Best Practice Sharing

Das MITRE ATT&CK Framework als Grundlage zur Angriffserkennung unter KRITIS/NIS2 clever nutzen

Matthias Maier, Splunk

CEH, CISSP, CISM

splunk> bitkom

Inhalt

1

KRITIS Anforderungen Verstehen

- Systeme zur Angriffserkennung nach § 8 a Absatz 1a
- Erbringung des Nachweises

2

Umsetzung in der Praxis

Planen mithilfe von MITRE ATT&CK

Implementierung im Security Betrieb

Aufgepasst: Die 5 häufigsten Stolpersteine

splunk> bitkom

01

KRITIS Anforderungen Verstehen

Systeme zur Angriffserkennung nach § 8 a Absatz 1a

Protokollierung, Detektion und Reaktion

ab dem **1. Mai 2023;**

Einsatz von Systemen zur Angriffserkennung

- geeignete Parameter und Merkmale aus dem laufenden Betrieb
- kontinuierlich und automatisch erfassen und auswerten.

Abdeckung:

- Alle informationstechnischen Systeme, Komponenten oder Prozesse die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind
- IT, OT, Rechenzentren, Embedded Systems und weitere Bereiche

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=14#:~:text=In%20%C2%A7%208a%20Absatz%201a,tomatisch%20erfassen%20und%20auswerten%E2%80%9C%20k%C3%B6nnen.

splunk> bitkom

Systeme zur Angriffserkennung nach § 8 a Absatz 1a

Nachweis

ab dem **1. Mai 2023 Aussagen zum SzA enthalten;**

Alle 2 Jahre beim BSI Einzureichen

SOLLTE, MUSS Vorgaben

Umsetzungsgradmodell 1-5

Im Ersten Nachweiszyklus wird Stufe 3 als ausreichend akzeptiert

- Stufe 3: Alle MUSS Anforderungen erfüllt.

Neu: Können Betreiber sich auch selbst prüfen?

- Nein, eine Selbstprüfung ist aufgrund der zwingend notwendigen Unabhängigkeit und Neutralität einer prüfenden Instanz nicht gültig/möglich.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=14#:~:text=In%20%C2%A7%208a%20Absatz%201a,tomatisch%20erfassen%20und%20auswerten%E2%80%9C%20k%C3%B6nnen.

https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-Systeme-Angriffserkennung/faq-systeme-angriffserkennung_node.html

splunk> bitkom

Systeme zur Angriffserkennung nach § 8 a Absatz 1a

MUSS - Beispiele

- Im Rahmen der Planung **MÜSSEN alle Systeme identifiziert werden**, die zur Aufrechterhaltung der kritischen Dienstleistung maßgeblich sind, damit deren Protokoll- und Protokollierungsdaten später erfasst werden können
- Es **MÜSSEN zentrale Komponenten** eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten
- Es **MÜSSEN Mitarbeitende** bzw. Mitarbeitende von Dienstleistern speziell damit beauftragt werden, alle Protokoll- und Protokollierungsdaten **auszuwerten**

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=14#:~:text=In%20%C2%A7%208a%20Absatz%201a,tomatisch%20erfassen%20und%20auswerten%E2%80%9C%20k%C3%B6nnen.

splunk> bitkom

02

Umsetzung in der Praxis

Umsetzung in der Praxis

Planung der Detektion

Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden. Dazu MÜSSEN die Ergebnisse der Risikoanalyse sowie die Größe und Struktur des Unternehmens in der Planung einbezogen werden. Zur Bestimmung der Abdeckung KANN (und es wird empfohlen) eine standardisierte Methode angewendet werden (z. B. *MITRE ATT&CK* bzw. *ATT&CK for ICS* [6]). In Abhängigkeit der Unternehmensgröße und der Bedrohungslandschaft KANN eine separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung erforderlich sein.

