



Best Practice Sharing

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

Matthias Maier, Splunk
CEH, CISSP, CISM

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

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



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.



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**



02

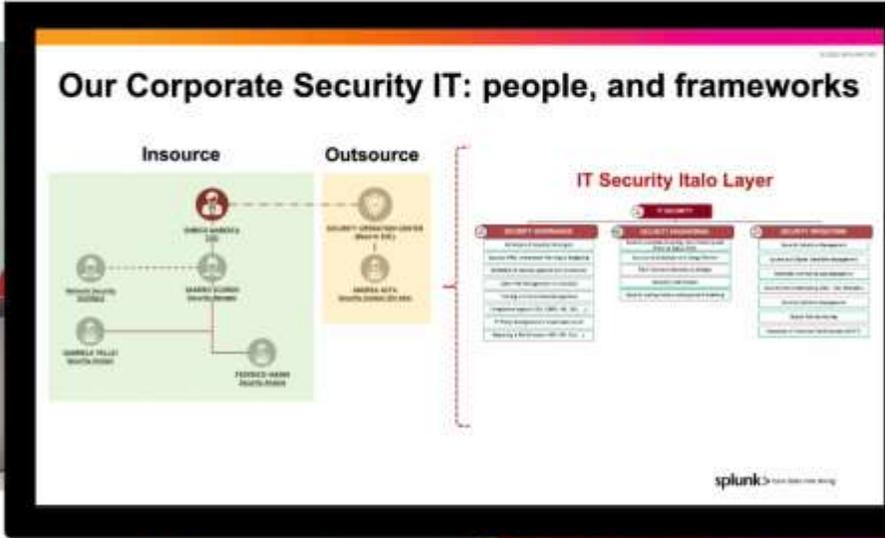
Umsetzung in der Praxis

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.

Umsetzung in der Praxis: .italo



CISO von .italo – KRITIS Public Transportation

MITRE ATT&CK

The screenshot shows the MITRE ATT&CK website interface. The top navigation bar includes 'MITRE | ATT&CK', 'Matrices', 'Tactics', 'Techniques', 'Data Sources', 'Mitigations', 'Groups', 'Software', 'Campaigns', 'Resources', 'Blog', 'Contribute', and a search box. The left sidebar lists various techniques, with 'Scheduled Task' highlighted in red. The main content area is titled 'Procedure Examples' and contains a table with the following data:

ID	Name	Description
S0331	Agent Tesla	Agent Tesla has achieved persistence via scheduled tasks. ^[5]
S0504	Anchor	Anchor can create a scheduled task for persistence. ^[6]
S0584	AppleJeuS	AppleJeuS has created a scheduled SYSTEM task that runs when a user logs in. ^[7]
G0099	APT-C-36	APT-C-36 has used a macro function to set scheduled tasks, disguised as those used by Google. ^[8]
G0016	APT29	APT29 used <code>scheduler</code> and <code>schtasks</code> to create new tasks on remote hosts as part of lateral movement. ^[9] They have manipulated scheduled tasks by updating an existing legitimate task to execute their tools and then returned the scheduled task to its original configuration. ^[10] APT29 also created a scheduled task to maintain SUNSPOT persistence when the host booted during the 2020 SolarWinds intrusion. ^[11] They previously used named and hijacked scheduled tasks to also establish persistence. ^[12]
G0022	APT3	An APT3 downloader creates persistence by creating the following scheduled task: <code>schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "system".^[13]</code>
G0050	APT32	APT32 has used scheduled tasks to persist on victim systems. ^{[14][15][16][17]}
G0064	APT33	APT33 has created a scheduled task to execute a .vbe file multiple times a day. ^[18]
G0067	APT37	APT37 has created scheduled tasks to run malicious scripts on a compromised host. ^[19]
G0082	APT38	APT38 has used Task Scheduler to run programs at system startup or on a scheduled basis for persistence. ^[20]
G0087	APT39	APT39 has created scheduled tasks for persistence. ^{[21][22][23]}

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

MITRE ATT&CK

MITRE ATT&CK

Matrices: Tactics: Techniques: Data Sources: Mitigations: Groups: Software: Campaigns: Resources: Blog: Contribute: Search

