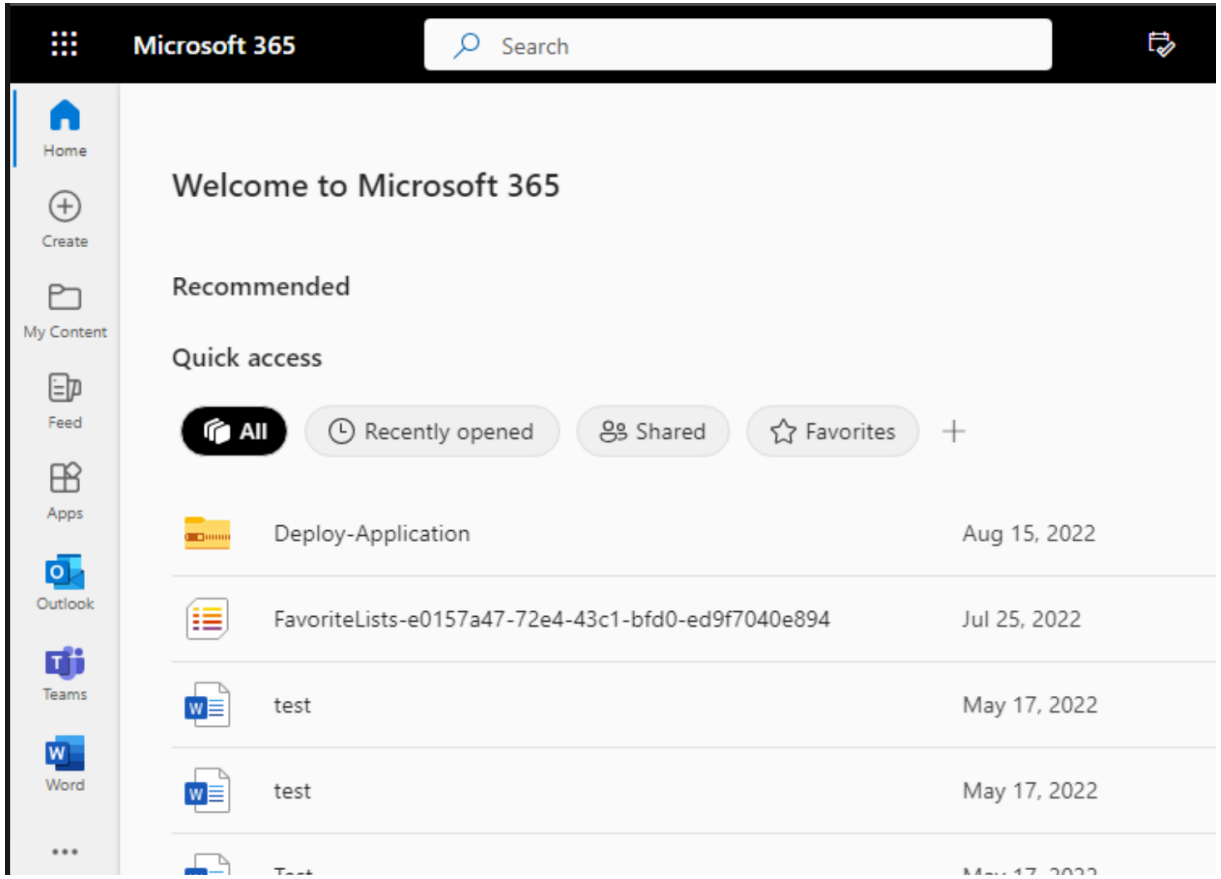


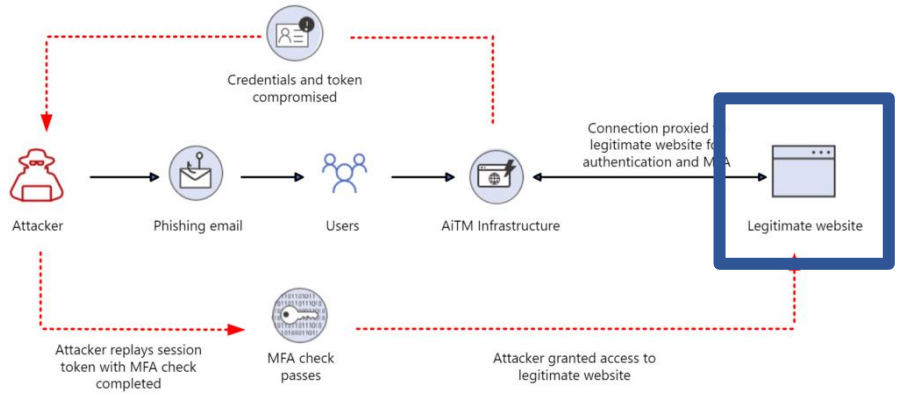



# Schritt 3 – Legitime Webseite



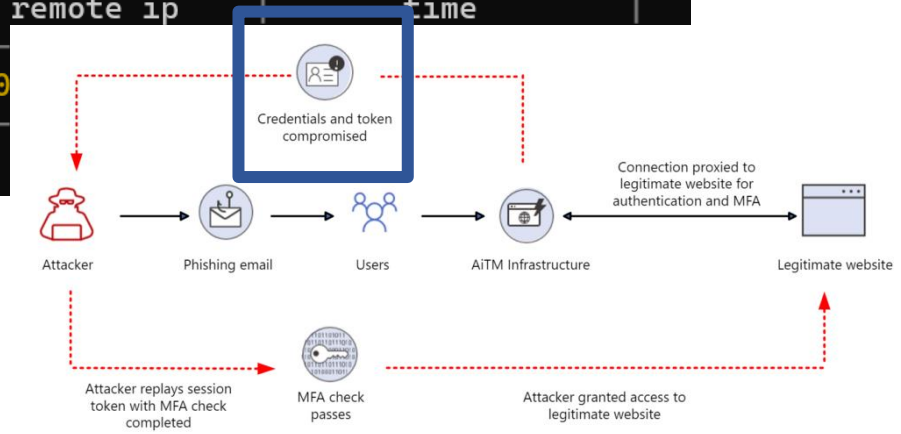
# Schritt 3 – Legitime Webseite



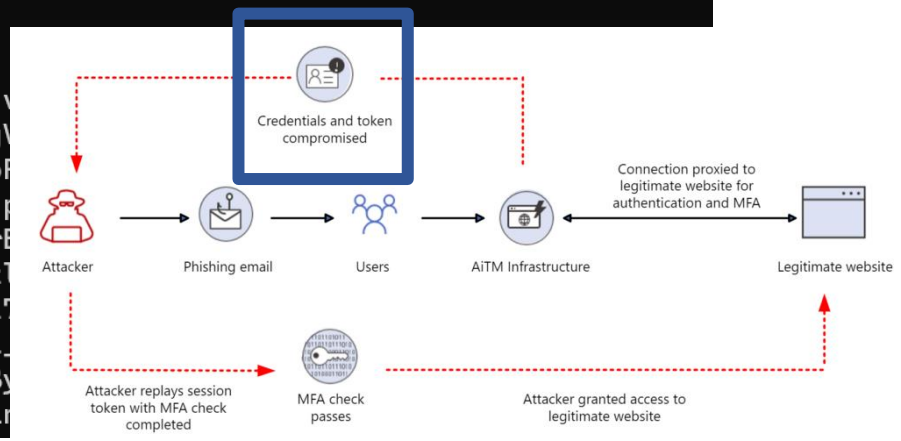
# Schritt 4 – Zugangsdaten und Token

```
[18:38:00] [+++] [0] Username: [td@swc-dev.ch]
[18:38:00] [+++] [0] Password: [redacted]
[18:38:00] [+++] [0] Username: [td@swc-dev.ch]
[18:38:55] [+++] [0] Username: [td@swc-dev.ch]
[18:38:55] [+++] [0] Custom: [mfaAuthMethod] = [PhoneAppNotification]
[18:38:59] [+++] [0] all authorization tokens intercepted!
[18:38:59] [imp] [0] redirecting to URL: https://portal.office.com (1)
: sessions

+-----+--------------+--------------+--------------+----------+----------------+-------------------+
| id  |   phishlet   |   username   |   password   |  tokens  |   remote ip    |       time        |
+-----+--------------+--------------+--------------+----------+----------------+-------------------+
| 13  | microsoft365 | td@swc-dev.ch | [redacted]  | captured | 20[redacted]   |                   |
+-----+--------------+--------------+--------------+----------+----------------+-------------------+
```

