Supercharge your Security Operations Center with Splunk and MITRE

Christian Heger
SOC Architect / Technical Head of SOC | DATEV eG

Dr. Sebastian Schmerl
Head of Cyber Defense | Computacenter

Christian Heger

SOC Architect / Technical Head of SOC | DATEV eG

Sebastian Schmerl

Head of Cyber Defense | Computacenter

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

Key takeaways

What you should take home from this session

Cyber Defense @DATEV

Strategic goals & approach

Prioritize the right things.

Be fast and use what is there…

Analysis & Response Workflow

Promote the Cyber Defense topic

Knowledge Sharing & Awareness

Promote the Cyber Defense topic

What is / does DATEV?

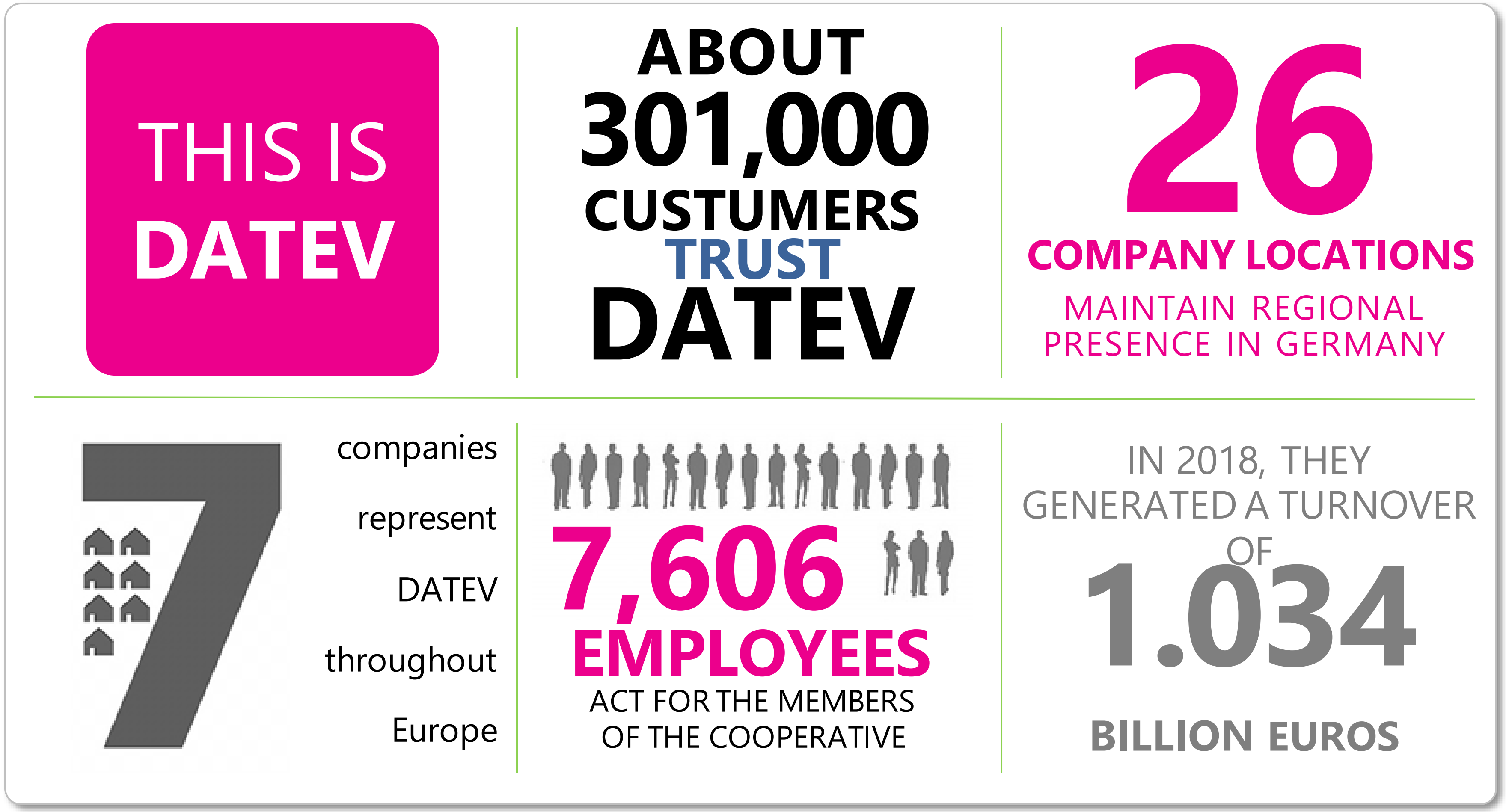
Financial Power

DATEV

Whom do 13 million employees trust each month?

DATEV eG

Shaping the future – together



THIS IS DATEV

ABOUT 301,000 CUSTUMERS TRUST DATEV

26 COMPANY LOCATIONS

MAINTAIN REGIONAL PRESENCE IN GERMANY

7 companies represent DATEV throughout Europe

7,606 EMPLOYEES

ACT FOR THE MEMBERS OF THE COOPERATIVE

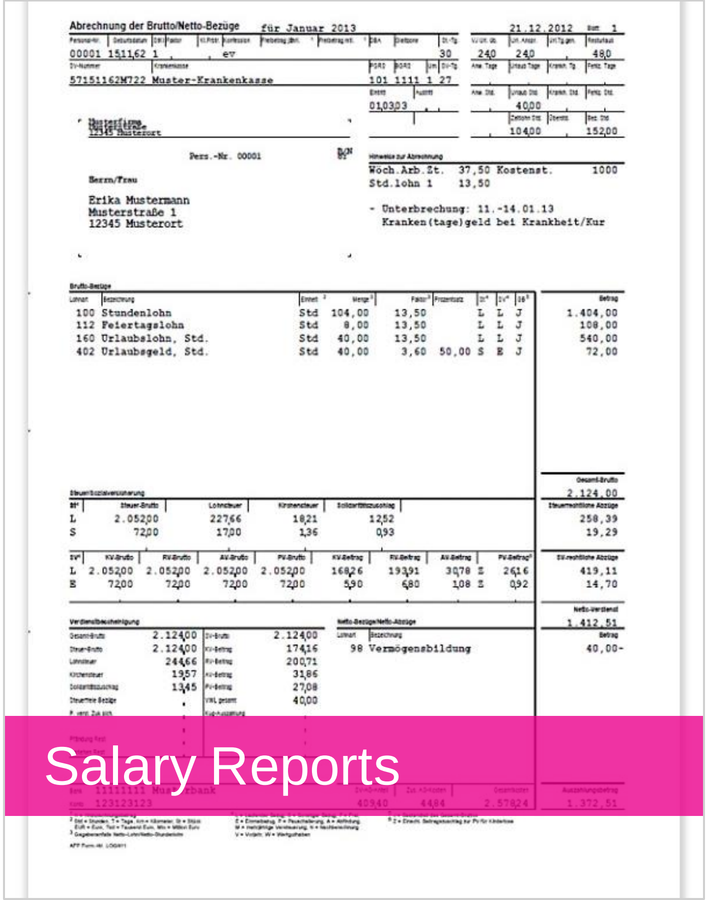
IN 2018, THEY GENERATED A TURNOVER OF

1.034

BILLION EUROS

What you usually see from us…

our software is the key doing tax business



Abrechnung der Brutto/Netto-Bezüge für Januar 2013 21.12.2012 1

Personal-Nr.	Geburtsdatum	StKl	Faktor	Kfr.Fbtr.	Konfession	Freibetrag jährl.	Freibetrag mtl.	DBA	Steuer-ID	St-Tg	VJ Url.	Url. Anspr.	Url.Tg gen.	Resturlaub
00001	15.11.62	1	,	,	ev					30	24,0	24,0	,	48,0

SV-Nummer	Krankenkasse	PGRS	BGRS	Um	SV-Tg
57151162M722	Muster-Krankenkasse	101	1111	1	27

Eintritt 01.03.03

Urlaub Std. 40,00

Zeitlohn Std. 104,00 — Bez. Std. 152,00

Musterfirma
Musterstraße
12345 Musterort

Pers.-Nr. 00001

Herrn/Frau

Erika Mustermann
Musterstraße 1
12345 Musterort

Hinweise zur Abrechnung

Wöch.Arb.Zt. 37,50 Kostenst. 1000
Std.lohn 1 13,50

- Unterbrechung: 11.-14.01.13
  Kranken(tage)geld bei Krankheit/Kur

Brutto-Bezüge

Lohnart	Bezeichnung	Einheit	Menge	Faktor	Prozentsatz	St	SV	GB	Betrag
100	Stundenlohn	Std	104,00	13,50		L	L	J	1.404,00
112	Feiertagslohn	Std	8,00	13,50		L	L	J	108,00
160	Urlaubslohn, Std.	Std	40,00	13,50		L	L	J	540,00
402	Urlaubsgeld, Std.	Std	40,00	3,60	50,00	S	E	J	72,00

Gesamt-Brutto 2.124,00

Steuer/Sozialversicherung

St	Steuer-Brutto	Lohnsteuer	Kirchensteuer	Solidaritätszuschlag	Steuerrechtliche Abzüge
L	2.052,00	227,66	18,21	12,52	258,39
S	72,00	17,00	1,36	0,93	19,29

SV	KV-Brutto	RV-Brutto	AV-Brutto	PV-Brutto	KV-Beitrag	RV-Beitrag	AV-Beitrag		PV-Beitrag	SV-rechtliche Abzüge
L	2.052,00	2.052,00	2.052,00	2.052,00	168,26	193,91	30,78	Z	26,16	419,11
E	72,00	72,00	72,00	72,00	5,90	6,80	1,08	Z	0,92	14,70

Netto-Verdienst 1.412,51

Verdienstbescheinigung

Gesamt-Brutto	2.124,00	SV-Brutto	2.124,00
Steuer-Brutto	2.124,00	KV-Beitrag	174,16
Lohnsteuer	244,66	RV-Beitrag	200,71
Kirchensteuer	19,57	AV-Beitrag	31,86
Solidaritätszuschlag	13,45	PV-Beitrag	27,08
Steuerfreie Bezüge	.	VWL gesamt	40,00
P. verst. Zuk.sich.	.	Kug-Auszahlung	.
Pfändung Rest	.		
Darlehen Rest	.		

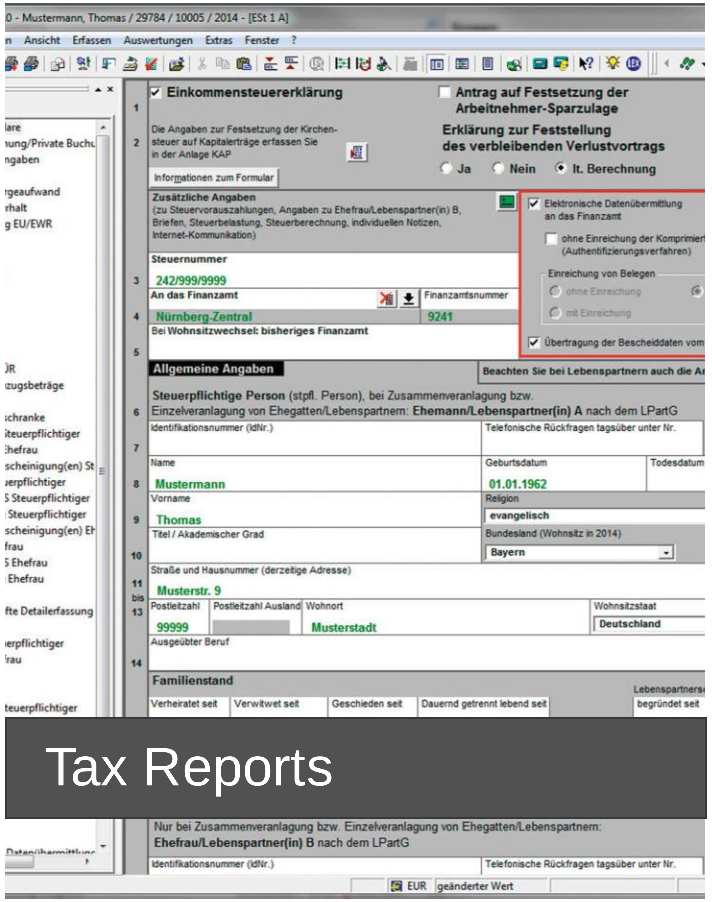
Netto-Bezüge/Netto-Abzüge

Lohnart	Bezeichnung	Betrag
98	Vermögensbildung	40,00-

Bank	11111111 Musterbank	SV-AG-Anteil	Zus. AG-Kosten	Gesamtkosten	Auszahlungsbetrag
Konto	123123123	409,40	44,84	2.578,24	1.372,51

APP Form.-Nr. LOG/11

Salary Reports



0 - Mustermann, Thomas / 29784 / 10005 / 2014 - [ESt 1 A]

lare
nung/Private Buchu
ngaben
rgeaufwand
rhalt
g EU/EWR
ÜR
zugsbeträge
schranke
Steuerpflichtiger
Ehefrau
scheinigung(en) St
uerpflichtiger
S Steuerpflichtiger
Steuerpflichtiger
scheinigung(en) Eh
frau
S Ehefrau
Ehefrau
fte Detailerfassung
uerpflichtiger
frau
teuerpflichtiger
Datenübermittlung

1 ☑ Einkommensteuererklärung

□ Antrag auf Festsetzung der Arbeitnehmer-Sparzulage

2 Die Angaben zur Festsetzung der Kirchensteuer auf Kapitalerträge erfassen Sie in der Anlage KAP

Erklärung zur Feststellung des verbleibenden Verlustvortrags

○ Ja ○ Nein ● lt. Berechnung

Informationen zum Formular

Zusätzliche Angaben
(zu Steuervorauszahlungen, Angaben zu Ehefrau/Lebenspartner(in) B, Briefen, Steuerbelastung, Steuerberechnung, individuellen Notizen, Internet-Kommunikation)

☑ Elektronische Datenübermittlung an das Finanzamt

□ ohne Einreichung der Komprimier (Authentifizierungsverfahren)

Einreichung von Belegen
○ ohne Einreichung
○ mit Einreichung

☑ Übertragung der Bescheiddaten vom

3 Steuernummer: 242/999/9999

4 An das Finanzamt: Nürnberg-Zentral — Finanzamtsnummer: 9241

5 Bei Wohnsitzwechsel: bisheriges Finanzamt

Allgemeine Angaben

Beachten Sie bei Lebenspartnern auch die A

6 Steuerpflichtige Person (stpfl. Person), bei Zusammenveranlagung bzw. Einzelveranlagung von Ehegatten/Lebenspartnern: Ehemann/Lebenspartner(in) A nach dem LPartG

7 Identifikationsnummer (IdNr.) — Telefonische Rückfragen tagsüber unter Nr.

8 Name: Mustermann — Geburtsdatum: 01.01.1962 — Todesdatum

9 Vorname: Thomas — Religion: evangelisch

10 Titel / Akademischer Grad — Bundesland (Wohnsitz in 2014): Bayern

11 bis 13 Straße und Hausnummer (derzeitige Adresse): Musterstr. 9

Postleitzahl: 99999 — Postleitzahl Ausland — Wohnort: Musterstadt — Wohnsitzstaat: Deutschland