SOFTWARE

- Agent Tesla
- Agent.btz
- Allwinner
- Amadey
- Anchor
- Android/AdDisplay.Ashas
- Android/Chull.A
- AndroidOS/MalLocker.B
- ANDROIDOS_ANSERVER.A
- AndroRAT
- Anubis
- AppleJeus
- AppleSeed
- Aria-body
- Arp
- Asacub
- ASPXSpy
- Astaroth
- at
- Atbar
- AuditCred
- AuTo Stealer
- AutoIt backdoor
- Avaddon
- Avenger
- Azorult
- Babuk
- BabyShark
- BackConfig
- Backdoor.Oldres

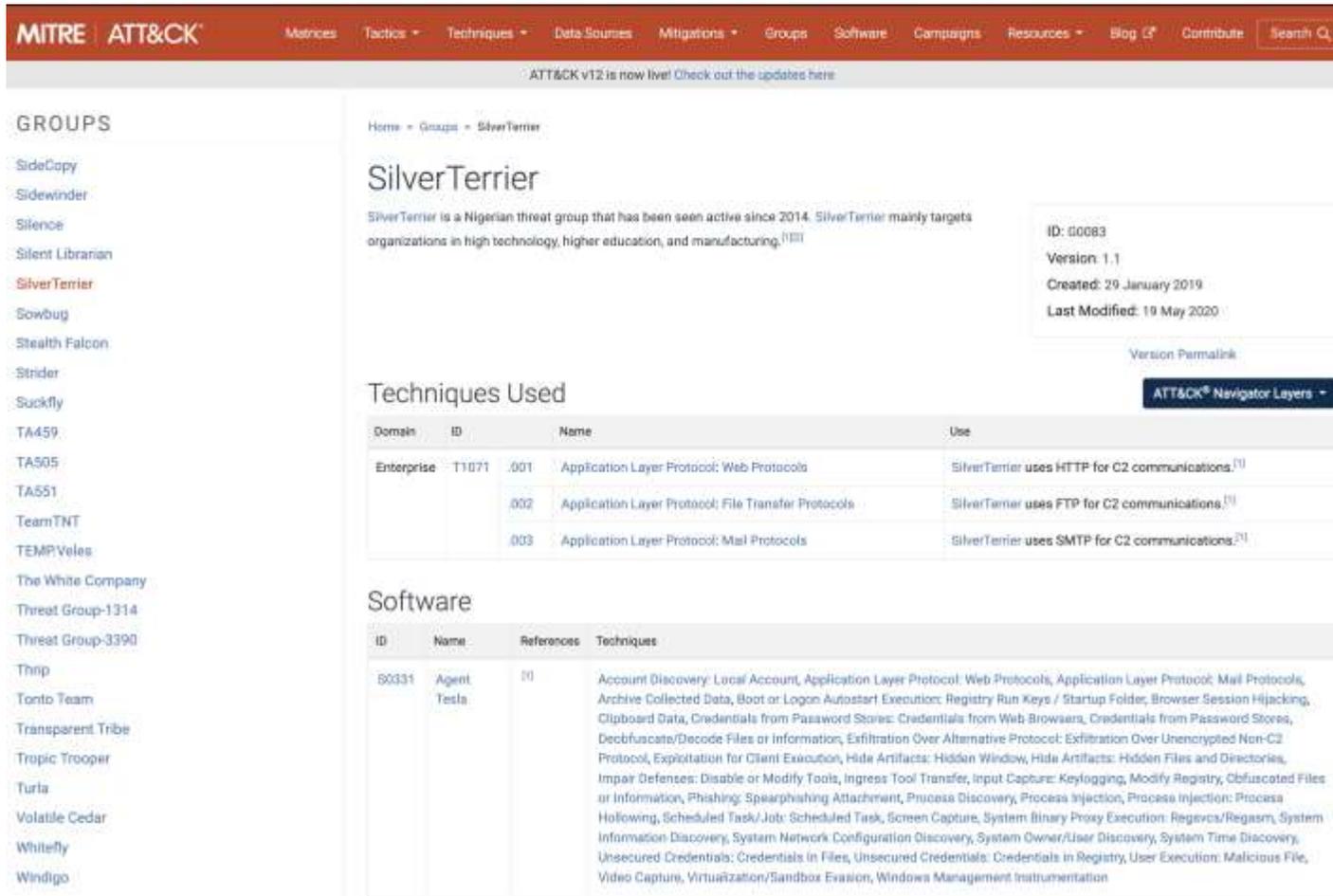
Enterprise	T1057	Process Discovery	Agent Tesla can list the current running processes on the system. ^[5]
Enterprise	T1055	Process Injection	Agent Tesla can inject into known, vulnerable binaries on targeted hosts. ^[7]
	.012	Process Hollowing	Agent Tesla has used process hollowing to create and manipulate processes through sections of unmapped memory by reallocating that space with its malicious code. ^[1]
Enterprise	T1053	Scheduled Task/Job: Scheduled Task	Agent Tesla has achieved persistence via scheduled tasks. ^[5]
Enterprise	T1113	Screen Capture	Agent Tesla can capture screenshots of the victim's desktop. ^{[8][9][10]}
Enterprise	T1218	System Binary Proxy Execution: Regsvcs/Regasm	Agent Tesla has dropped RegAam.exe onto systems for performing malicious activity. ^[1]
Enterprise	T1082	System Information Discovery	Agent Tesla can collect the system's computer name and also has the capability to collect information on the processor, memory, OS, and video card from the system. ^{[1][9][11]}
Enterprise	T1016	System Network Configuration Discovery	Agent Tesla can collect the IP address of the victim machine and spawn instances of netsh.exe to enumerate wireless settings. ^{[6][7]}
Enterprise	T1033	System Owner/User Discovery	Agent Tesla can collect the username from the victim's machine. ^{[6][12]}
Enterprise	T1134	System Time Discovery	Agent Tesla can collect the timestamp from the victim's machine. ^[6]
Enterprise	T1552	Unsecured Credentials: Credentials in Files	Agent Tesla has the ability to extract credentials from configuration or support files. ^[1]
	.002	Unsecured Credentials: Credentials in Registry	Agent Tesla has the ability to extract credentials from the Registry. ^[1]
Enterprise	T1204	User Execution: Malicious File	Agent Tesla has been executed through malicious e-mail attachments. ^[1]
Enterprise	T1125	Video Capture	Agent Tesla can access the victim's webcam and record video. ^{[1][6][13]}
Enterprise	T1497	Virtualization/Sandbox Evasion	Agent Tesla has the ability to perform anti-sandboxing and anti-virtualization checks. ^[1]
Enterprise	T1047	Windows Management Instrumentation	Agent Tesla has used wmi queries to gather information from the system. ^[1]