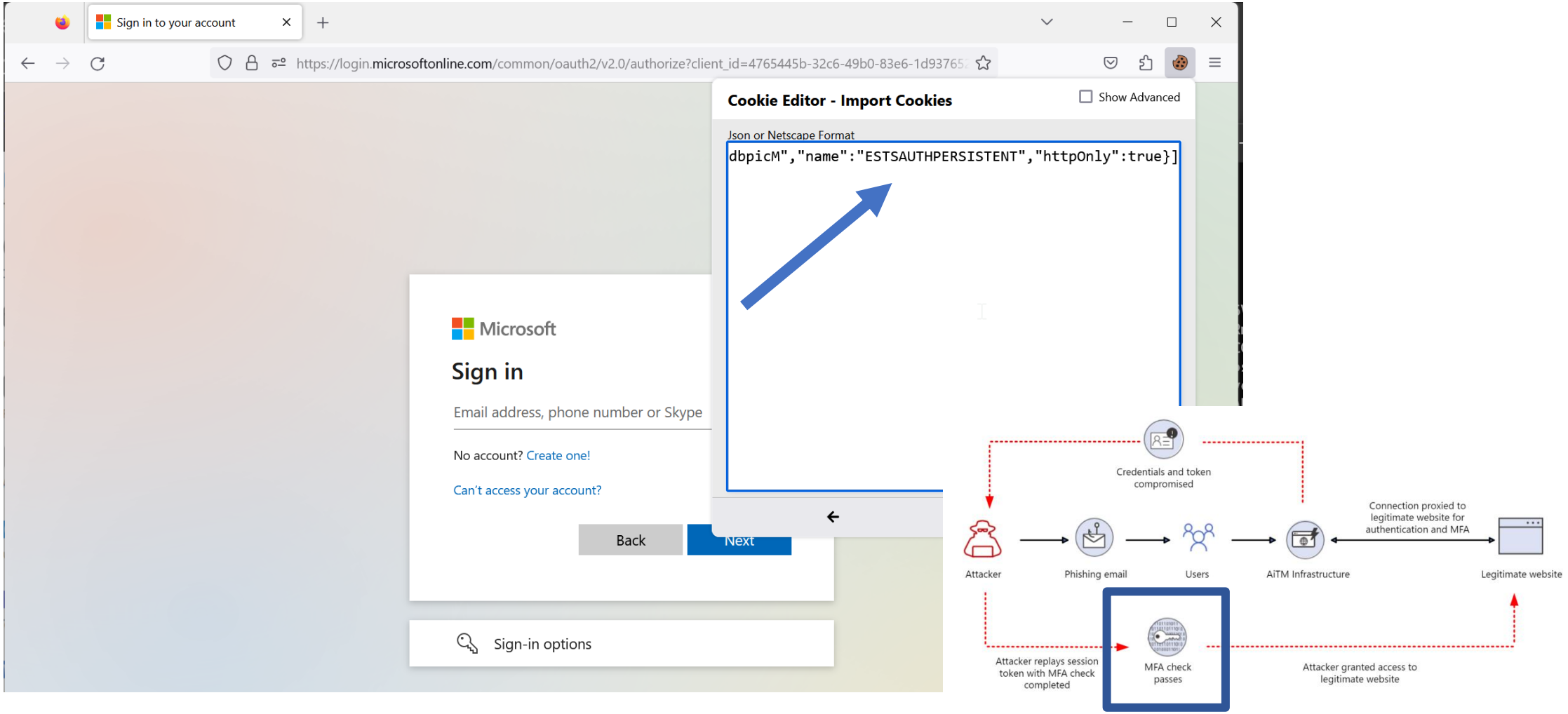


# Schritt 4 – Zugangsdaten und Token

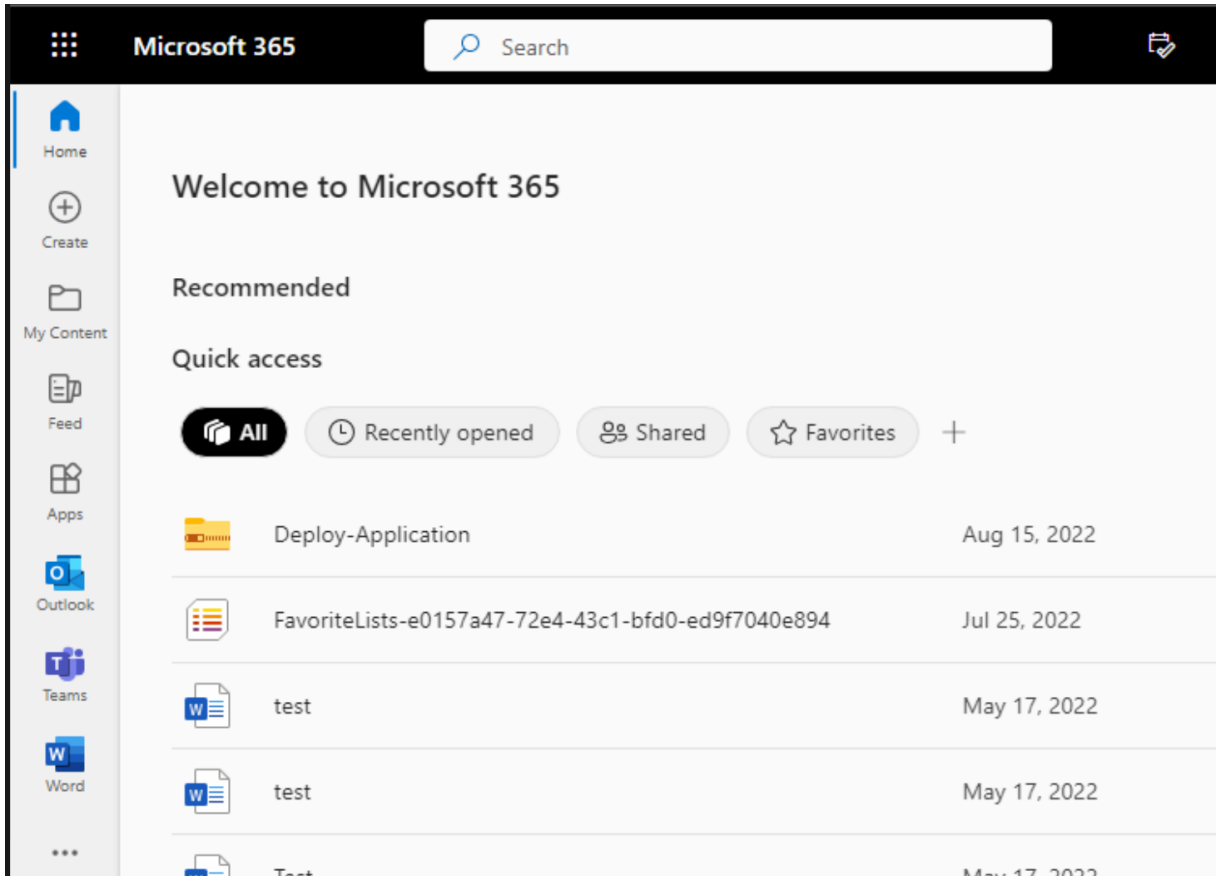
```
 username     : td@swc-dev.ch
 password     : [redacted]
 tokens       : captured
 landing url  : https://login.migrosoftonline.com/lxGyDYMl
 user-agent   : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari
/537.36 Edg/115.0.1901.203
 remote ip    : 20.203.211.25
 create time  : 2023-08-15 18:33
 update time  : 2023-08-15 18:38

[ custom ]
 mfaAuthMethod   : PhoneAppNotification

[ cookies ]
[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1723660754,"
AgDs_wUA9P-AQt5pYF3HpysZGzRlcN8x2uDJhHCC_bw7YZPRrgw0NYF-MsbcjqUrrJl50mQlBSQTLrg
sBiRELHNjTHnom3oI-JAEEKBE6Ykdqb_sbqD2lS5Pb10oJGsF4MnJl_KO8-Det_fZkOBwysaG_wmWPo
fCRaW4DB1Bfo9oKfMq4FGOsho733hps","name":"SignInStateCookie","httpOnly":true},{"
.com","expirationDate":1723660754,"value":"0.AUcAI1pkSkP9PE6-YuspkdX551tEZUfGMr
tlI4uGjEPAgDs_wUA9P8ZmRSXEXnggBNB7Ml7kYkH4Djpz1S1Y0ClQjydFFKiu72TzGczh_rfPZN8az
Only":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1
kdX551tEZUfGMrBJg-Ydk3ZSdspHABc.AgABAAQAAAAtyolDObpQQ5VtlI4uGjEPAgDs_wUA9P-Twfl
9dgrqW1g81NDO_ZUdDzh0HYRQPzHECrvHCu4dUYcaT1VrE0c3eE24nhic6Sax1Rm3HWhbiBW7lSBS3B
ietv0NHFsnq98ne0L5CL2PyKnvAtZjKvNj5aynvZMPXCsC2kUBjjz3fVDhSK7cut3cayjq85_uHeLLL
```