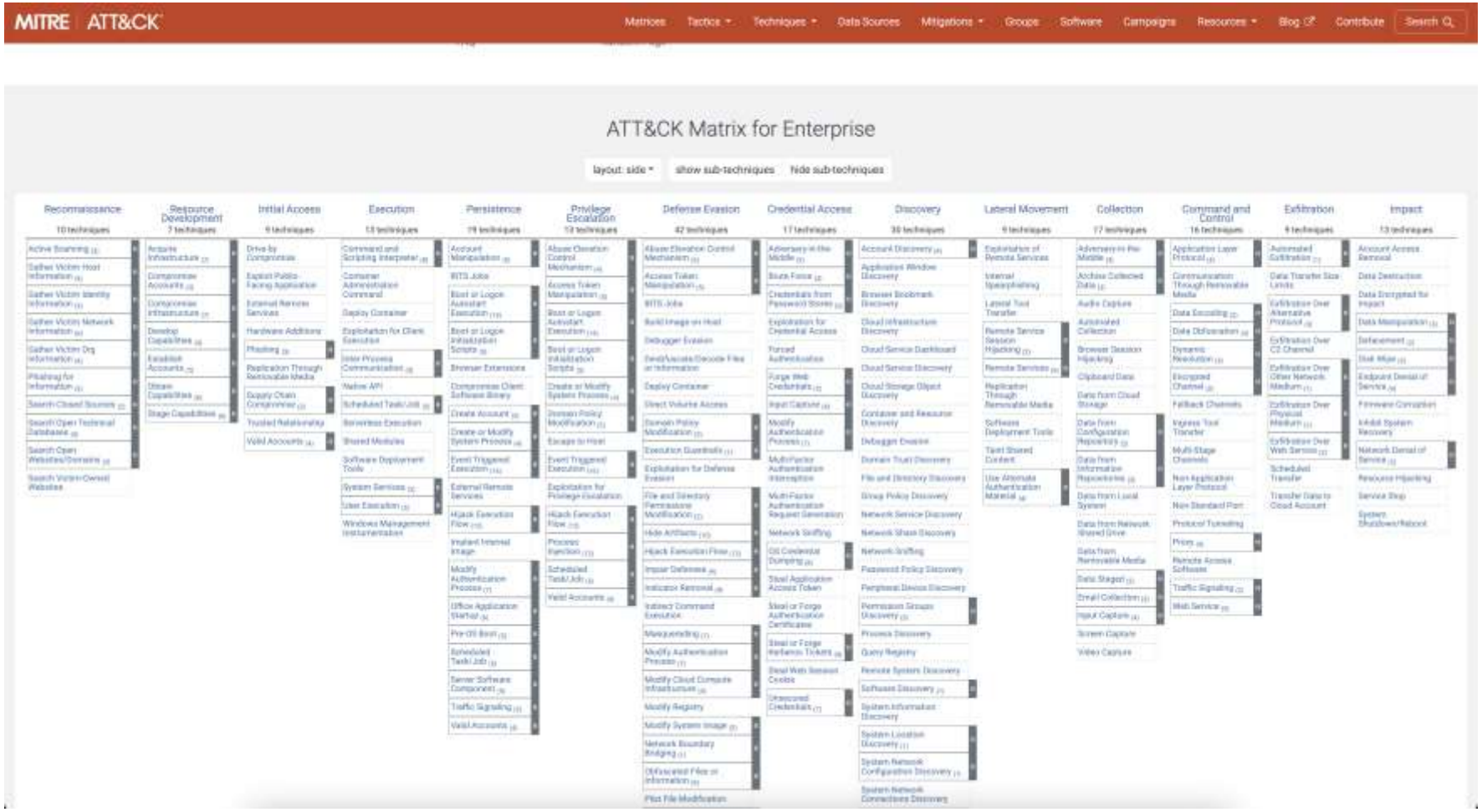
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=14#:~:text=In%20%C2%A7%208a%20Absatz%201a,tomatisch%20erfassen%20und%20auswerten%E2%80%9C%20k%C3%B6nnen.

Umsetzung in der Praxis: .italo

CISO von .italo – KRITIS Public Transportation

https://events.splunk.com/SOC-Amore-Mio-Following-italos-Tracks-to-a-More-Mature-SOC