Groups That Use This Software

ID	Name	References
G0083	SilverTerrier	[6]

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

MITRE ATT&CK



MITRE ATT&CK

Matrices | Tactics | Techniques | Data Sources | Mitigations | Groups | Software | Campaigns | Resources | Blog | Contribute | Search

ATT&CK v12 is now live! Check out the updates here

GROUPS

- SideCopy
- Sidewinder
- Silence
- Silent Librarian
- SilverTerrier**
- Sowbug
- Stealth Falcon
- Strider
- Suckfly
- TA459
- TA505
- TA551
- TeamTNT
- TEMPVeles
- The White Company
- Threat Group-1314
- Threat Group-3390
- Thrip
- Tonto Team
- Transparent Tribe
- Tropic Trooper
- Turla
- Volatile Cedar
- Whitefly
- Windigo

Home » Groups » SilverTerrier

SilverTerrier

SilverTerrier is a Nigerian threat group that has been seen active since 2014. SilverTerrier mainly targets organizations in high technology, higher education, and manufacturing.^{[1][2]}

ID: G0083
Version: 1.1
Created: 29 January 2019
Last Modified: 19 May 2020

Version Permalink

Techniques Used

Domain	ID	Name	Use
Enterprise	T11071	.001	Application Layer Protocol: Web Protocols SilverTerrier uses HTTP for C2 communications. ^[1]
		.002	Application Layer Protocol: File Transfer Protocols SilverTerrier uses FTP for C2 communications. ^[1]
		.003	Application Layer Protocol: Mail Protocols SilverTerrier uses SMTP for C2 communications. ^[1]