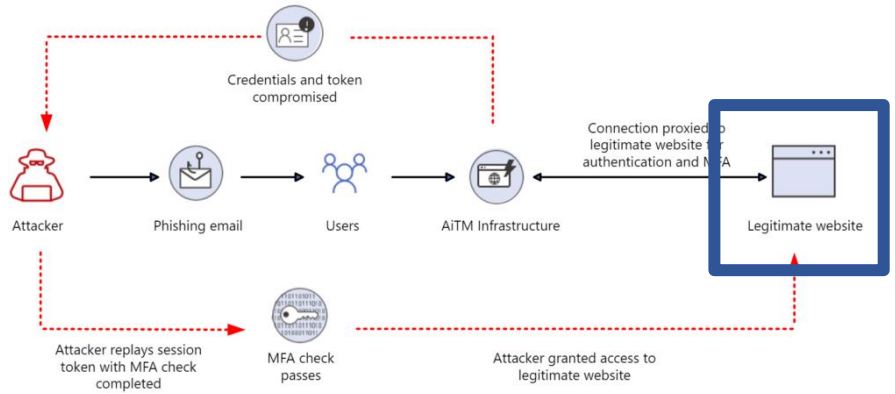


# Schritt 5 – Replay Attack

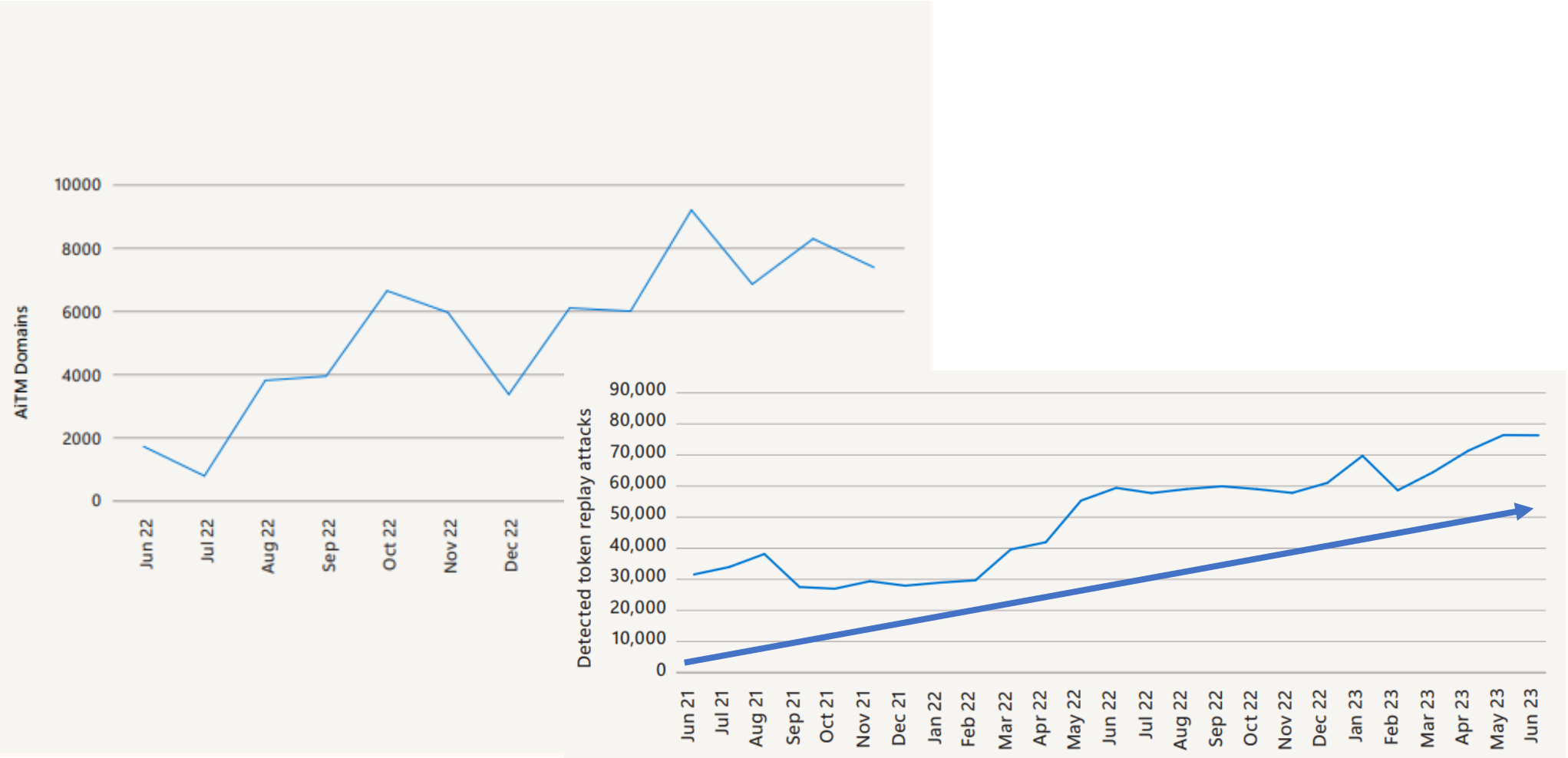