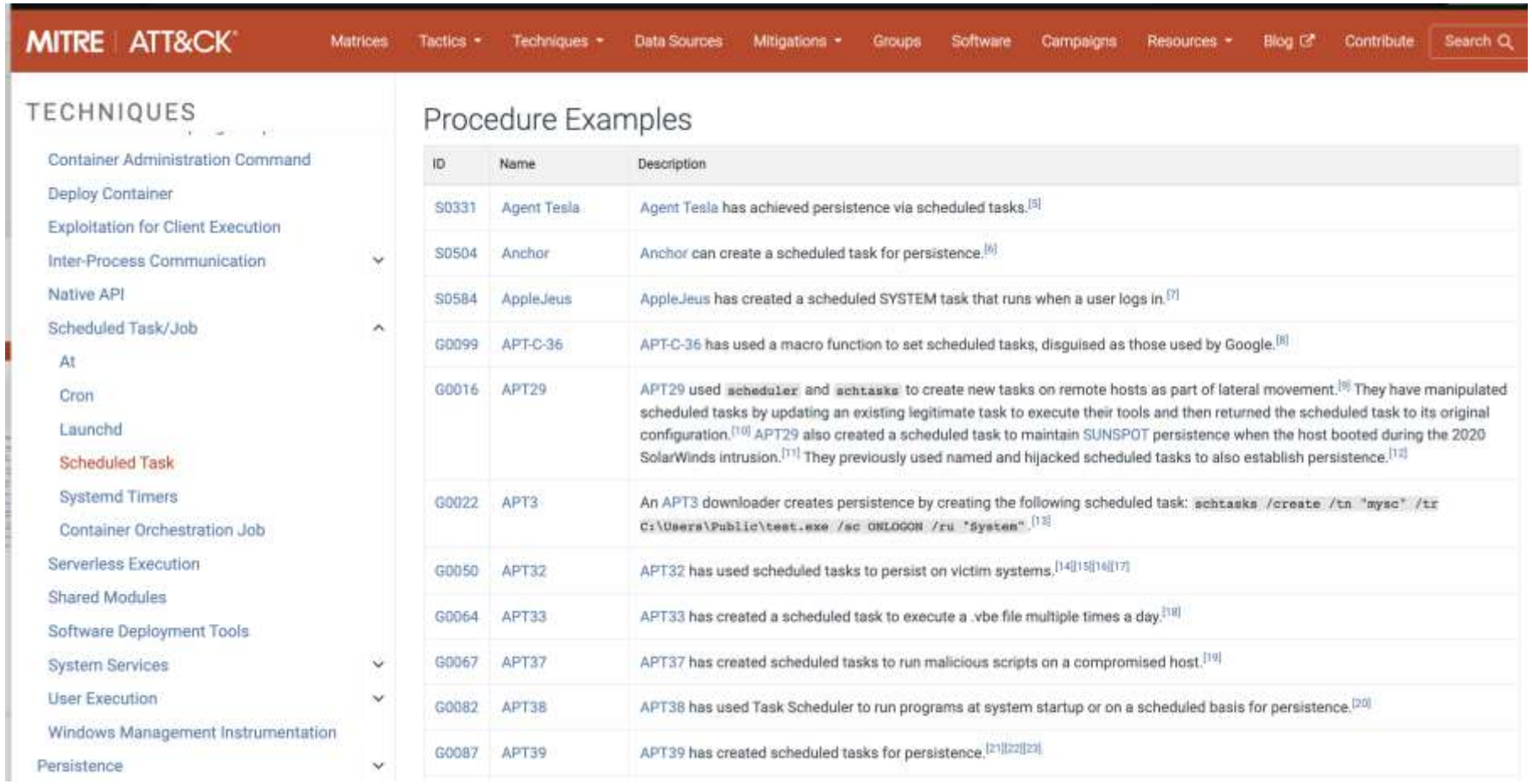
MITRE ATT&CK



https://attack.mitre.org/

splunk> bitkom

MITRE ATT&CK

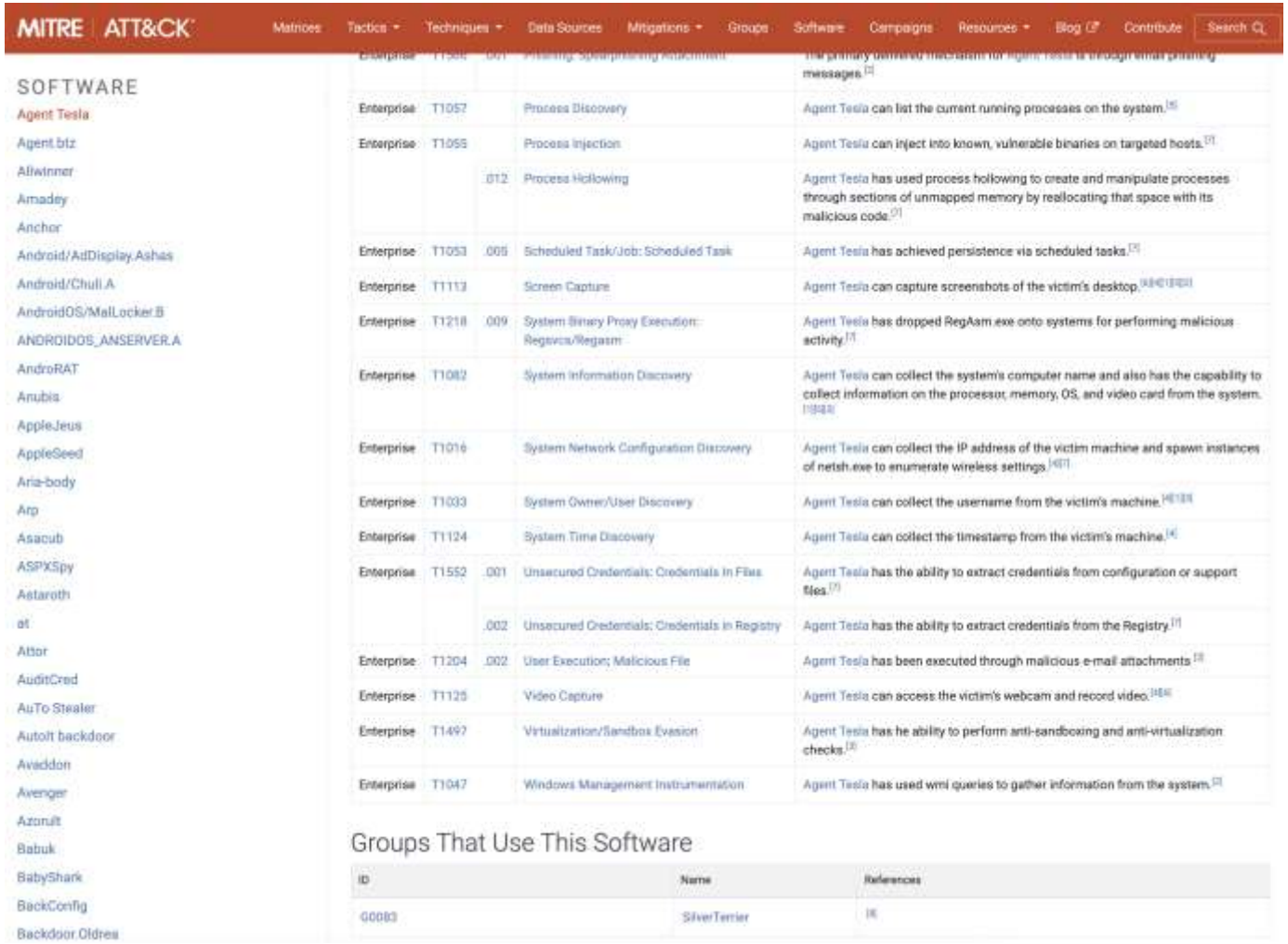