Software

ID	Name	References	Techniques
50331	Agent Tesla	[1]	Account Discovery: Local Account, Application Layer Protocol: Web Protocols, Application Layer Protocol: Mail Protocols, Archive Collected Data, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Browser Session Hijacking, Clipboard Data, Credentials from Password Stores: Credentials from Web Browsers, Credentials from Password Stores, Decfuscate/Decode Files or Information, Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol, Exploitation for Client Execution, Hide Artifacts: Hidden Window, Hide Artifacts: Hidden Files and Directories, Impair Defenses: Disable or Modify Tools, Ingress Tool Transfer, Input Capture: Keylogging, Modify Registry, Obfuscated Files or Information, Phishing: Spearphishing Attachment, Process Discovery, Process Injection, Process Injection: Process Hollowing, Scheduled Task/Job: Scheduled Task, Screen Capture, System Binary Proxy Execution: Regsvcs/Regasm, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, System Time Discovery, Unsecured Credentials: Credentials in Files, Unsecured Credentials: Credentials in Registry, User Execution: Malicious File, Video Capture, Virtualization/Sandbox Evasion, Windows Management Instrumentation

- 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

MITRE ATT&CK

GROUPS	MITRE ID	Group Name	Aliases	Description
SideCopy	G0138	Andarjel	Silent Cholima	Andarjel is a North Korean state-sponsored threat group that has been active since at least 2009. Andarjel has primarily focused its operations—which have included destructive attacks—against South Korean government agencies, military organizations, and a variety of domestic companies; they have also conducted cyber financial operations against ATMs, banks, and cryptocurrency exchanges. Andarjel's notable activity includes Operation Black Mine, Operation GoldenAxe, and Campaign Rifle.
Sidewinder				
Silence				
Silent Librarian				Andarjel is considered a sub-set of Lazarus Group, and has been attributed to North Korea's Reconnaissance General Bureau.
SilverTemier				North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name Lazarus Group instead of tracking clusters or subgroups.
Sowbug	G1007	Aoqin Dragon		Aoqin Dragon is a suspected Chinese cyber espionage threat group that has been active since at least 2013. Aoqin Dragon has primarily targeted government, education, and telecommunication organizations in Australia, Cambodia, Hong Kong, Singapore, and Vietnam. Security researchers noted a potential association between Aoqin Dragon and UNC94, based on malware, infrastructure, and targets.
Stealth Falcon				
Strider				
Suckfly				
TA459				
TA505				
TA551				
TeamTNT	G0099	APT-C-36	Blind Eagle	APT-C-36 is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colombian government institutions as well as important corporations in the financial sector, petroleum industry, and professional manufacturing .
TEMP/Veles				
The White Company	G0006	APT1	Comment Crew, Comment Group, Comment Panda	APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398.
Threat Group-1314				
Threat Group-3390				
Thrip	G0005	APT12	IXESHE, DynCalc, Numbered Panda, DNSCALC	APT12 is a threat group that has been attributed to China. The group has targeted a variety of victims including but not limited to media outlets, high-tech companies, and multiple governments.
Tonto Team				
Transparent Tribe				
Tropic Trooper	G0023	APT16		APT16 is a China-based threat group that has launched spearfishing campaigns targeting Japanese and Taiwanese organizations.
Turla				
Volatile Cedar	G0023	APT17	Deputy Dog	APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations.
Whitefly				
Windigo				
Windshift	G0026	APT18	TQ-0416, Dynamite Panda, Threat Group-0416	APT18 is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing , human rights groups, government, and medical.
Winnit Group				
WIRTE	G0073	APT19	Codoso, Codsoo0, Codoso Team, Sunshop Group	APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing , and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. Some analysts track APT19 and Deep Panda as the same group, but this content does not contain information if the groups are the same.
Wizard Spider				
ZIRCONIUM				