# Schritt 6 – Zugang erhalten

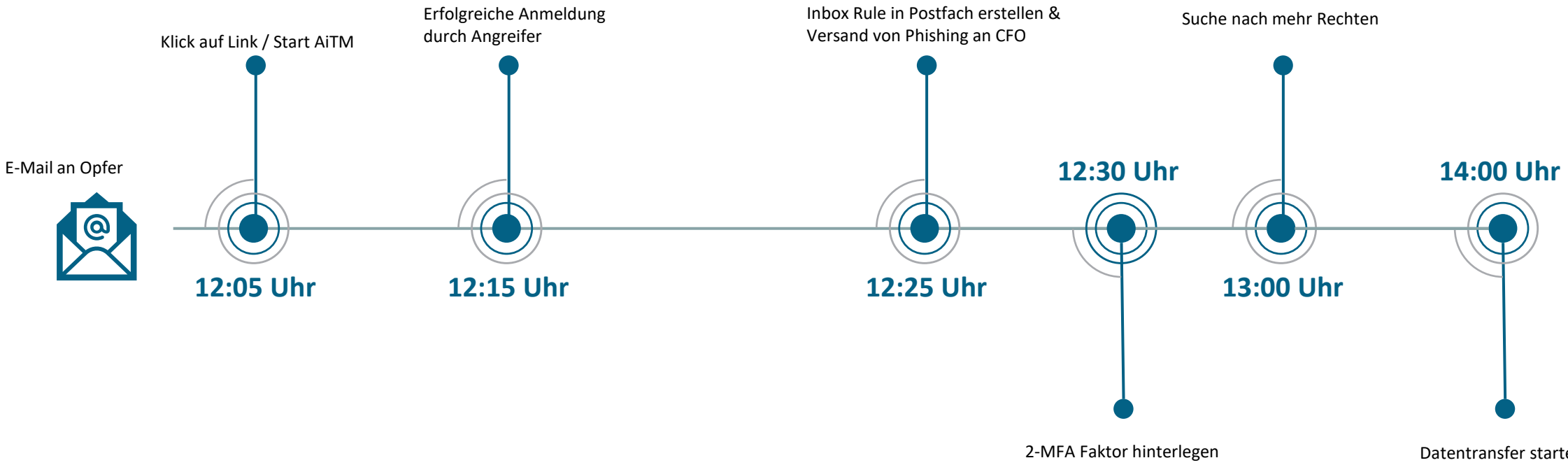