14 Ausgeübter Beruf

Familienstand

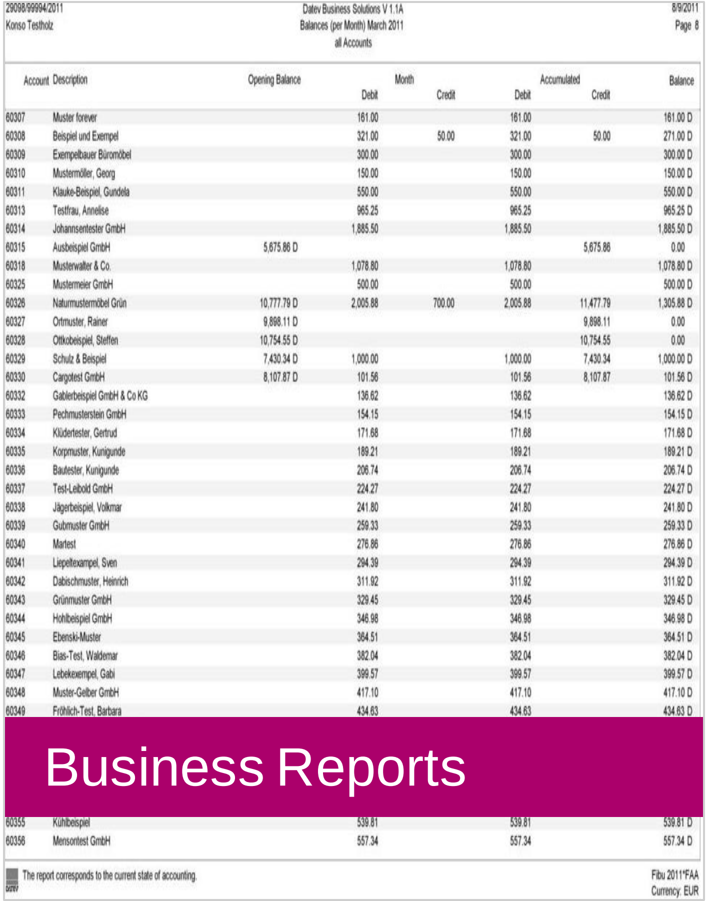
Verheiratet seit — Verwitwet seit — Geschieden seit — Dauernd getrennt lebend seit — Lebenspartners begründet seit

Tax Reports

Nur bei Zusammenveranlagung bzw. Einzelveranlagung von Ehegatten/Lebenspartnern: Ehefrau/Lebenspartner(in) B nach dem LPartG

Identifikationsnummer (IdNr.) — Telefonische Rückfragen tagsüber unter Nr.

EUR geänderter Wert



29098/99994/2011
Konso Testholz

Datev Business Solutions V 1.1A
Balances (per Month) March 2011
all Accounts

8/9/2011
Page 8

Account	Description	Opening Balance	Month Debit	Month Credit	Accumulated Debit	Accumulated Credit	Balance
60307	Muster forever		161.00		161.00		161.00 D
60308	Beispiel und Exempel		321.00	50.00	321.00	50.00	271.00 D
60309	Exempelbauer Büromöbel		300.00		300.00		300.00 D
60310	Mustermöller, Georg		150.00		150.00		150.00 D
60311	Klauke-Beispiel, Gundela		550.00		550.00		550.00 D
60313	Testfrau, Annelise		965.25		965.25		965.25 D
60314	Johannsentester GmbH		1,885.50		1,885.50		1,885.50 D
60315	Ausbeispiel GmbH	5,675.86 D				5,675.86	0.00
60318	Musterwalter & Co.		1,078.80		1,078.80		1,078.80 D
60325	Mustermeier GmbH		500.00		500.00		500.00 D
60326	Naturmustermöbel Grün	10,777.79 D	2,005.88	700.00	2,005.88	11,477.79	1,305.88 D
60327	Ortmuster, Rainer	9,898.11 D				9,898.11	0.00
60328	Ottkobeispiel, Steffen	10,754.55 D				10,754.55	0.00
60329	Schulz & Beispiel	7,430.34 D	1,000.00		1,000.00	7,430.34	1,000.00 D
60330	Cargotest GmbH	8,107.87 D	101.56		101.56	8,107.87	101.56 D
60332	Gablerbeispiel GmbH & Co KG		136.62		136.62		136.62 D
60333	Pechmusterstein GmbH		154.15		154.15		154.15 D
60334	Klüdertester, Gertrud		171.68		171.68		171.68 D
60335	Korpmuster, Kunigunde		189.21		189.21		189.21 D
60336	Bautester, Kunigunde		206.74		206.74		206.74 D
60337	Test-Leibold GmbH		224.27		224.27		224.27 D
60338	Jägerbeispiel, Volkmar		241.80		241.80		241.80 D
60339	Gubmuster GmbH		259.33		259.33		259.33 D
60340	Martest		276.86		276.86		276.86 D
60341	Liepeltexampel, Sven		294.39		294.39		294.39 D
60342	Dabischmuster, Heinrich		311.92		311.92		311.92 D
60343	Grünmuster GmbH		329.45		329.45		329.45 D
60344	Hohlbeispiel GmbH		346.98		346.98		346.98 D
60345	Ebenski-Muster		364.51		364.51		364.51 D
60346	Bias-Test, Waldemar		382.04		382.04		382.04 D
60347	Lebekexempel, Gabi		399.57		399.57		399.57 D
60348	Muster-Gelber GmbH		417.10		417.10		417.10 D
60349	Fröhlich-Test, Barbara		434.63		434.63		434.63 D
60355	Kühlbeispiel		539.81		539.81		539.81 D
60356	Mensontest GmbH		557.34		557.34		557.34 D

DATEV The report corresponds to the current state of accounting.

Fibu 2011*FAA
Currency: EUR

Business Reports

Cyber Defense @DATEV

Strategic goals & approach

DATEV and Attacker

Why we are interesting for the dark side…

Why is DATEV interesting for Attacker?

Fraud -> steal Money

- Changed receiver,…

Espionage -> get customer data

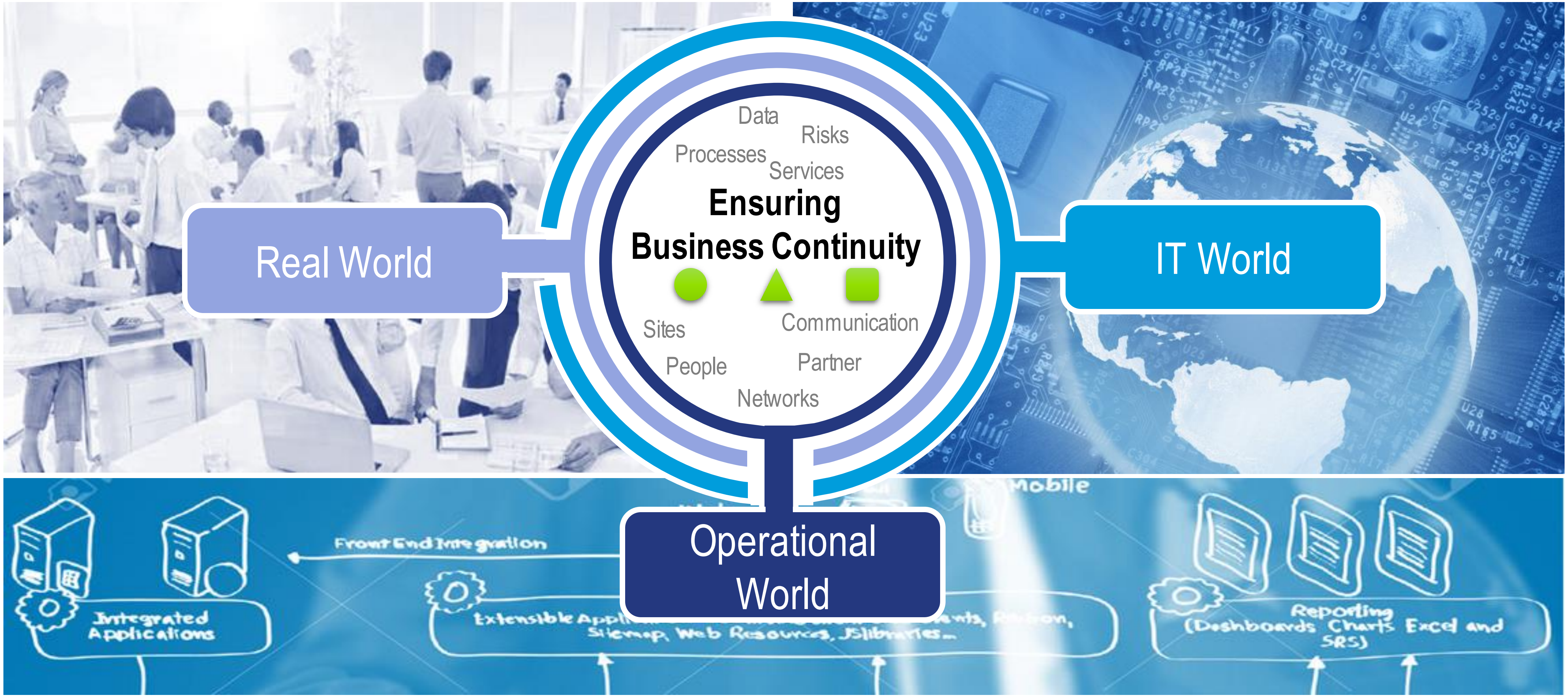
- Date Leakage of customer business information
- CEO/VIP Salary Statements,…

Personally Identifiable Information -> identity theft

- Information on health insurance, confession, tax ID, place of residence, bank connection, vacation days, birthday, salary,…

Our Cyber-Defense Approach

THREE WORLDS, THREE PERSPECTIVES, BUT ONE GOAL



Real World

IT World

Operational World

Data

Risks

Processes

Services

Ensuring Business Continuity

Sites

Communication

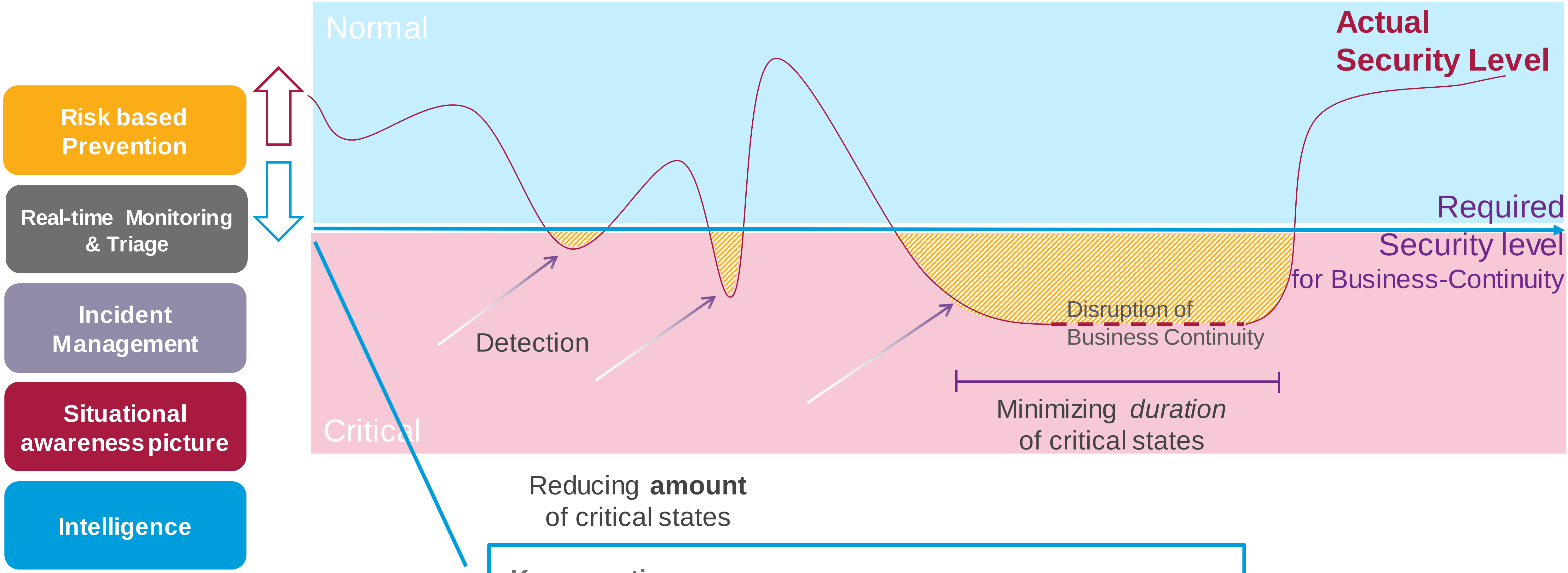
People

Partner

Networks

General Cyber Defense Strategy

Prevention, **Detection, Reaction**, Resilience


Risk based Prevention
Real-time Monitoring & Triage
Incident Management
Situational awareness picture
Intelligence
Normal
Critical
Actual Security Level
Required Security level for Business-Continuity
Detection
Disruption of Business Continuity
Minimizing *duration* of critical states

Reducing **amount** of critical states

Key question:

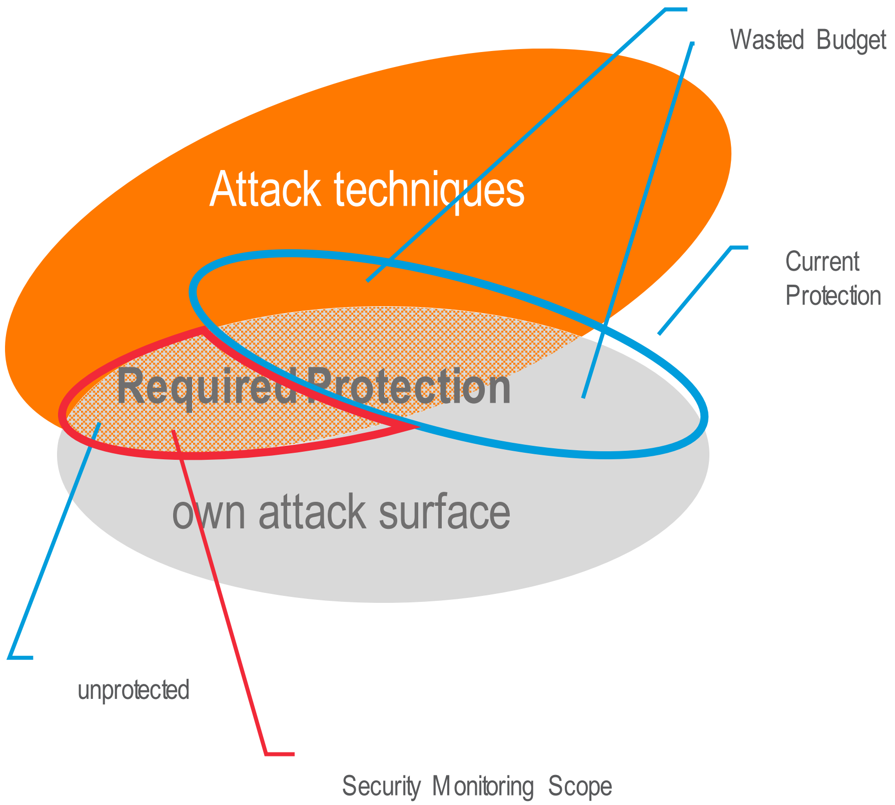
- Where should be the blue line?
- What is the appropriate security level?
- What do we need to detect?
- **How to balance operation, blocking and detection?**

Prioritize the right things

What should we detect?