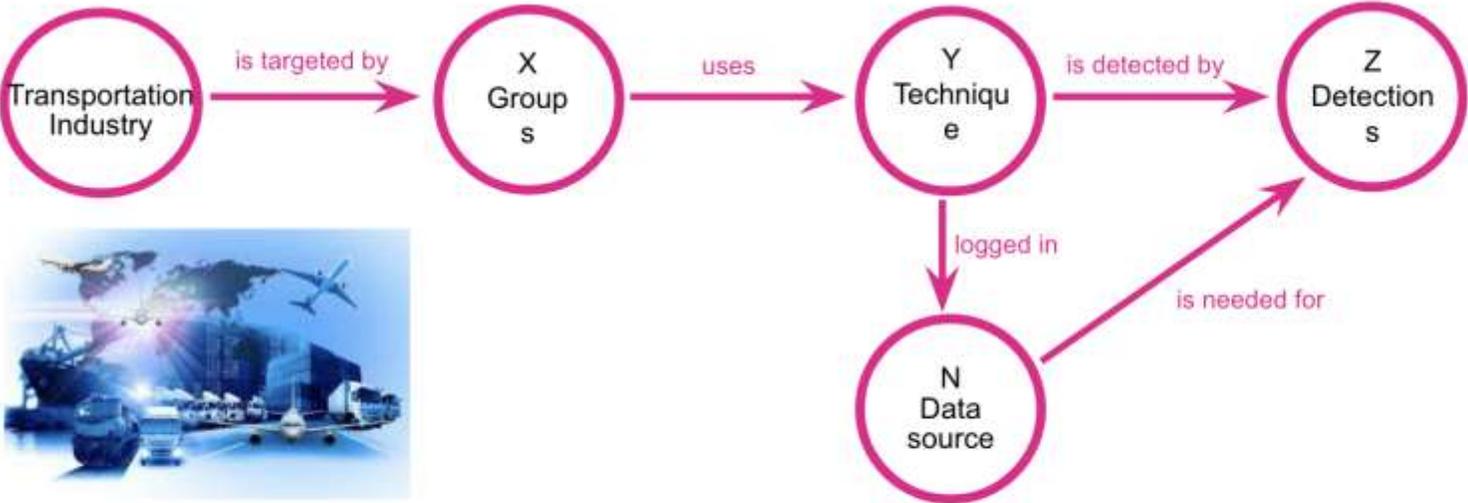
- Start with Threat Actors!

Umsetzung in der Praxis: .italo

© 2020 SPLUNK INC.