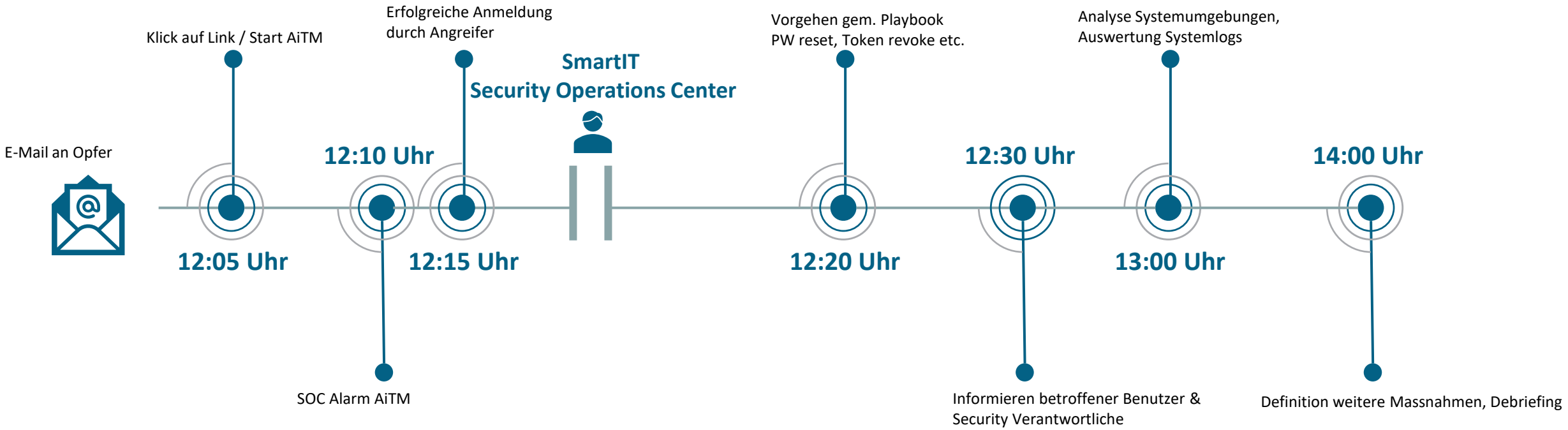
# Übersicht Microsoft – Digital Defense Report 2023