SOC/Cyber Defense Alignment

Adapting security monitoring to the required scope



If you know

- the attacker,
- the threats,
- used techniques and
- the own attack surface.

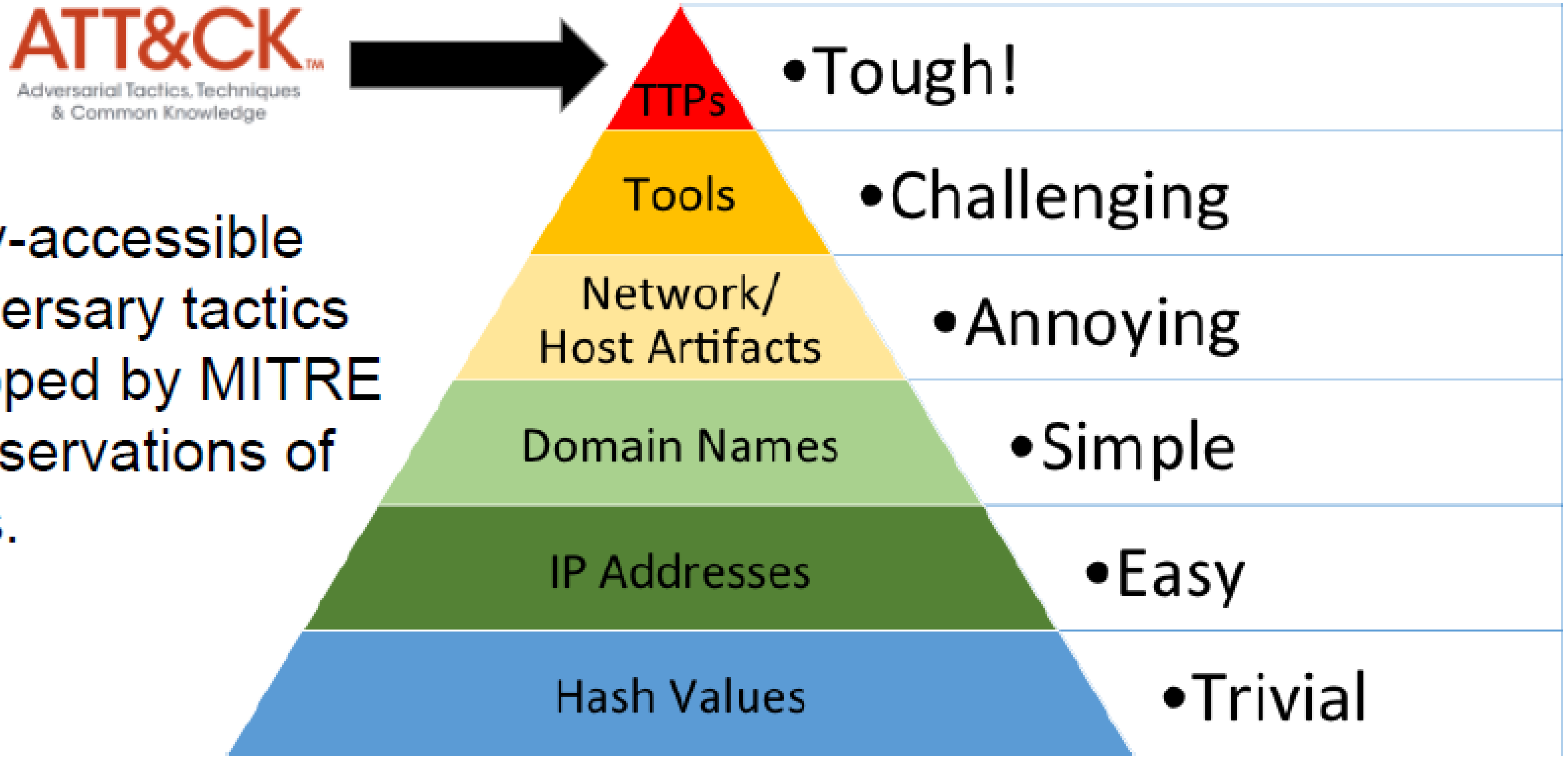
But where to start, if you don’t know?

→ use MITRE ATT&CK

MITRE ATT&CK

Overview on Attacker Techniques and Attack Phases

attack.mitre.org



ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques, developed by MITRE based on real-world observations of adversaries' operations.

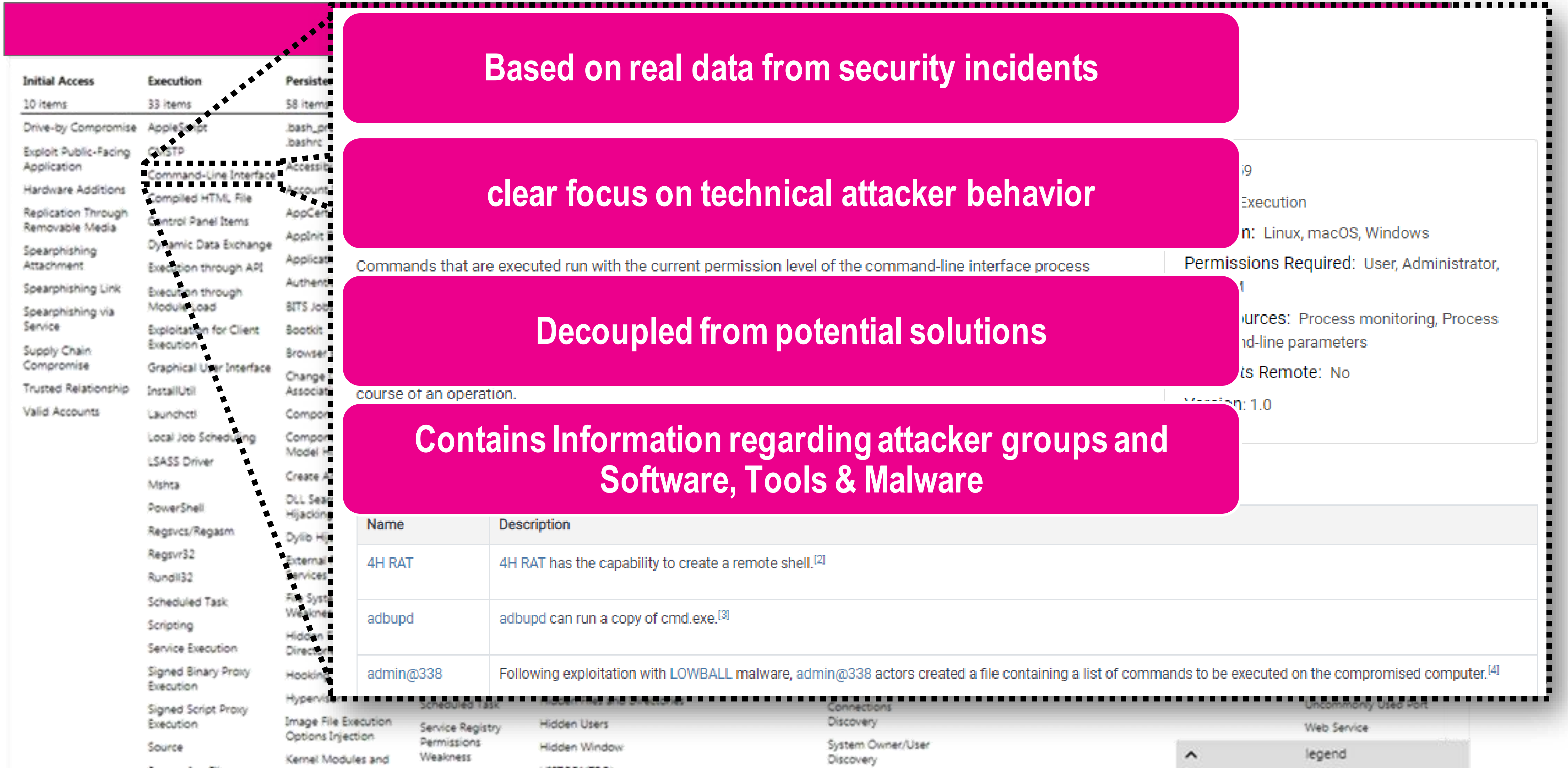
Source: David Bianco

https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

TTPs = Tactics, Techniques, and Procedures

ATT&CK for Enterprise

Attacker Techniques – how a goal is achieved



Based on real data from security incidents

clear focus on technical attacker behavior

Decoupled from potential solutions

Contains Information regarding attacker groups and Software, Tools & Malware

Initial Access
10 items
- Drive-by Compromise
- Exploit Public-Facing Application
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
33 items
- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source

Persiste
58 items
- .bash_pr .bashrc
- Accessib
- Account
- AppCert
- AppInit
- Applicat
- Authent
- BITS Jobs
- Bootkit
- Browser
- Change Associat
- Compon
- Compon Model H
- Create A
- DLL Sear Hijacking
- Dylib Hi
- External Services
- File Syst Weakne
- Hidden Directo
- Hookin
- Hypervis
- Image File Execution Options Injection
- Kernel Modules and

Scheduled Task

Service Registry Permissions Weakness

Hidden Files and Directories

Hidden Users

Hidden Window

Connections Discovery

System Owner/User Discovery

Uncommonly Used Port

Web Service

legend

Commands that are executed run with the current permission level of the command-line interface process

course of an operation.

9

Execution

n: Linux, macOS, Windows

Permissions Required: User, Administrator,

urces: Process monitoring, Process nd-line parameters

ts Remote: No

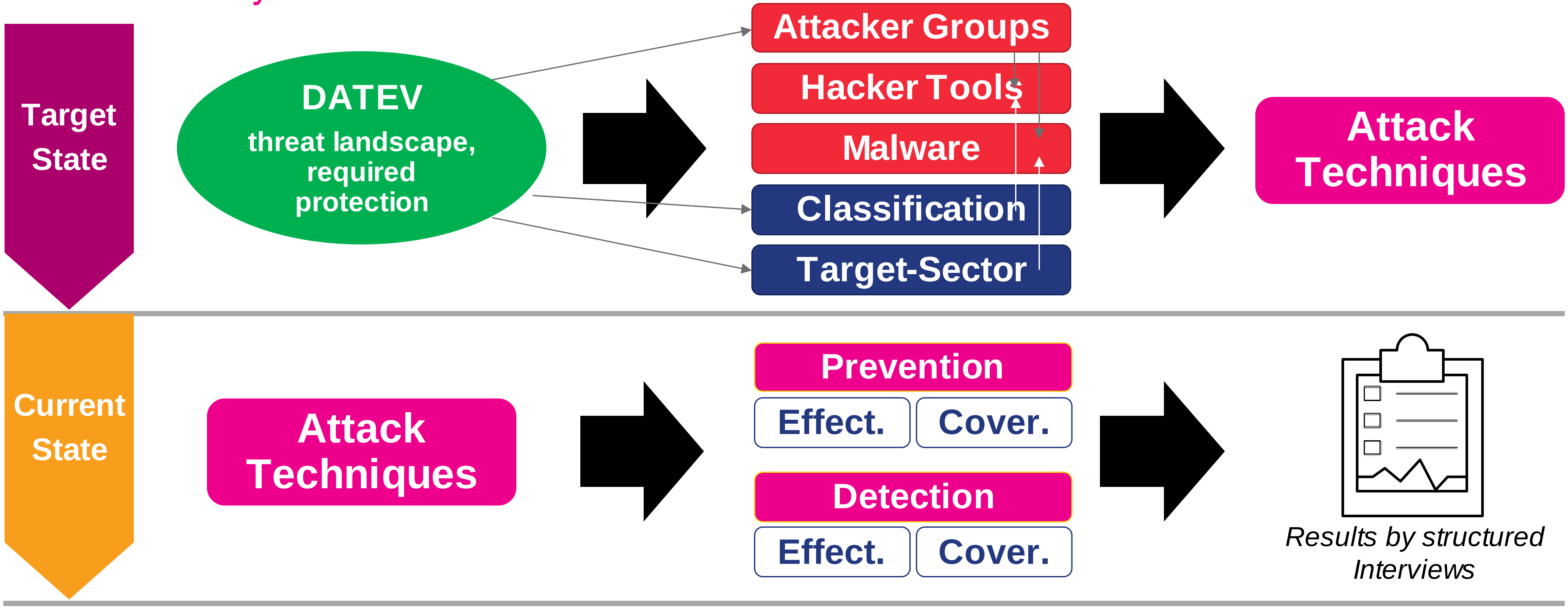
Version: 1.0

Name	Description
4H RAT	4H RAT has the capability to create a remote shell.[2]
adbupd	adbupd can run a copy of cmd.exe.[3]
admin@338	Following exploitation with LOWBALL malware, admin@338 actors created a file containing a list of commands to be executed on the compromised computer.[4]

https://mitre-attack.github.io/attack-navigator/enterprise/

Self Assessment

Know where you are …



Target State

DATEV

threat landscape, required protection

Attacker Groups

Hacker Tools

Malware

Classification

Target-Sector

Attack Techniques

Current State

Attack Techniques

Prevention

Effect. | Cover.

Detection

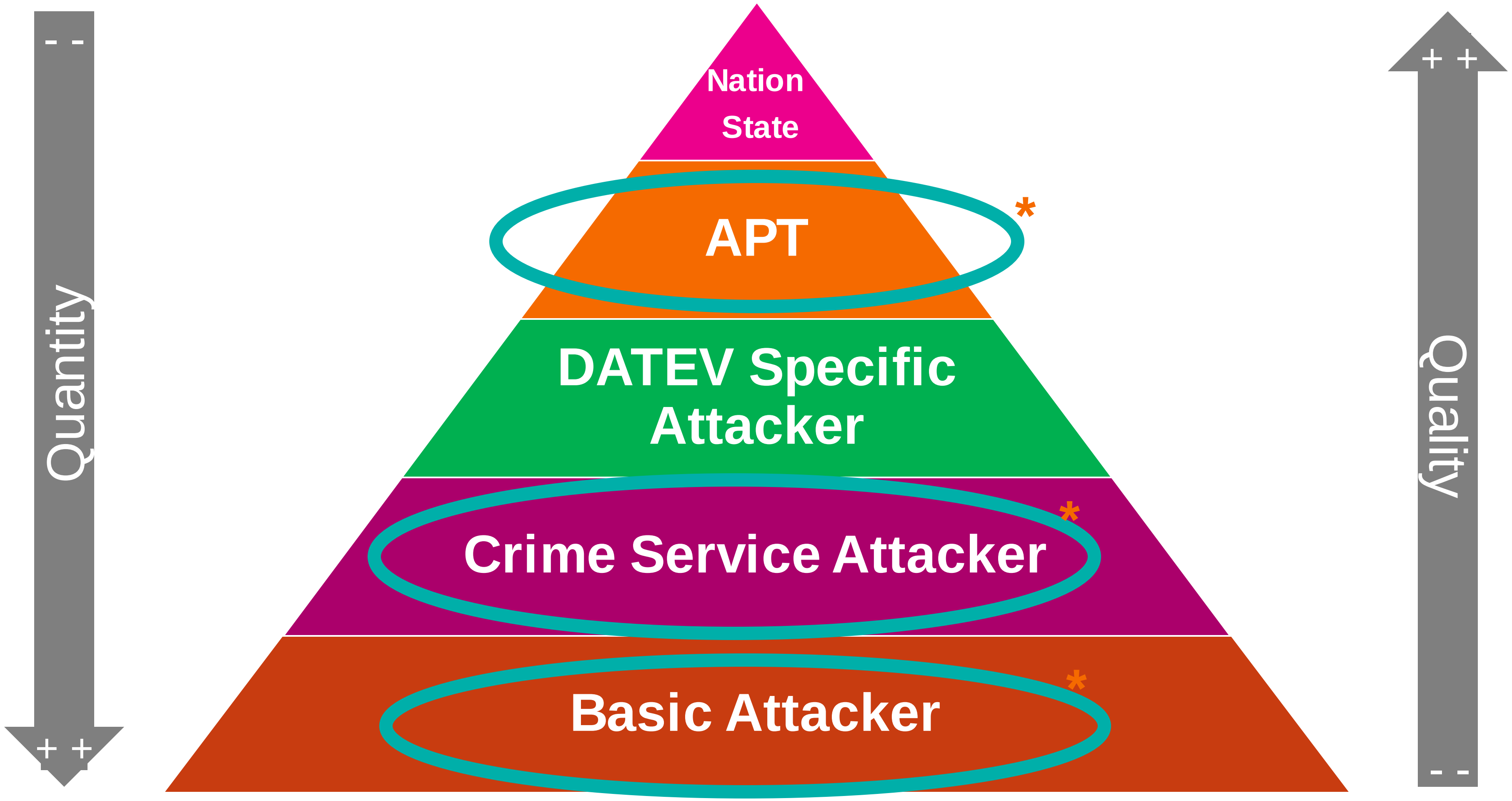
Effect. | Cover.