- Sub-Technique: Schedule Task
- Procedure Used by “Agent Tesla” Trojan

https://attack.mitre.org/

splunk> bitkom

MITRE ATT&CK

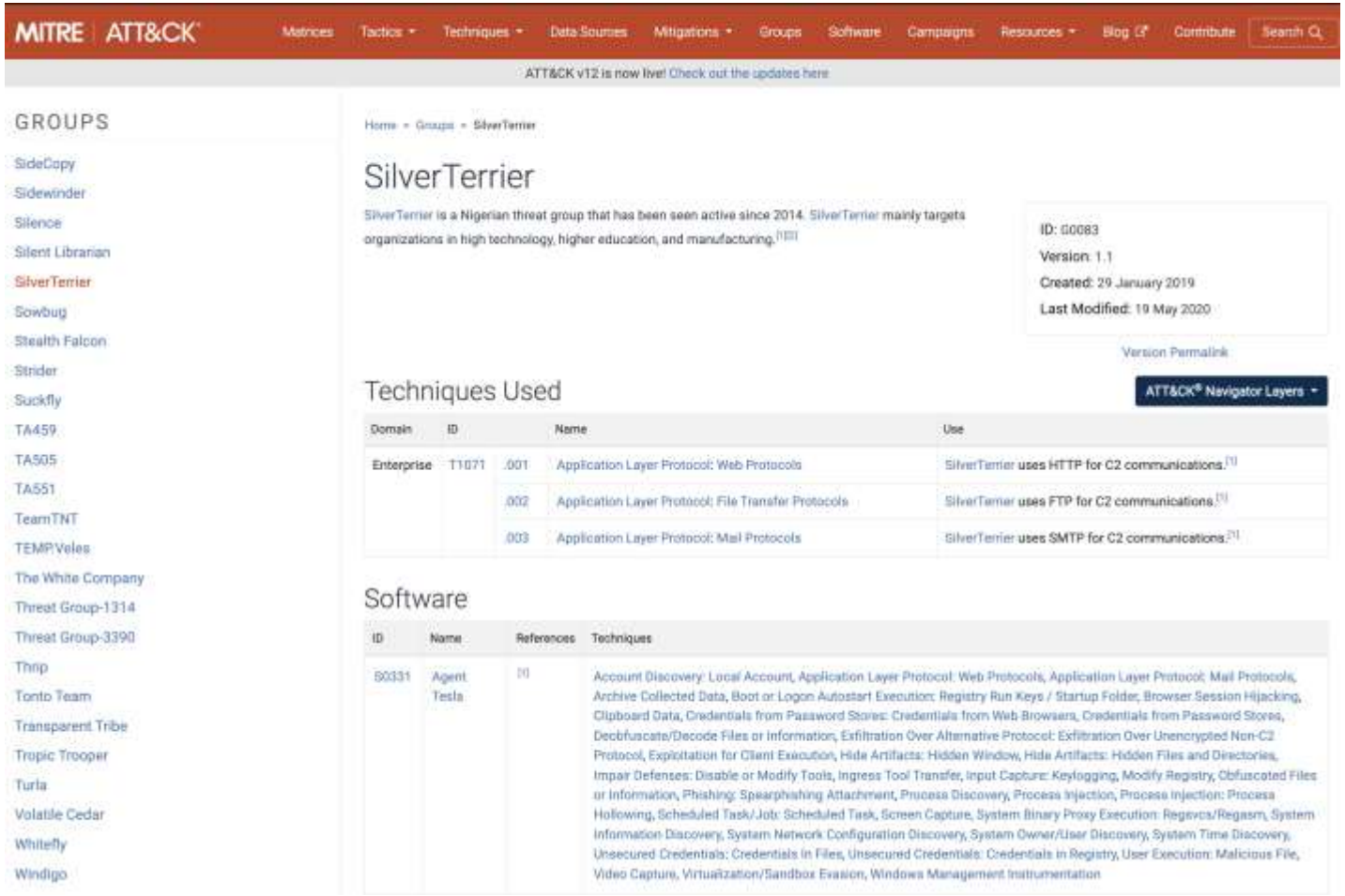


- Sub-Technique: Schedule Task
- Procedure Used by “Agent Tesla” Trojan
- Agent Tesla Trojan used by Threat Actor Group “SilverTerrier”