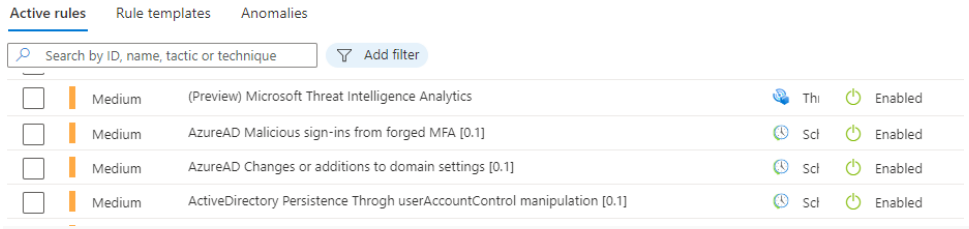
# Phishing mit AiTM
# SmartIT Security Operations Center

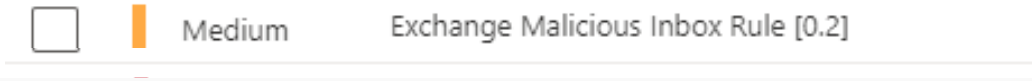


# Phishing mit AiTM
# SmartIT Security Operations Center

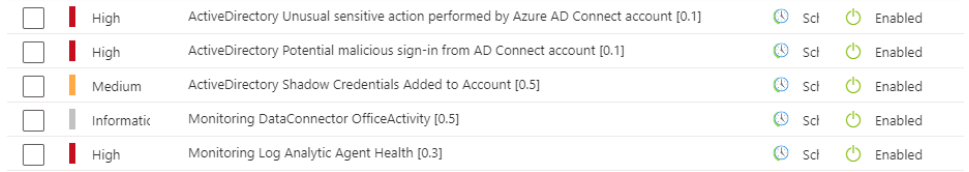


# Ablauf SmartIT SOC – Angriff wird erkannt




```
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
```



SmartIT

# Angebot

## Sicherheit als Managed Service zum monatlichen Preis

# SmartIT SOC – wiederkehrende Kosten pro Monat

| Service Leistung | Preis | Anzahl | Summe |
|---|---|---|---|
| Managed Security Operation Center - Basispreis | CHF 350.00 | 1 | CHF 350.00 |
| Managed Security Operation Center - Endpoint | CHF 19.00 | 50 | CHF 950.00 |
| **Total wiederkehrende Kosten / Benutzer** | | | **CHF 26.00** |

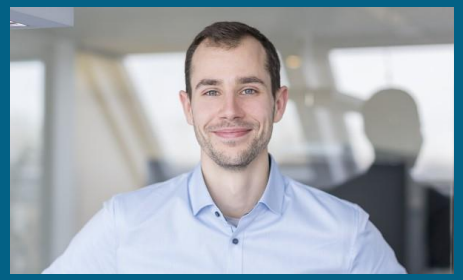
| Lizenzen und Azure Consumption* | Preis | Anzahl | Summe |
|---|---|---|---|
| Microsoft Defender for Endpoint Plan 2 | CHF 4.70 | 50 | CHF 235.00 |
| Microsoft Defender for Server P1 | CHF 5.10 | 5 | CHF 25.50 |
| Microsoft Azure Consumption | CHF 20.00 | 1 | CHF 20.00 |

*Je nach Lizenzierungsmodell bereits im Einsatz

# Herzlichen Dank für ihre Aufmerksamkeit
# Sehr gerne beantworten wir nun ihre Fragen

**Aladin Steiner**
a.steiner@smartit.ch

**Head of Value Stream Azure & Datacenter**
**Service Owner Security Operations Center**



**Martin Schmidli**
m.schmidli@smartit.ch

**Senior System Engineer**
**Security Operations Center Analyst**

SmartIT

# Security Operation in Practice