Results by structured Interviews

Results:

- What is well protected?
- Where are preventive controls failing or missing?

Attacker Classes



- -

Quantity

+ +

Nation State

APT *

DATEV Specific Attacker

Crime Service Attacker *

Basic Attacker *

+ +

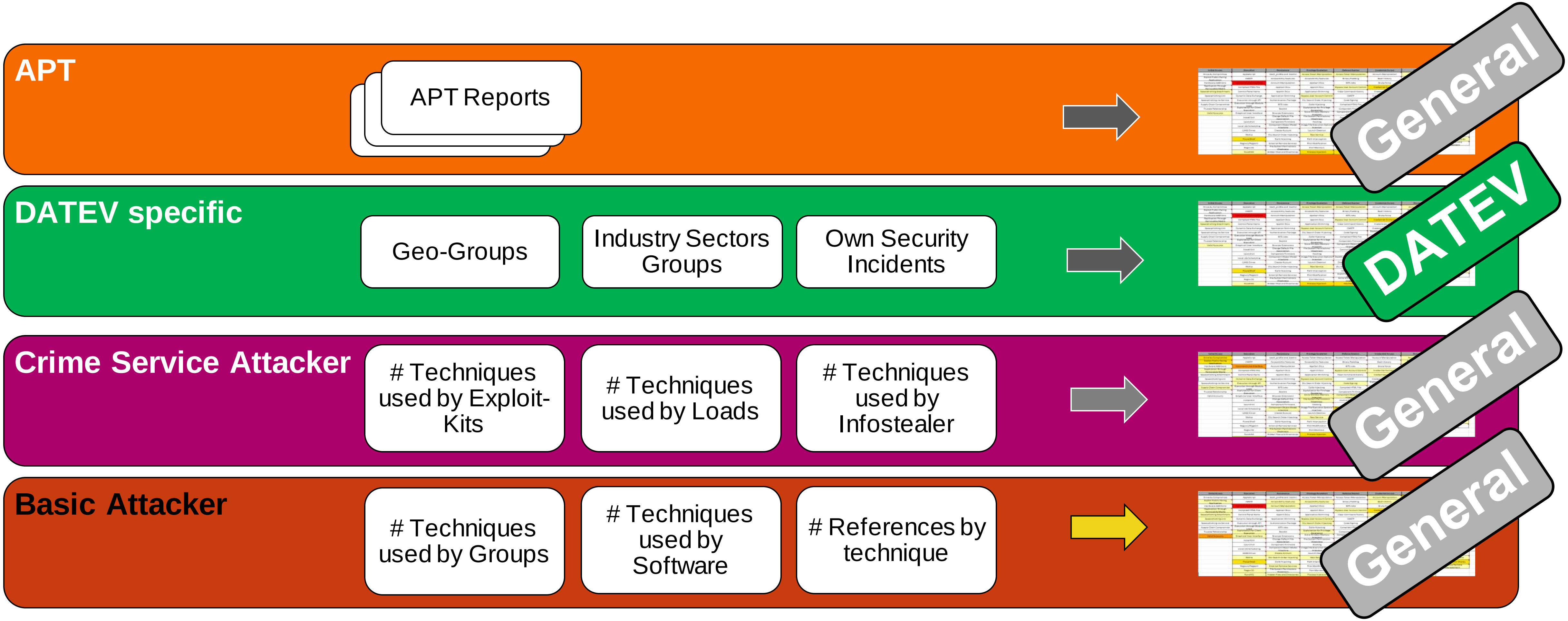
Quality

- -

*We tailor attacker classes specific to industry domains

From Attacker classes to techniques

Which attacker classes uses which techniques?



APT

APT Reports

General

DATEV specific

Geo-Groups

Industry Sectors Groups

Own Security Incidents

DATEV

Crime Service Attacker

# Techniques used by Exploit-Kits

# Techniques used by Loads

# Techniques used by Infostealer

General

Basic Attacker

# Techniques used by Groups

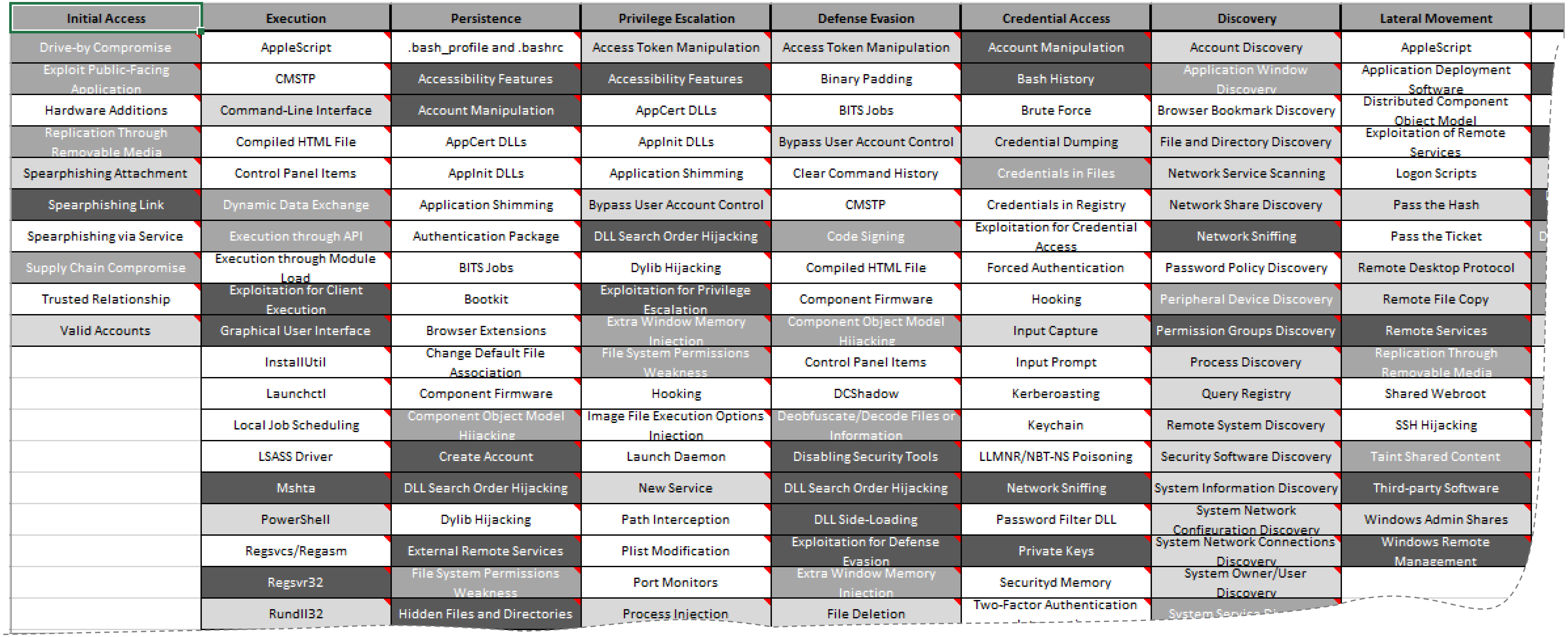
# Techniques used by Software

# References by technique

General

Combined view on all Attacker classes

Without DATEV specifics attacker groups



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery	
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication	System Service Di	

Most used Techniques for the different attacker groups

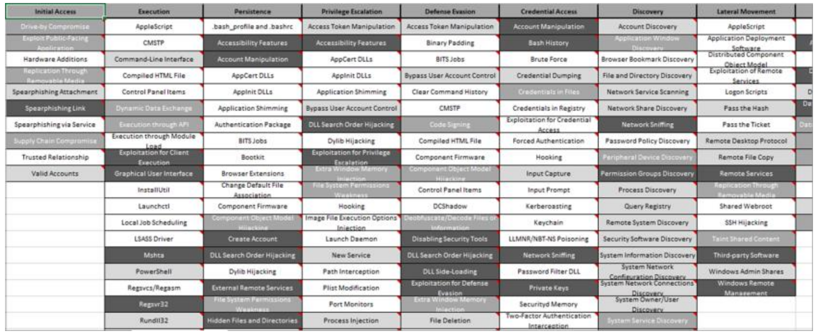
░ basic attacker ▒ crime service attacker ▓ APT

splunk> .conf19

Detection Scope of the SOC

Now we know what we should detect, but what next?

Selected attack techniques



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery	
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery	

How Splunk helped us?

SPL Support: Security Essentials – LogSources, MITRE Mapping,… Analytics Stories

1) Prioritized Log-Sources & Log-Level and Quality
   - Available
   - To be connected & tuned

2) Prioritized SIEM-Rules
   - Available
   - To be developed

3) Prioritized Playbooks
   - Available
   - To be developed

Analysis & Response Workflow

Be fast and use what is there…

SOC & Cyber Defense Challenges

Cyber Defense is an organization performance

Be fast! You have to be fast as an organization to avoid reputation loss, brand damage and other cyber attack impacts

To be fast, requires that analysis and response parties are fast.

Several operational units with different working modes

- All have to work with the same tools
- Already common tools in use

Workflow: Splunk → Tier 1 → Tier 2 → Operational Unit → Feedback loop

Playbooks with RACI Matrix

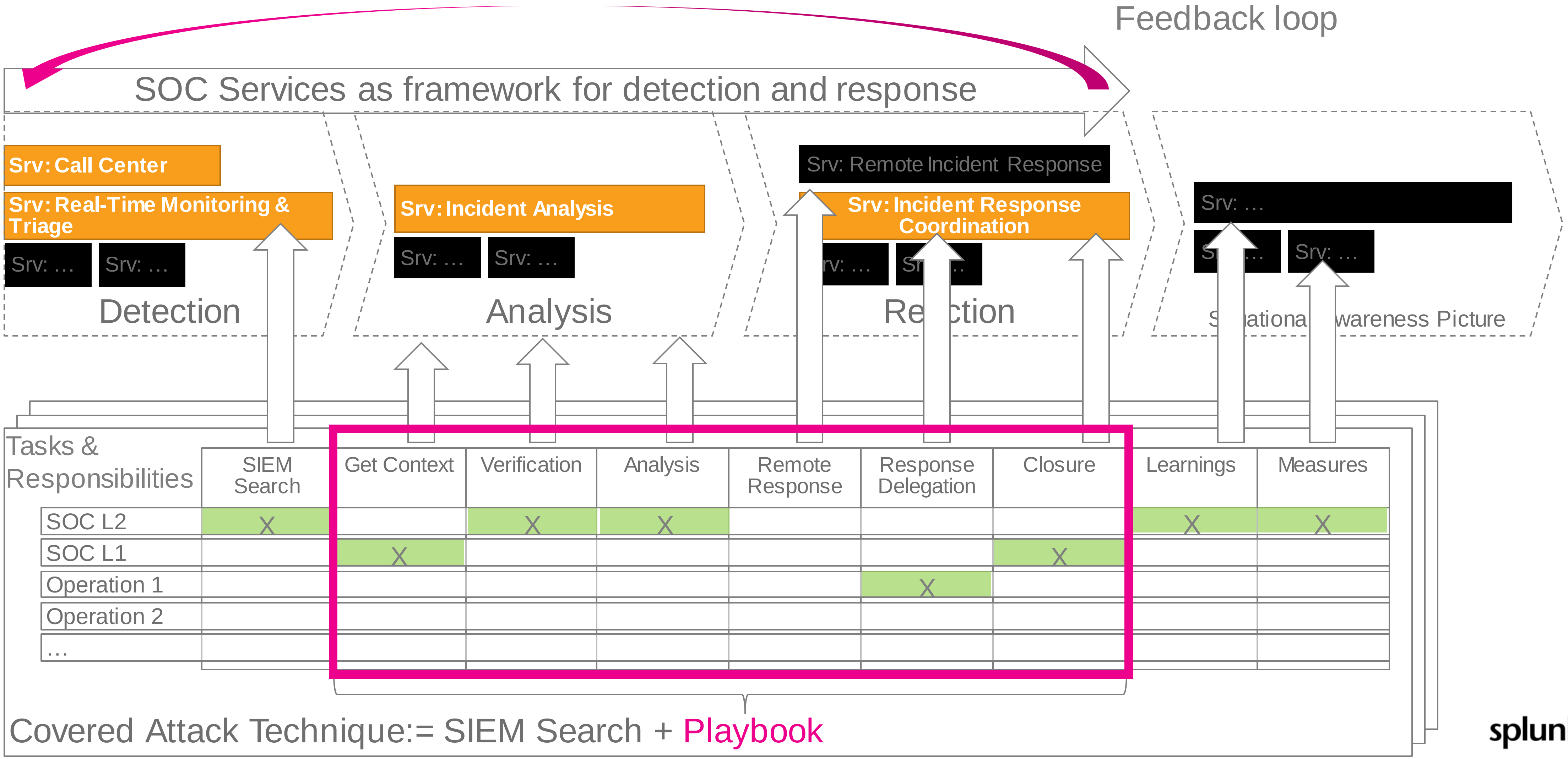
Common KPIs over all entities

What: ShimCache, AmCache, Scheduled tasks, Process list, Services, Drivers, Autoruns • Prefetch, Browser history, Hash of running processes, downloaded files, open network connections • Event logs • Command line history • AV, HIDS, HIPS logs

How: GRR, **PsRecon**, CrowdResponse

SOC-Services, Playbooks, Responsibilities

Who does when what?