https://attack.mitre.org/

splunk> bitkom

MITRE ATT&CK

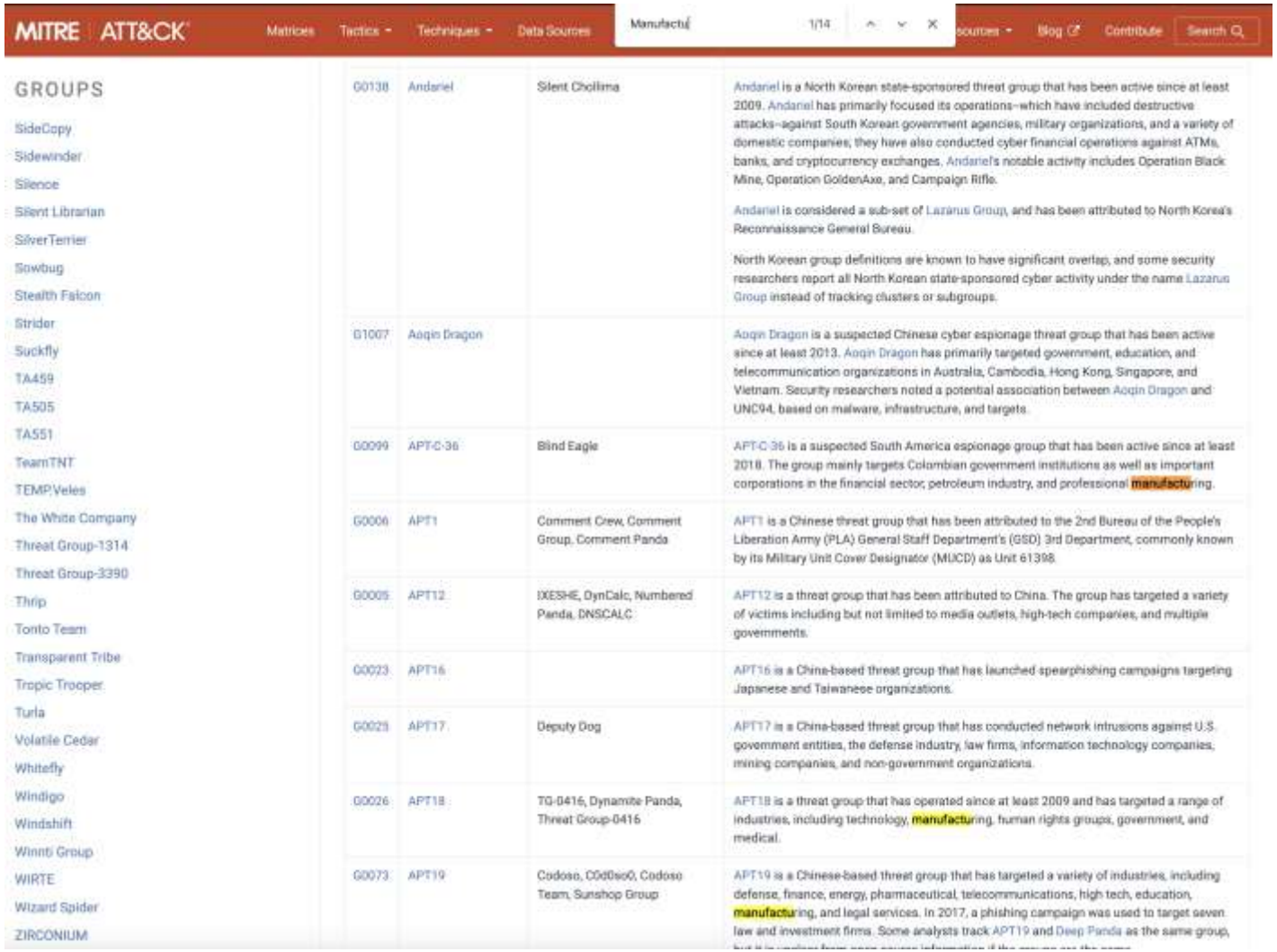


- Sub-Technique: Schedule Task
- Procedure Used by “Agent Tesla” Trojan
- Agent Tesla Trojan used by Threat Actor Group “SilverTerrier”
- ”SilverTerrier” is mostly targeting high tech, education and manufacturing

https://attack.mitre.org/

splunk> bitkom

MITRE ATT&CK



- Start with Threat Actors!