Goal

Contextualized Detection Strategy

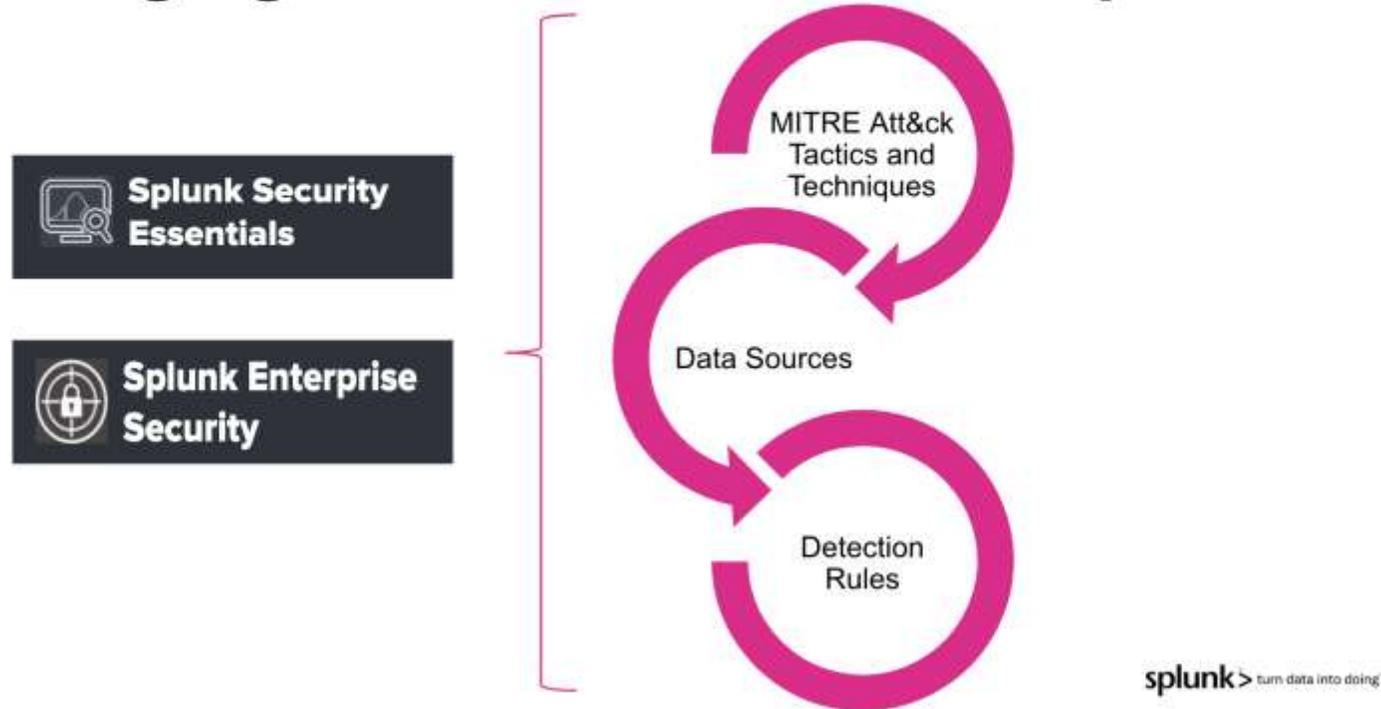


splunk > turn data into doing

Umsetzung in der Praxis: .italo

© 2020 SPLUNK INC.

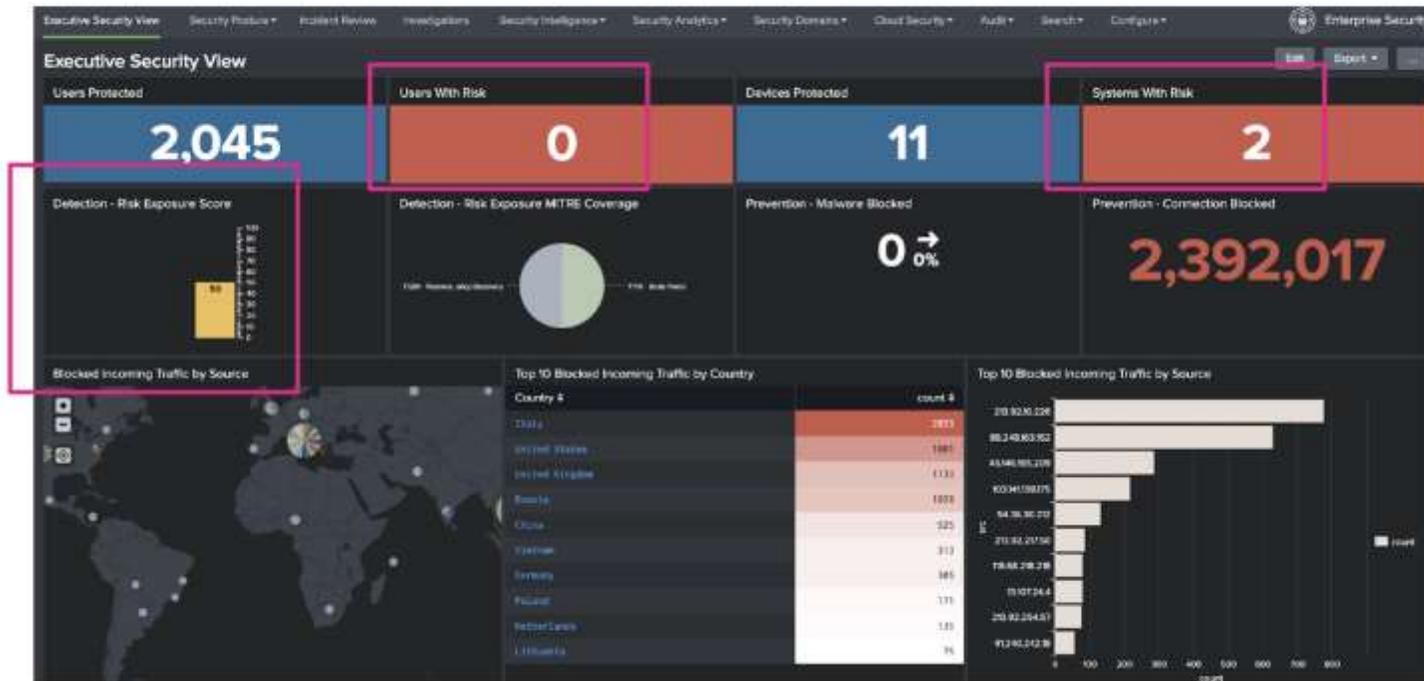
Leveraging MITRE ATT&CK with Splunk



Umsetzung in der Praxis: .italo

© 2020 SPLUNK INC

Italo Executive Security view, Risk exposure metrics



splunk > turn data into doing



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)