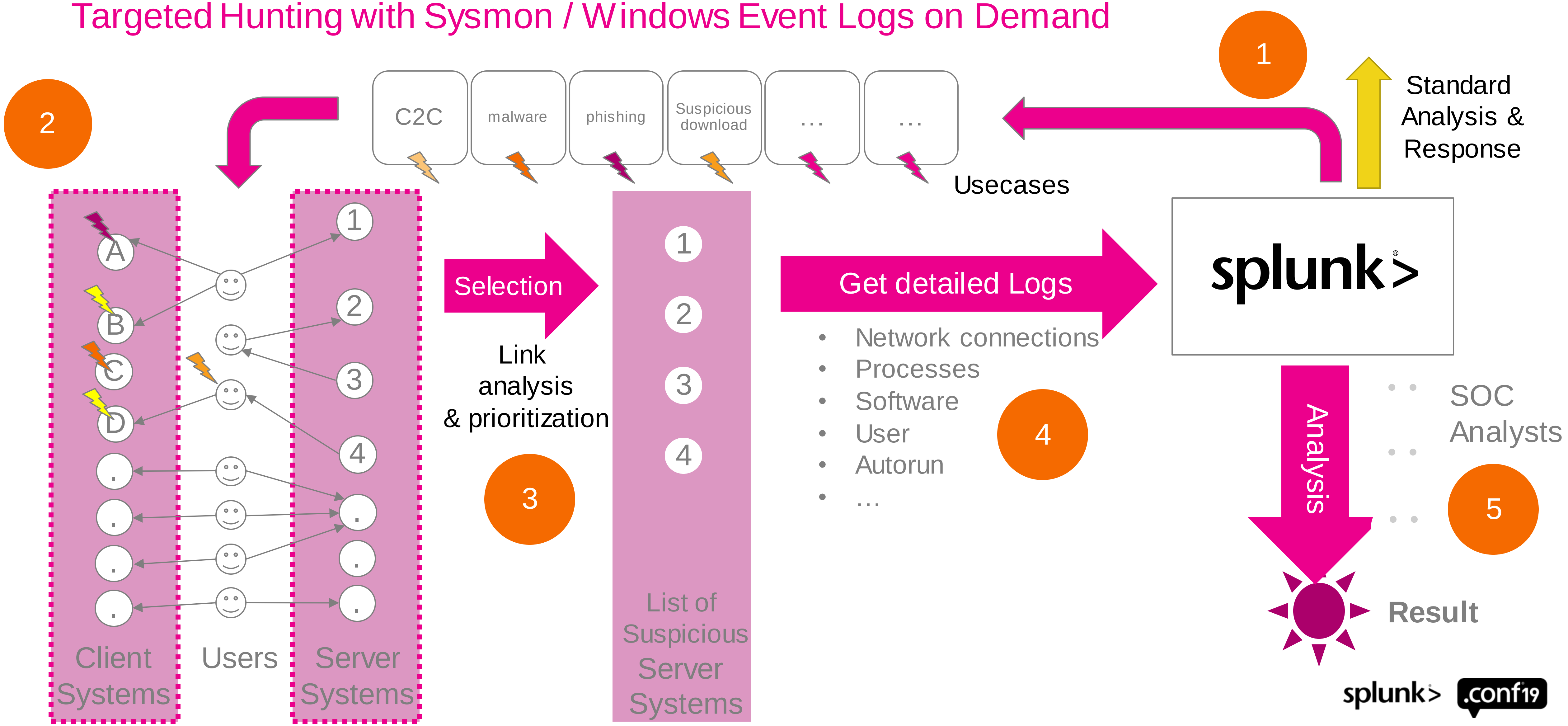

Feedback loop
SOC Services as framework for detection and response
Srv: Call Center
Srv: Real-Time Monitoring & Triage
Srv: …
Srv: …
Detection
Srv: Incident Analysis
Srv: …
Srv: …
Analysis
Srv: Remote Incident Response
Srv: Incident Response Coordination
Srv: …
Srv: …
Reaction
Srv: …
Srv: …
Srv: …
Situational Awareness Picture

Tasks & Responsibilities	SIEM Search	Get Context	Verification	Analysis	Remote Response	Response Delegation	Closure	Learnings	Measures
SOC L2	X		X	X				X	X
SOC L1		X					X		
Operation 1						X			
Operation 2									
…									

Covered Attack Technique:= SIEM Search + Playbook

Endpoint and User are Key

Targeted Hunting with Sysmon / Windows Event Logs on Demand



1 Standard Analysis & Response

C2C | malware | phishing | Suspicious download | … | …

Usecases

2 Client Systems | Users | Server Systems

Selection

Link analysis & prioritization

3

List of Suspicious Server Systems

Get detailed Logs

- Network connections
- Processes
- Software
- User
- Autorun
- …

4

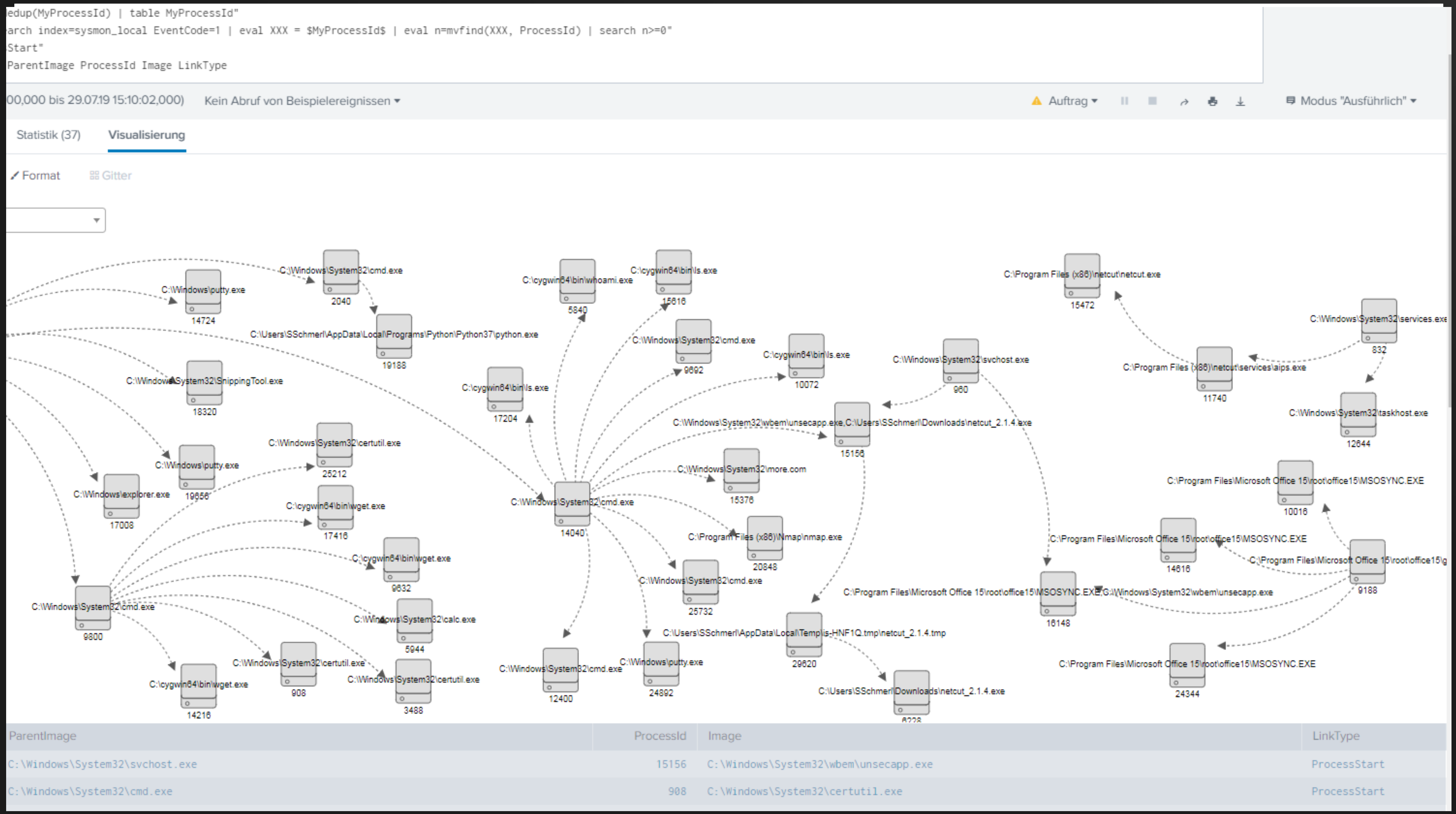
splunk>

Analysis

SOC Analysts

5

Result



```
edup(MyProcessId) | table MyProcessId"
arch index=sysmon_local EventCode=1 | eval XXX = $MyProcessId$ | eval n=mvfind(XXX, ProcessId) | search n>=0"
Start"
ParentImage ProcessId Image LinkType
```

00,000 bis 29.07.19 15:10:02,000)
Kein Abruf von Beispielereignissen ▾
Auftrag ▾
Modus "Ausführlich" ▾
Statistik (37)
Visualisierung
Format
Gitter
C:\Windows\System32\cmd.exe
2040
C:\Windows\putty.exe
14724
C:\Users\SSchmerl\AppData\Local\Programs\Python\Python37\python.exe
19188
C:\Windows\System32\SnippingTool.exe
18320
C:\Windows\System32\certutil.exe
25212
C:\Windows\putty.exe
19656
C:\Windows\explorer.exe
17008
C:\cygwin64\bin\wget.exe
17416
C:\cygwin64\bin\wget.exe
9632
C:\Windows\System32\cmd.exe
9800
C:\Windows\System32\calc.exe
5944
C:\Windows\System32\certutil.exe
908
C:\Windows\System32\certutil.exe
3488
C:\cygwin64\bin\wget.exe
14216
C:\cygwin64\bin\whoami.exe
5840
C:\cygwin64\bin\ls.exe
15616
C:\Windows\System32\cmd.exe
9692
C:\cygwin64\bin\ls.exe
10072
C:\cygwin64\bin\ls.exe
17204
C:\Windows\System32\svchost.exe
960
C:\Windows\System32\wbem\unsecapp.exe,C:\Users\SSchmerl\Downloads\netcut_2.1.4.exe
15156
C:\Windows\System32\more.com
15376
C:\Windows\System32\cmd.exe
14040
C:\Program Files (x86)\Nmap\nmap.exe
20848
C:\Windows\System32\cmd.exe
25732
C:\Users\SSchmerl\AppData\Local\Temp\is-HNF1Q.tmp\netcut_2.1.4.tmp
29620
C:\Windows\System32\cmd.exe
12400
C:\Windows\putty.exe
24892
C:\Users\SSchmerl\Downloads\netcut_2.1.4.exe
6228
C:\Program Files (x86)\netcut\netcut.exe
15472
C:\Windows\System32\services.exe
832
C:\Program Files (x86)\netcut\services\aips.exe
11740
C:\Windows\System32\taskhost.exe
12644
C:\Program Files\Microsoft Office 15\root\office15\MSOSYNC.EXE
10016
C:\Program Files\Microsoft Office 15\root\office15\MSOSYNC.EXE
14616
C:\Program Files\Microsoft Office 15\root\office15\g
9188
C:\Program Files\Microsoft Office 15\root\office15\MSOSYNC.EXE,C:\Windows\System32\wbem\unsecapp.exe
16148
C:\Program Files\Microsoft Office 15\root\office15\MSOSYNC.EXE
24344

ParentImage	ProcessId	Image	LinkType
C:\Windows\System32\svchost.exe	15156	C:\Windows\System32\wbem\unsecapp.exe	ProcessStart
C:\Windows\System32\cmd.exe	908	C:\Windows\System32\certutil.exe	ProcessStart

Real-Time Monitoring & Triage

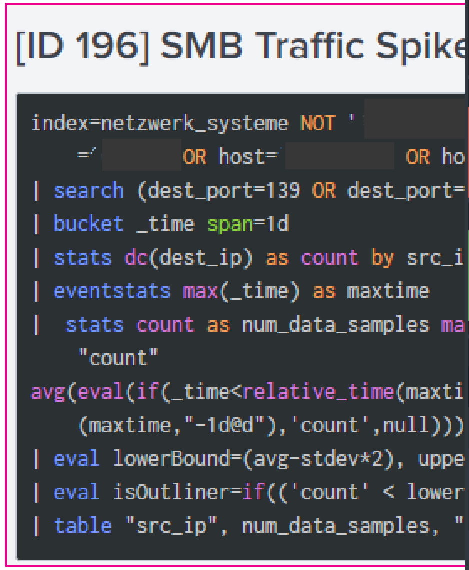
SIEM Splunk Rule to Ticket

Step 01
Build up the search and make an Alert

Step 02
Integrate that in the Splunk MITRE Framework

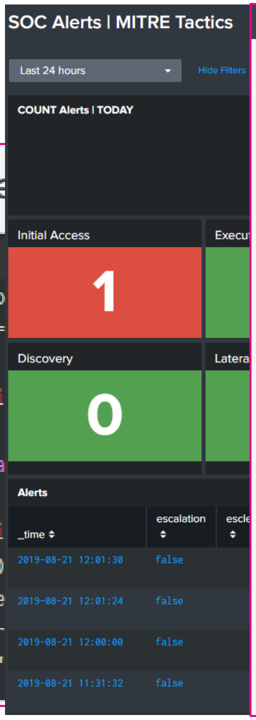
Step 03
Prioritize the alerts based on impact and urgency

Step 04
open a ticket with all the necessary information



[ID 196] SMB Traffic Spike

```
index=netzwerk_systeme NOT ' [redacted]
   =' [redacted] OR host= [redacted] OR ho
| search (dest_port=139 OR dest_port=
| bucket _time span=1d
| stats dc(dest_ip) as count by src_i
| eventstats max(_time) as maxtime
|  stats count as num_data_samples ma
   "count"
avg(eval(if(_time<relative_time(maxti
   (maxtime,"-1d@d"),'count',null)))
| eval lowerBound=(avg-stdev*2), uppe
| eval isOutliner=if(('count' < lower
| table "src_ip", num_data_samples, "
```



SOC Alerts | MITRE Tactics

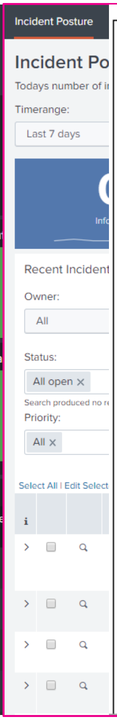
COUNT Alerts | TODAY

Initial Access	Execu
1	

Discovery	Latera
0	

Alerts

_time	escalation	escle
2019-08-21 12:01:30	false	
2019-08-21 12:01:24	false	
2019-08-21 12:00:00	false	
2019-08-21 11:31:32	false	



Incident Posture

Incident Po

Todays number of i

Timerange: Last 7 days

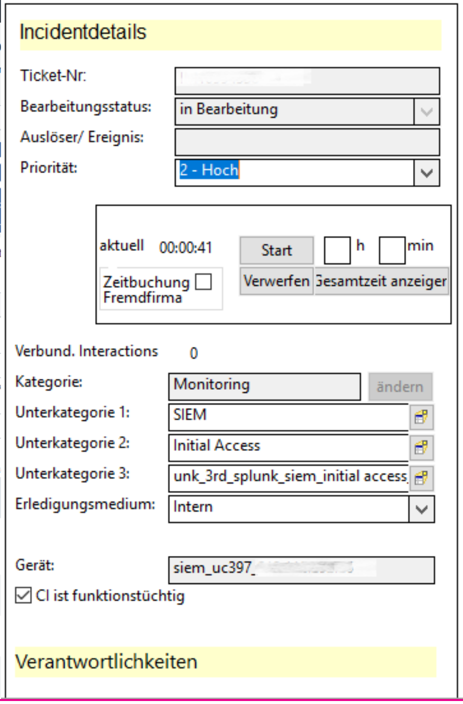
Recent Incident

Owner: All

Status: All open ×

Search produced no r

Priority: All ×



Incidentdetails

Ticket-Nr:	[redacted]
Bearbeitungsstatus:	in Bearbeitung
Auslöser/ Ereignis:	
Priorität:	2 - Hoch