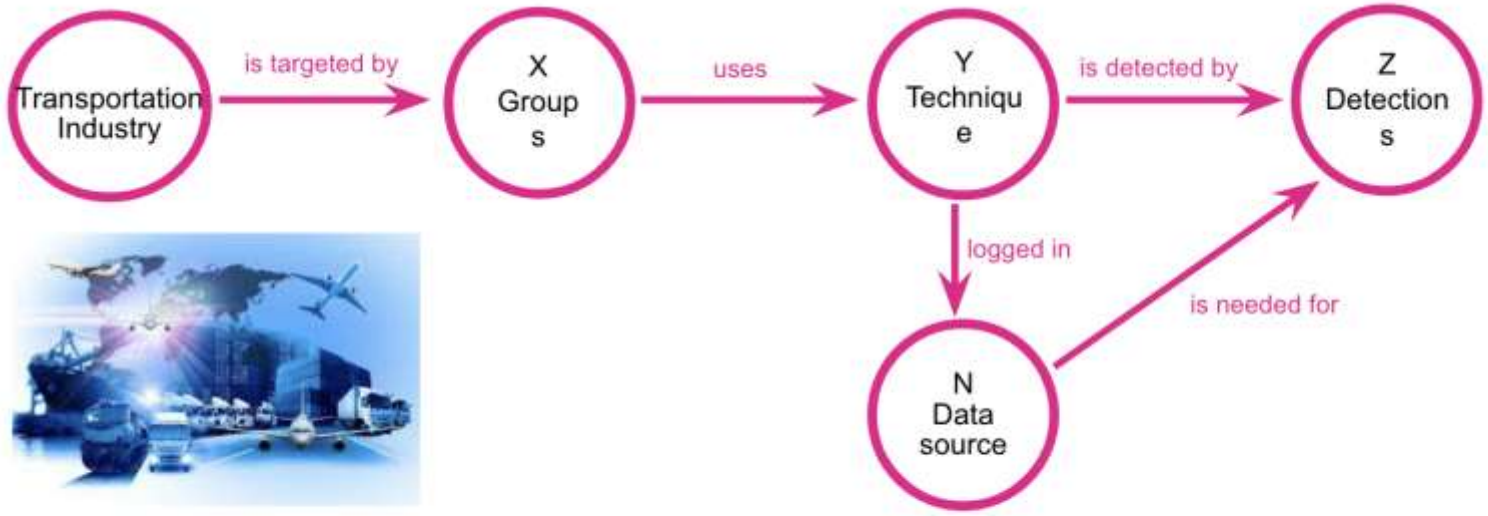
https://attack.mitre.org/

splunk> bitkom

Umsetzung in der Praxis: .italo

Goal

Contextualized Detection Strategy



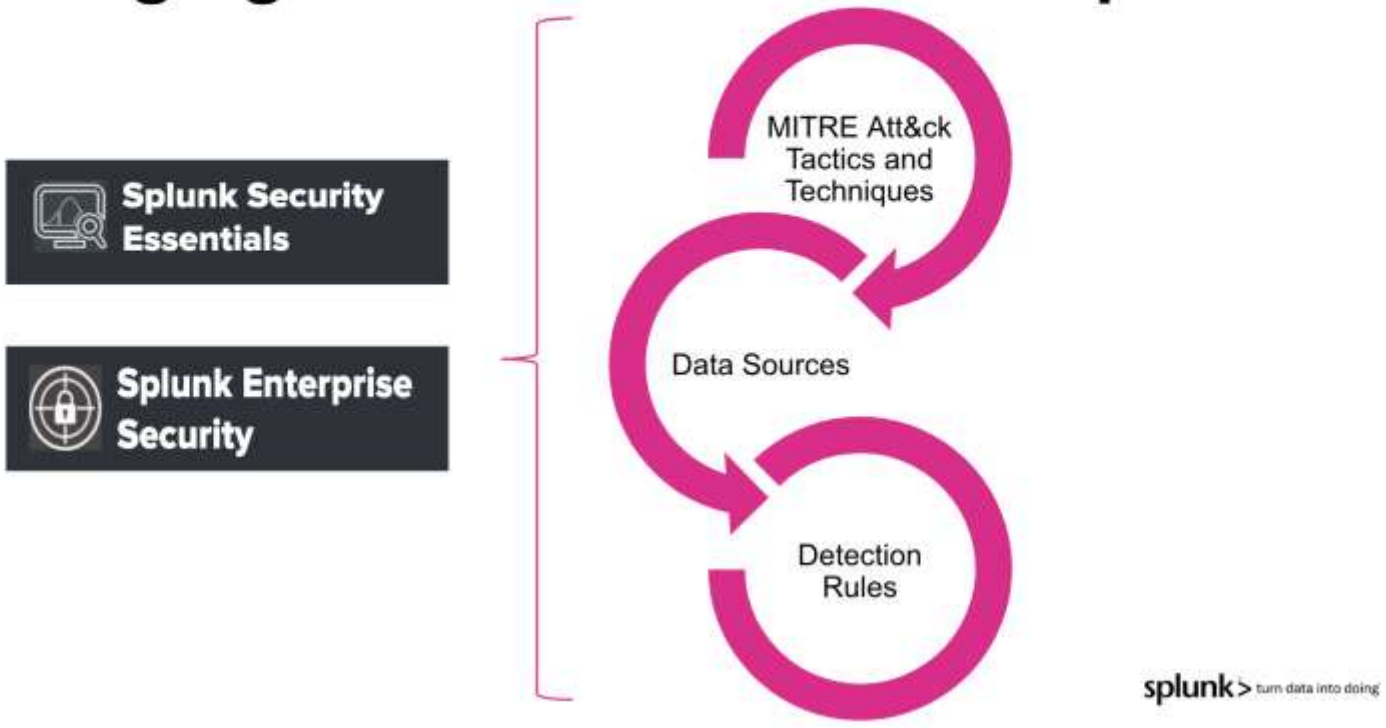
splunk> turn data into doing

https://events.splunk.com/SOC-Amore-Mio-Following-italos-Tracks-to-a-More-Mature-SOC

splunk> bitkom

Umsetzung in der Praxis: .italo

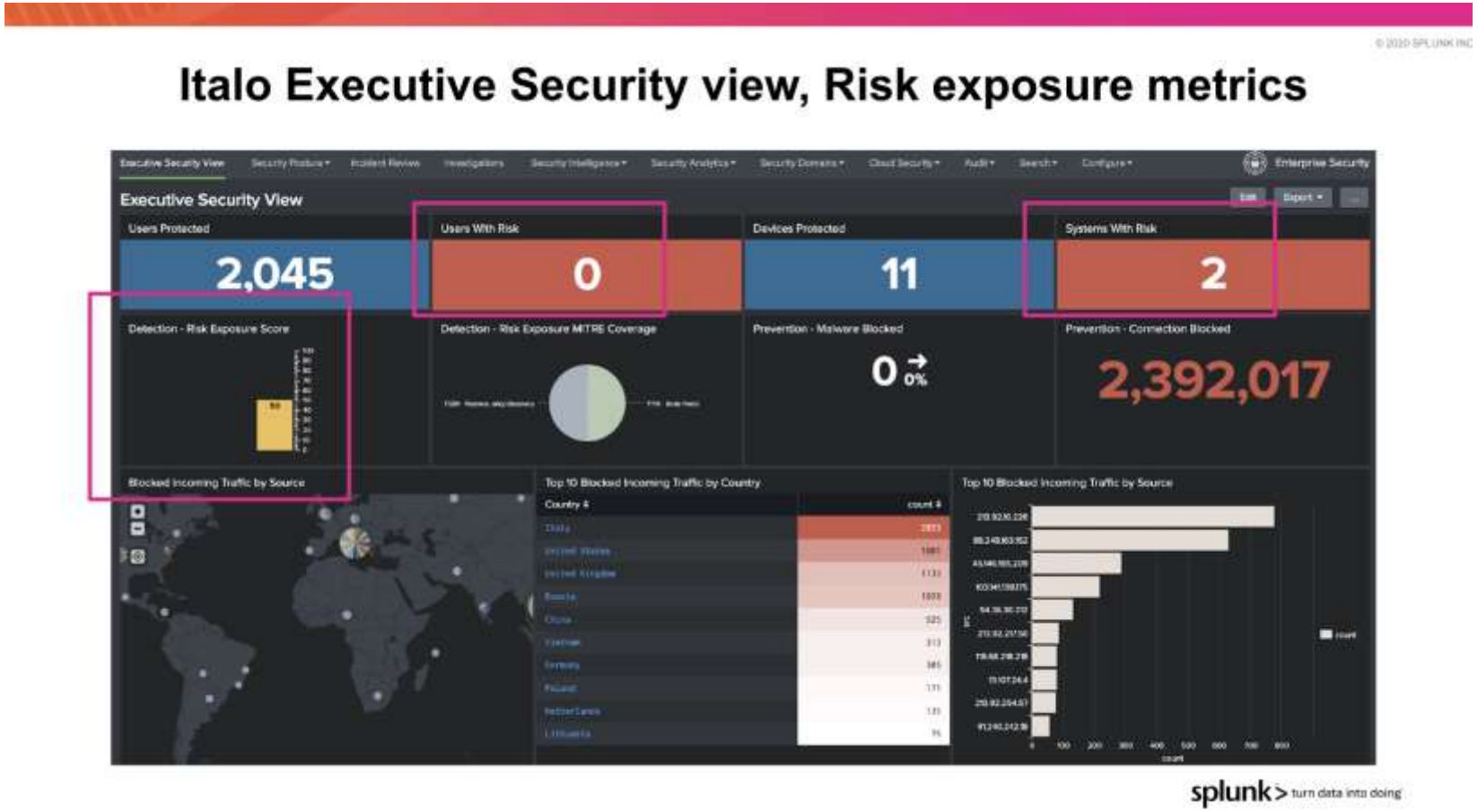
Leveraging MITRE ATT&CK with Splunk



https://events.splunk.com/SOC-Amore-Mio-Following-italos-Tracks-to-a-More-Mature-SOC

splunk> bitkom

Umsetzung in der Praxis: .italo



https://events.splunk.com/SOC-Amore-Mio-Following-italos-Tracks-to-a-More-Mature-SOC

splunk> bitkom

Aufgepasst: Die 5 häufigsten Stolpersteine

Aufgepasst: Die 5 häufigsten Stolpersteine

- Fehlende Vorab-Planung

Aufgepasst: Die 5 häufigsten Stolpersteine

- Fehlende Vorab-Planung
- Unterschätzung der Wichtigkeit von People & Process

Aufgepasst: Die 5 häufigsten Stolpersteine

- Fehlende Vorab-Planung
- Unterschätzung der Wichtigkeit von People & Process
- Unterschätzung der Komplexität hinsichtlich Querschnittsdienste

Aufgepasst: Die 5 häufigsten Stolpersteine

- Fehlende Vorab-Planung
- Unterschätzung der Wichtigkeit von People & Process
- Unterschätzung der Komplexität hinsichtlich Querschnittsdienste
- Fehlende Priorisierung und von Alarmen / Unklare Reaktionsmaßnahmen

Aufgepasst: Die 5 häufigsten Stolpersteine

- Fehlende Vorab-Planung
- Unterschätzung der Wichtigkeit von People & Process
- Unterschätzung der Komplexität hinsichtlich Querschnittsdienste
- Fehlende Priorisierung und von Alarmen / Unklare Reaktionsmaßnahmen
- Die laufende Suche nach dem “Easy Button”

Danke

1

KRITIS Anforderungen

2

Umsetzung in der Praxis

3

Lassen Sie uns in Kontakt bleiben

https://www.linkedin.com/in/sec-ninja-matthias/

Hall 7A - Booth Number 7A-112

Matthias Maier (He/Him)

splunk> bitkom