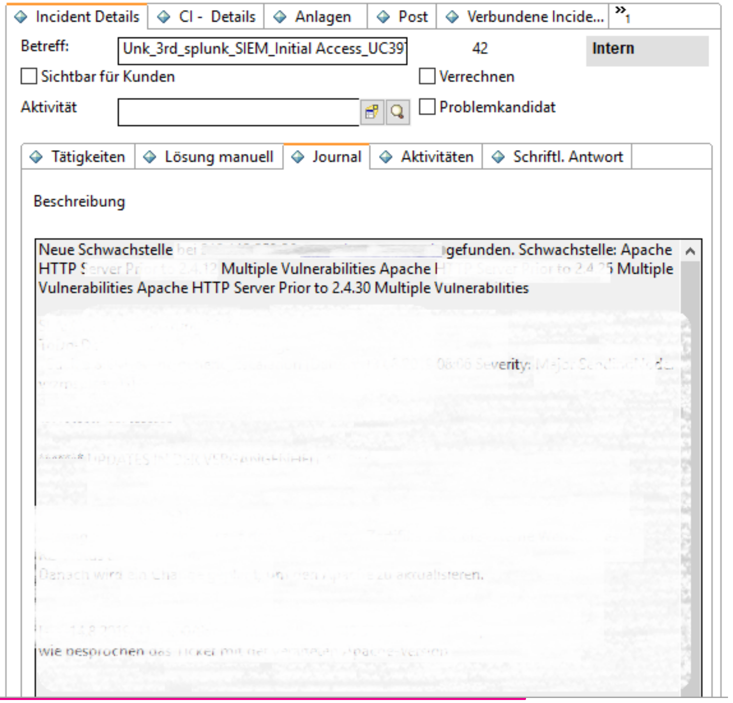
aktuell 00:00:41 Start □ h □ min

Zeitbuchung Fremdfirma □ Verwerfen Gesamtzeit anzeigen

Verbund. Interactions	0
Kategorie:	Monitoring
Unterkategorie 1:	SIEM
Unterkategorie 2:	Initial Access
Unterkategorie 3:	unk_3rd_splunk_siem_initial access
Erledigungsmedium:	Intern
Gerät:	siem_uc397_ [redacted]

☑ CI ist funktionstüchtig

Verantwortlichkeiten



Betreff: Unk_3rd_splunk_SIEM_Initial Access_UC39 42 Intern

□ Sichtbar für Kunden □ Verrechnen

Aktivität □ Problemkandidat

Beschreibung

Neue Schwachstelle [redacted] gefunden. Schwachstelle: Apache HTTP S [redacted] Multiple Vulnerabilities Apache H [redacted] Multiple Vulnerabilities Apache HTTP Server Prior to 2.4.30 Multiple Vulnerabilities

[redacted]

splunk> .conf19

Incident Analysis

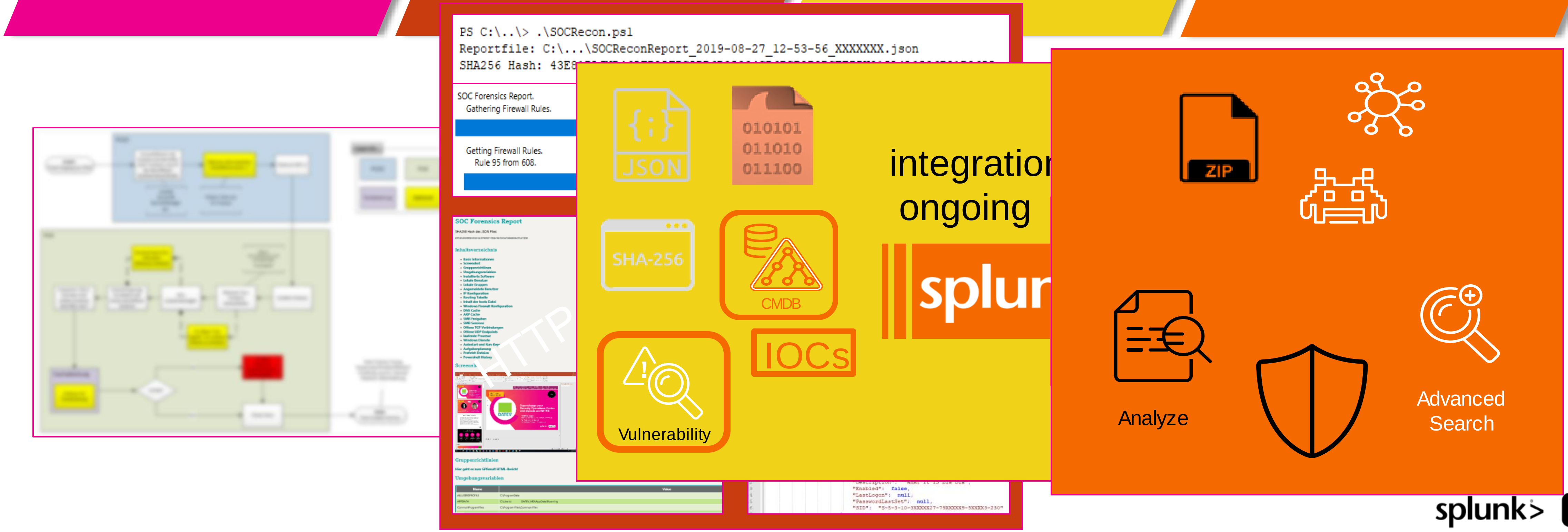
How we handle this

Step 05
Analyst have a link in the Ticket to the Playbook

Step 06
Analyst “get Context” form the system

Step 07
put all the stuff into Splunk

Step 08
analyze and evaluate the data



```
PS C:\..\> .\SOCRecon.psl
Reportfile: C:\...\SOCReconReport_2019-08-27_12-53-56_XXXXXXX.json
SHA256 Hash: 43E8
```

SOC Forensics Report.
Gathering Firewall Rules.

Getting Firewall Rules.
Rule 95 from 608.

SOC Forensics Report

SHA256 Hash des JSON Files:

Inhaltsverzeichnis

- Basis Informationen
- Screenshot
- Gruppenrichtlinien
- Umgebungsvariablen
- Installierte Software
- Lokale Benutzer
- Lokale Gruppen
- Angemeldete Benutzer
- IP Konfiguration
- Routing Tabelle
- Inhalt der hosts Datei
- Windows Firewall Konfiguration
- DNS Cache
- ARP Cache
- SMB Freigaben
- SMB Sessions
- Offene TCP Verbindungen
- Offene UDP Endpoints
- laufende Prozesse
- Windows Dienste
- Autostart und Run-Keys
- Aufgabenplanung
- Prefetch Dateien
- Powershell History

Screensh

Gruppenrichtlinien

Hier geht es zum GPResult HTML-Bericht

Umgebungsvariablen

Name	Value
ALLUSERSPROFILE	C:\ProgramData
APPDATA	C:\Users\ DATEV_MD\AppData\Roaming
CommonProgramFiles	C:\Program Files\Common Files

```
"Description":  "What it is bla bla",
"Enabled":  false,
"LastLogon":  null,
"PasswordLastSet":  null,
"SID":  "S-5-3-10-3XXXXX27-79XXXXX9-5XXXX3-230"
```

integration ongoing

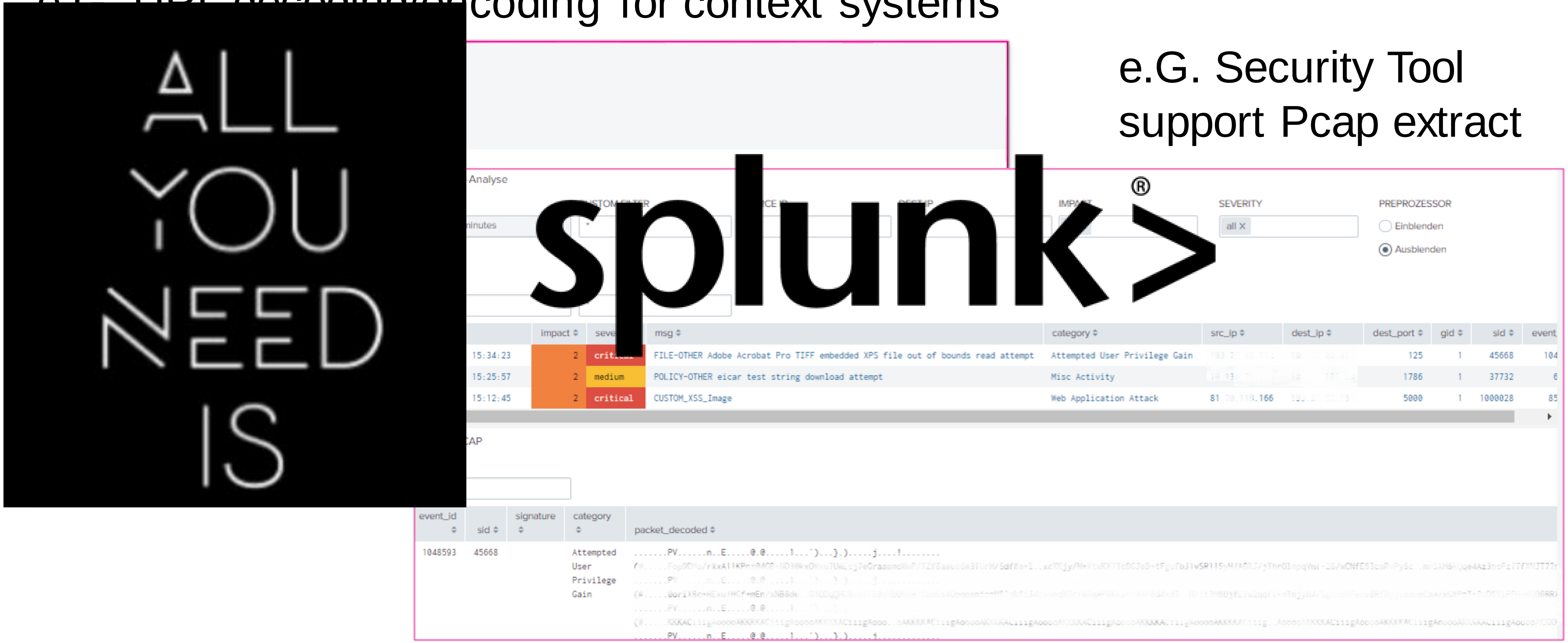
Analyze

Advanced Search

Dashboards

for analysts

- e.G. URL decoding/encoding for context systems



Analyse

CUSTOM FILTER · SOURCE IP · DEST IP · IMPACT · SEVERITY · PREPROZESSOR

minutes

SEVERITY: all X

PREPROZESSOR: ○ Einblenden ● Ausblenden

	impact	severity	msg	category	src_ip	dest_ip	dest_port	gid	sid	event
15:34:23	2	critical	FILE-OTHER Adobe Acrobat Pro TIFF embedded XPS file out of bounds read attempt	Attempted User Privilege Gain	[redacted]	[redacted]	125	1	45668	104
15:25:57	2	medium	POLICY-OTHER eicar test string download attempt	Misc Activity	[redacted]	[redacted]	1786	1	37732	6
15:12:45	2	critical	CUSTOM_XSS_Image	Web Application Attack	81.[redacted].166	[redacted]	5000	1	1000028	85

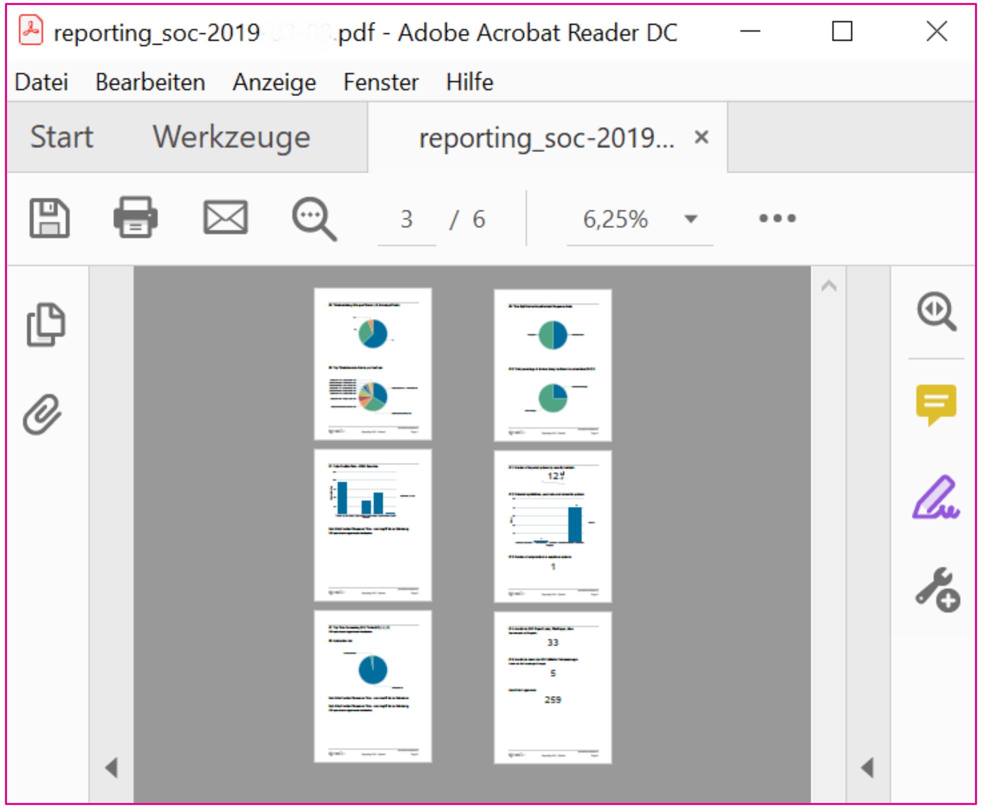
CAP

event_id	sid	signature	category	packet_decoded
1048593	45668		Attempted User Privilege Gain	.......PV......n..E.....@.@.....1...`)...}.)......j....!........ (#.....[redacted] ....PV......n..E.....@.@.....1...[redacted] (#.....0oriX8c+HExu!HGf+mEn/xNB8de[redacted] ....PV......n..E.....@.@.....[redacted] (#.....KKKAC1iigAooooAKKKKAC1iigAooooAKKKKAC1iigAooo..oAKKKKAC1iigAooooAKKKKAC1iigAooooAKKKKAC1iigAooooAKKKKAC1iigAooooAKKKKAC1iig..AooooAKKKKAC1iigAooooAKKKKAC1iigAooooAKKKKAC1iigAoooo ....PV......n..E.....@.@.....1...`)...}.)......j............

e.G. Security Tool support Pcap extract

Dashboards

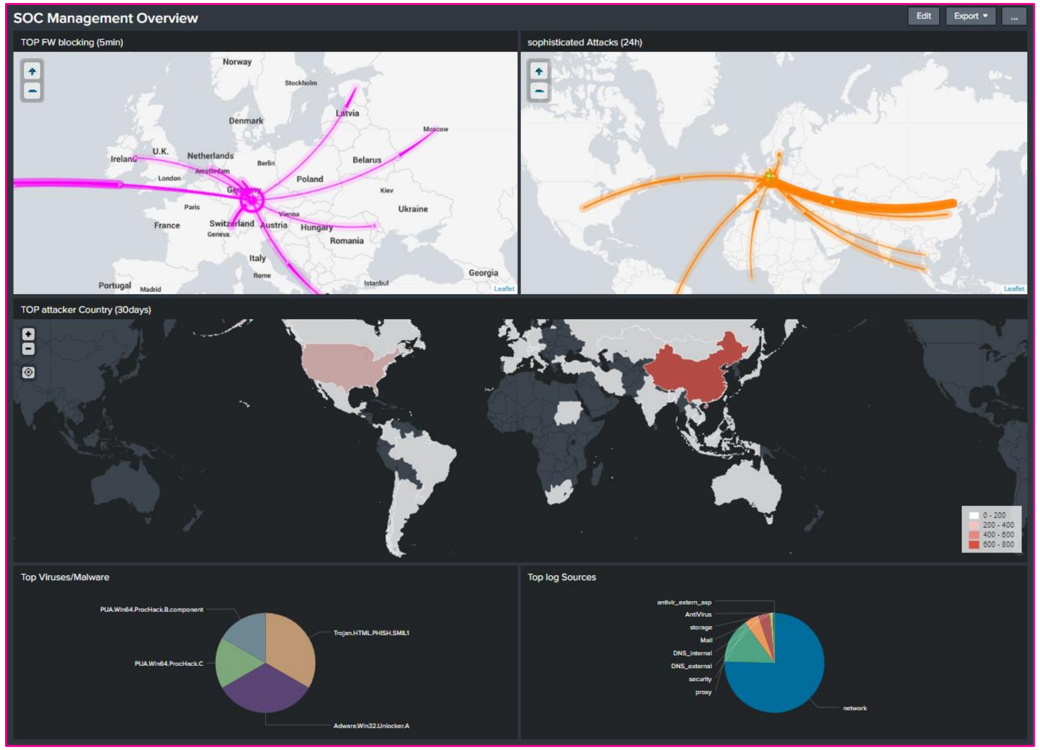
for Manager



☹

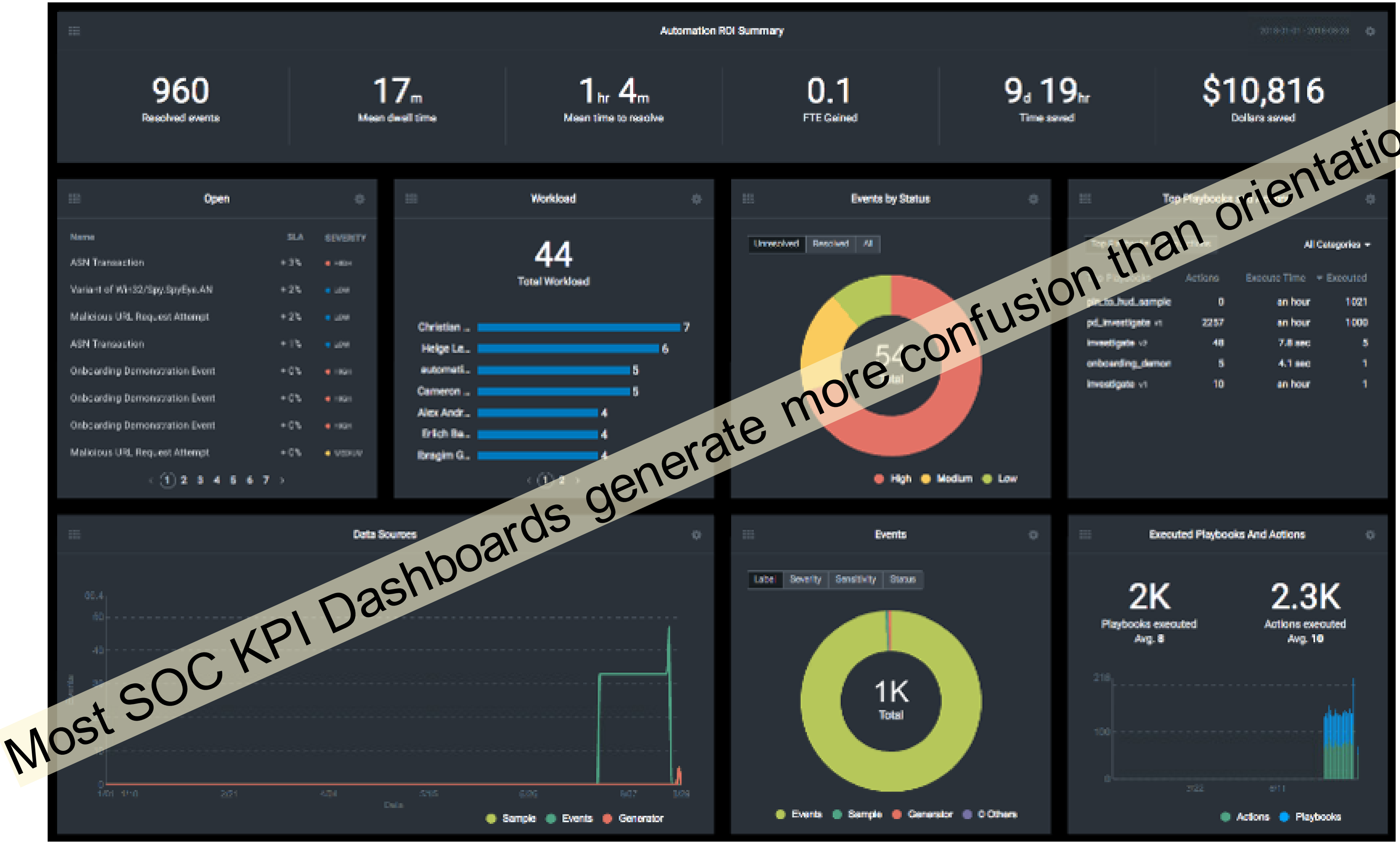
😐

☺



SOC KPIs

Cyber Defense and SOC is a company Performance



Automation ROI Summary

960 Resolved events | 17m Mean dwell time | 1hr 4m Mean time to resolve | 0.1 FTE Gained | 9d 19hr Time saved | $10,816 Dollars saved

Open

Name	SLA	SEVERITY
ASN Transaction	+ 3%	● HIGH
Variant of Win32/Spy.SpyEye.AN	+ 2%	● LOW
Malicious URL Request Attempt	+ 2%	● LOW
ASN Transaction	+ 1%	● LOW
Onboarding Demonstration Event	+ 0%	● HIGH
Onboarding Demonstration Event	+ 0%	● HIGH
Onboarding Demonstration Event	+ 0%	● HIGH
Malicious URL Request Attempt	+ 0%	● MEDIUM

‹ 1 2 3 4 5 6 7 ›

Workload

44 Total Workload

Top Playbooks and Actions

All Categories ▾

Top Playbooks	Actions	Execute Time	▾ Executed
pin_to_hud_sample	0	an hour	1021
pd_investigate v1	2257	an hour	1000
investigate v2	48	7.8 sec	5
onboarding_demor	5	4.1 sec	1
investigate v1	10	an hour	1

Executed Playbooks And Actions

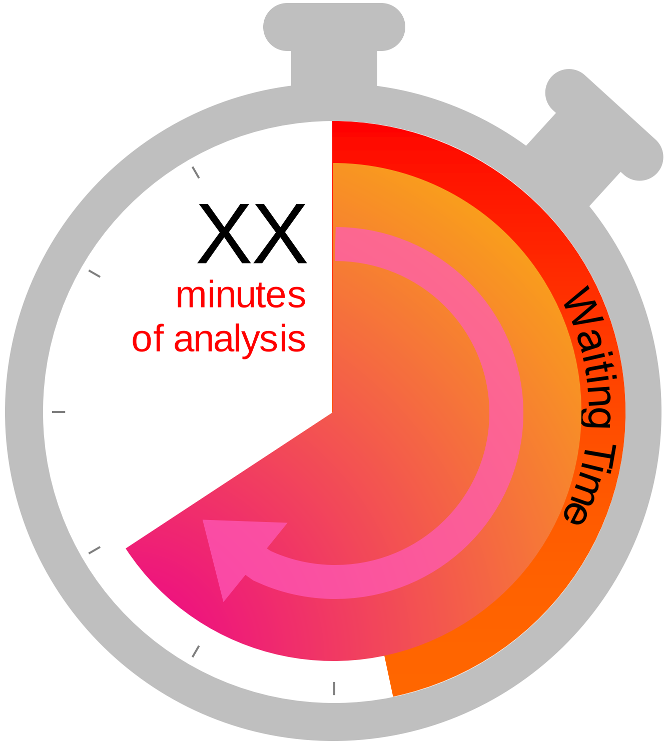
2K Playbooks executed Avg. 8

2.3K Actions executed Avg. 10

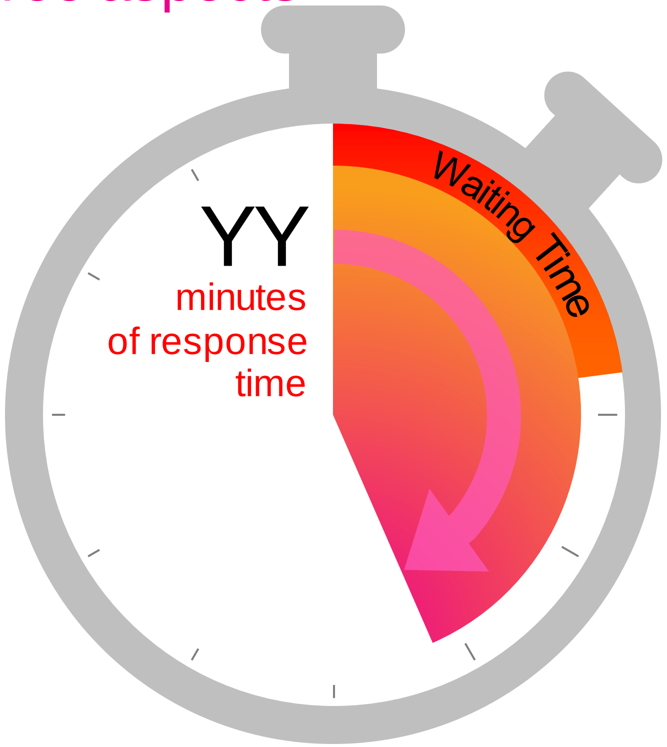
Most SOC KPI Dashboards generate more confusion than orientation

SOC KPIs

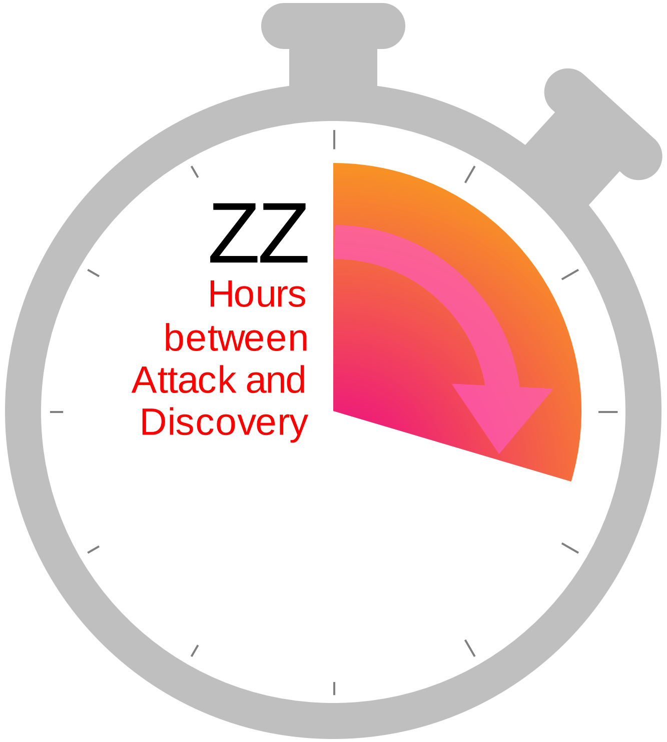
therefore we concentrate on three aspects



End to end **Analysis time**
(measure us and operational units)



End to end **Response Time**
(measure operational units)



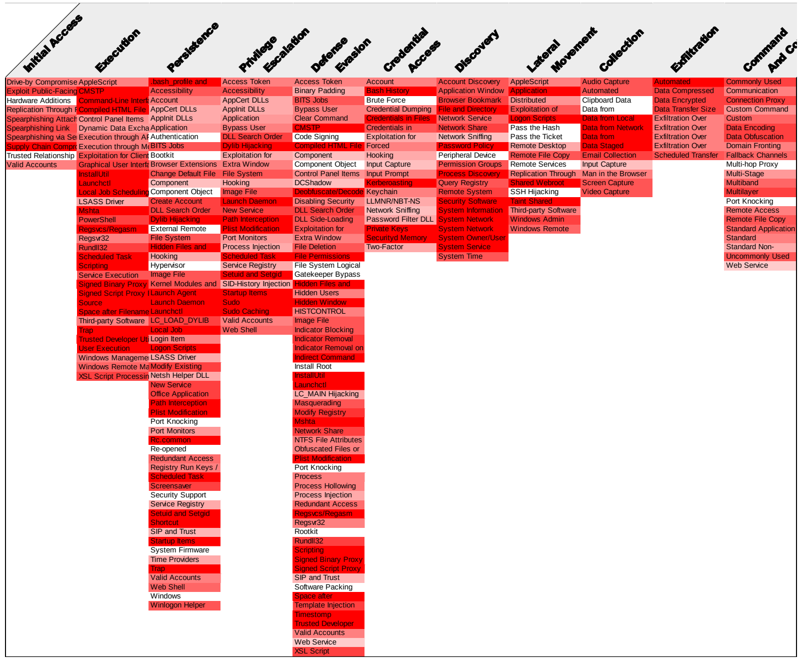
Attacker Turnaround time
(measures the Dwell Time + Analysis to reduce the recognition time of Attacks)

Biggest enemy for SOC is waiting

SOC KPIs

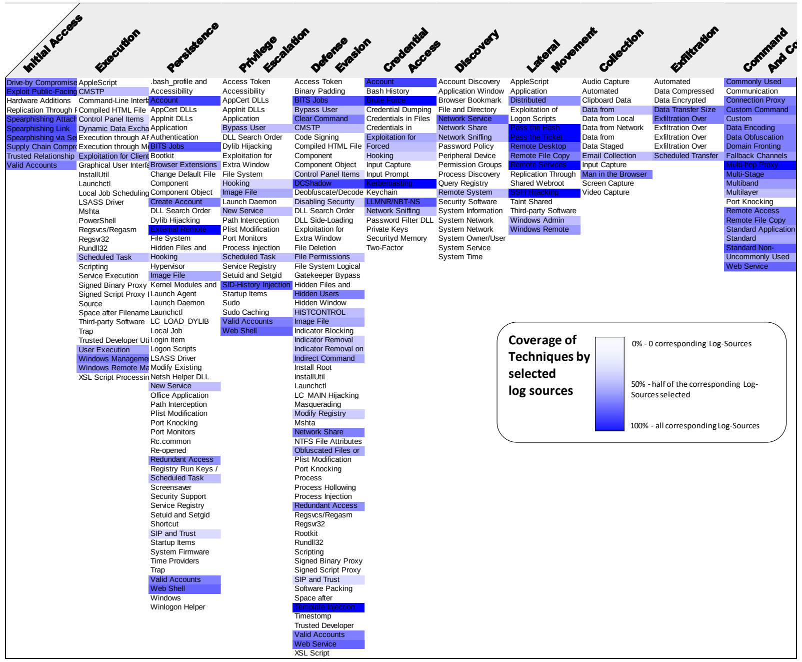
Coverage (measure SOC detection performance)

Target Scope



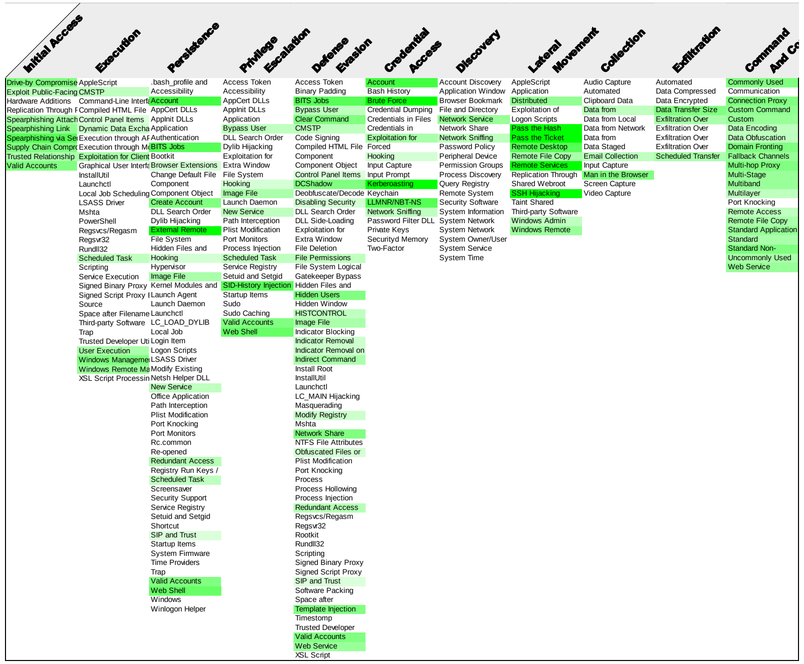
coverage of
196 Techniques
With 13 Mitre Log-Sources

Current Logs



6874 from ~60.000 log-sources
In sufficient log-quality & coverage
→Detection Potential: 103 techniques

Current Detections



80 from 196 techniques

All numbers are not real and just explaining the principle

For us useful Apps…

Alert Manager

Qualys Technology Add-on (TA) for Splunk

Cisco Networks App for Splunk Enterprise

Missile Map 😞😐🙂

Splunk ES Content Update

JellyFisher

Network Topology - Custom Visualization

App for IP Address and CIDR operations

Knowledge Sharing

Promote the
Cyber Defense topic

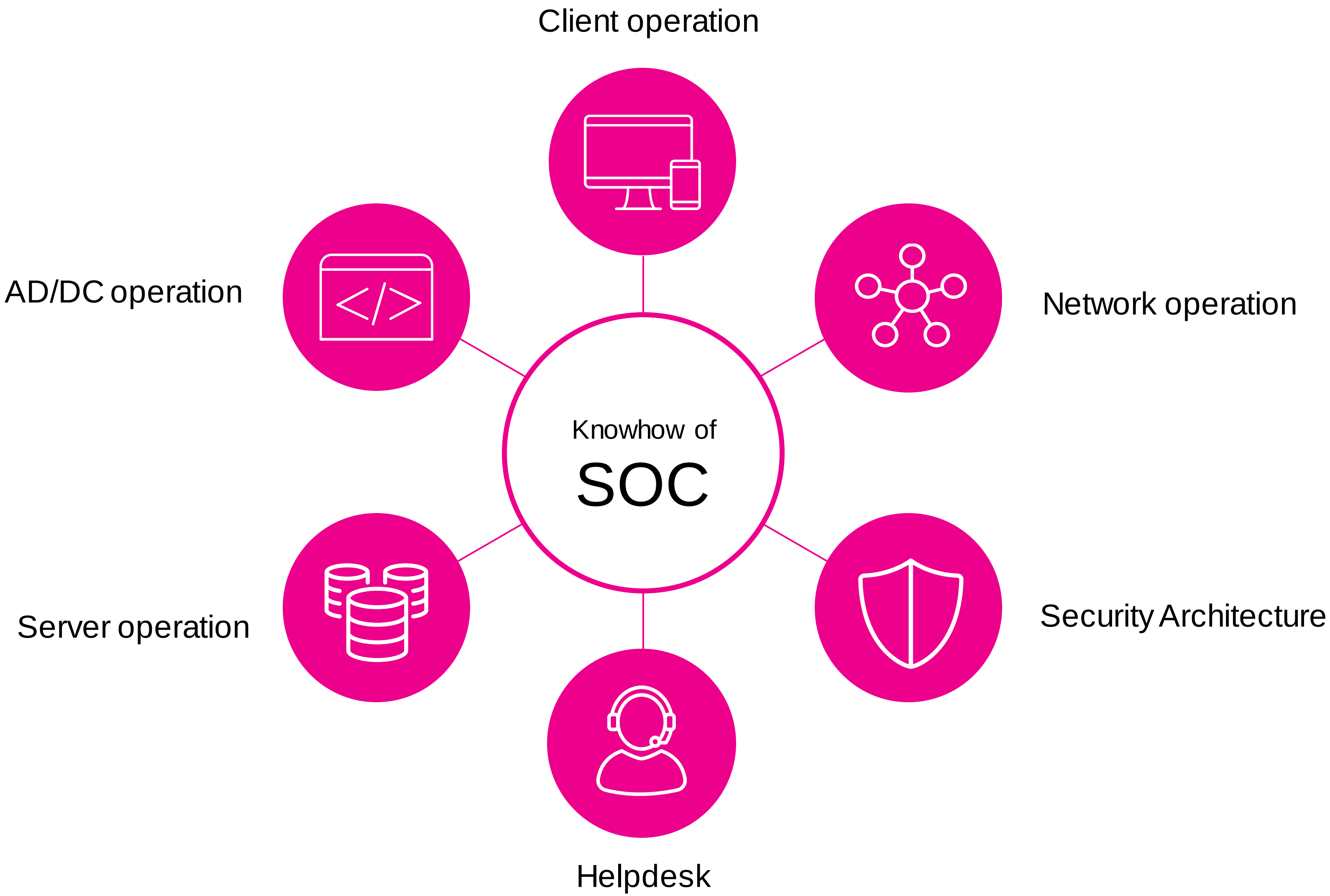
Why we need this?

What is the Challenge & Mission in a SOC?

1. What we need to be fast?
2. Who do we need?
3. Do others understand our needs?
4. The Goal is 1/10/60 Paradigm!!!

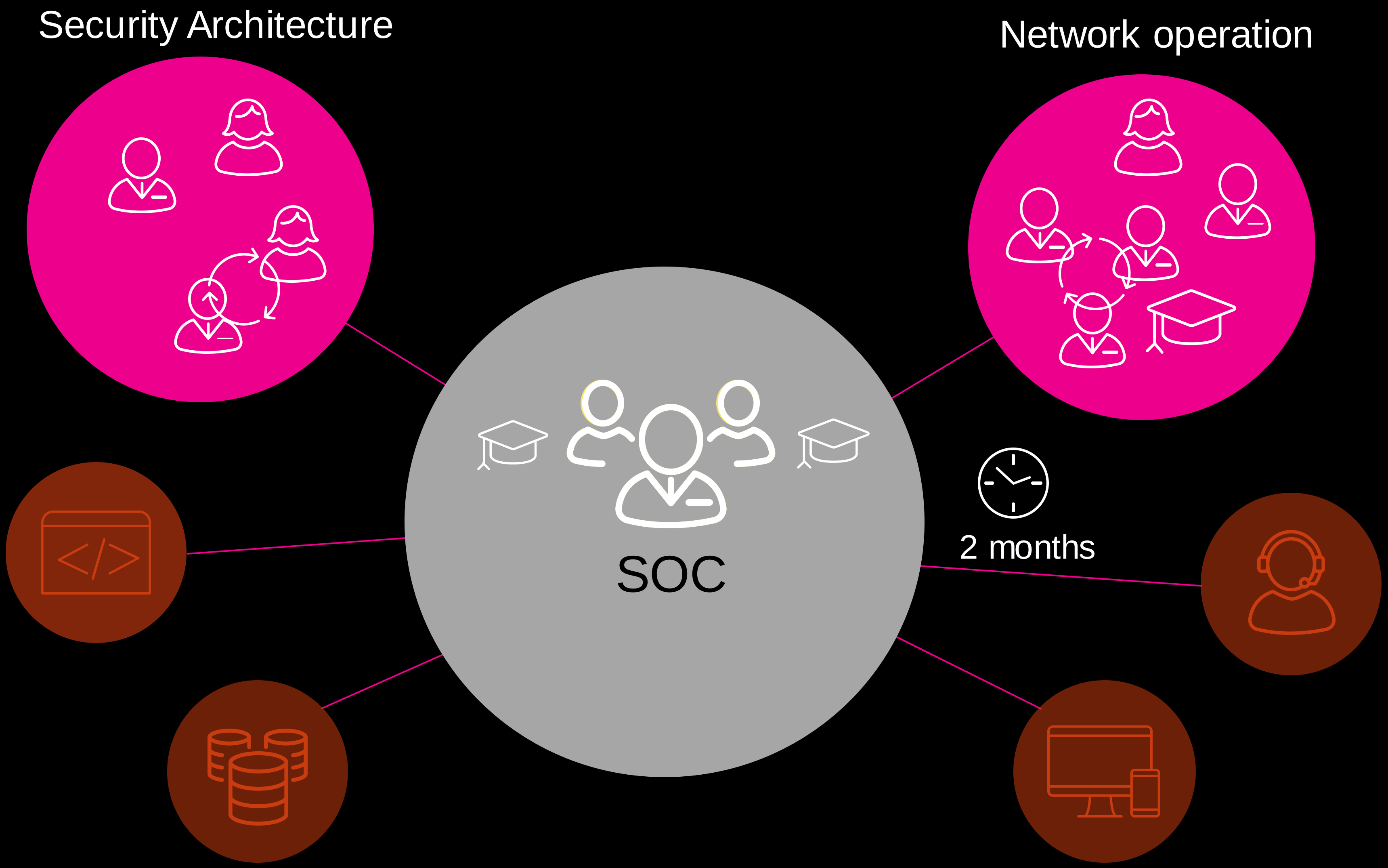
SOC Job Rotation

Core Idea



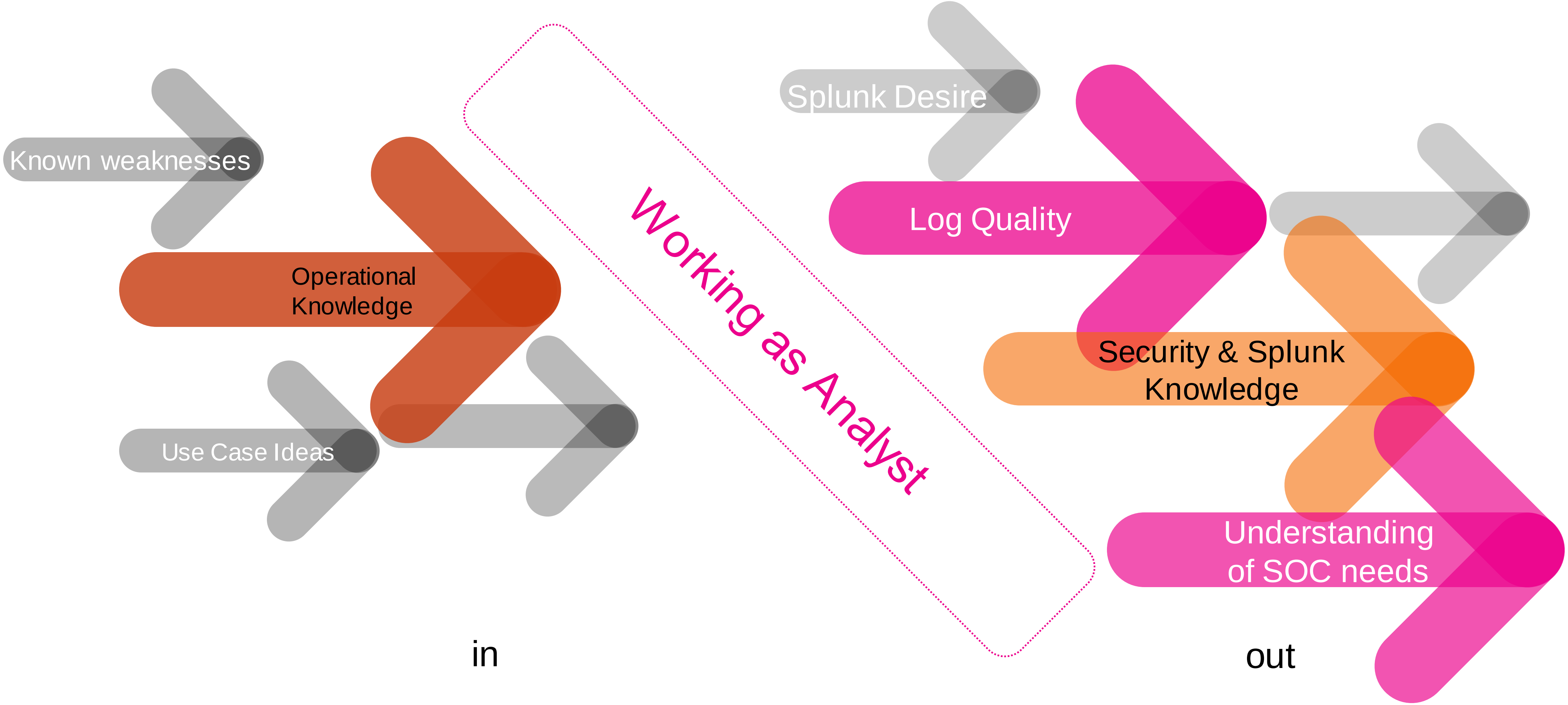
SOC Job Rotation

in practice



Outcome

what does the traveling concept do?



Known weaknesses

Operational Knowledge

Use Case Ideas

Working as Analyst

Splunk Desire

Log Quality

Security & Splunk Knowledge

Understanding of SOC needs

in

out

SOC Job Rotation

lessons learned

new traveler

workload to onboard traveler

¼ FTE

interval

optimal Time windows for traveler

2 months

skill-base

mandatory Skill-base for Traveler (Splunk Course)

Splunk Fundamentals 1+2
IR Analyst Training

trouble

most and common Challenges for Travelers

pause operational tasks (workload)
+ re-learn SOC tasks after 2 months

typical tasks

what traveler will do in daily business?

each SOC L2 tasks once
+ tasks depending on suitability

Key Takeaways

What should you take home?

Takeaways

1. MITRE ATT&CK gives you answers for:
   - What do you need in Splunk?
   - What do you want to detect?
   - What and how can your organization react on it?

2. Don’t underestimate the process definitions and required organizational changes

3. You don’t need many fancy tools particular not in the beginning

4. Use Playbooks for tasking operational units

5. Job rotation works great.

6. And always consider: You have to show results in max. 6 months. 🙁😐🙂
   - You can use MITRE ATT&CK for showing progress and needs….

Security is not Luxury,
It is a necessity.

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION