

# Mit dem MITRE ATT&CK Framework Cyberangriffe frühzeitig erkennen & abwehren

Angelo Brancato CISSP, CISM, CCSK | Security Specialist, EMEA

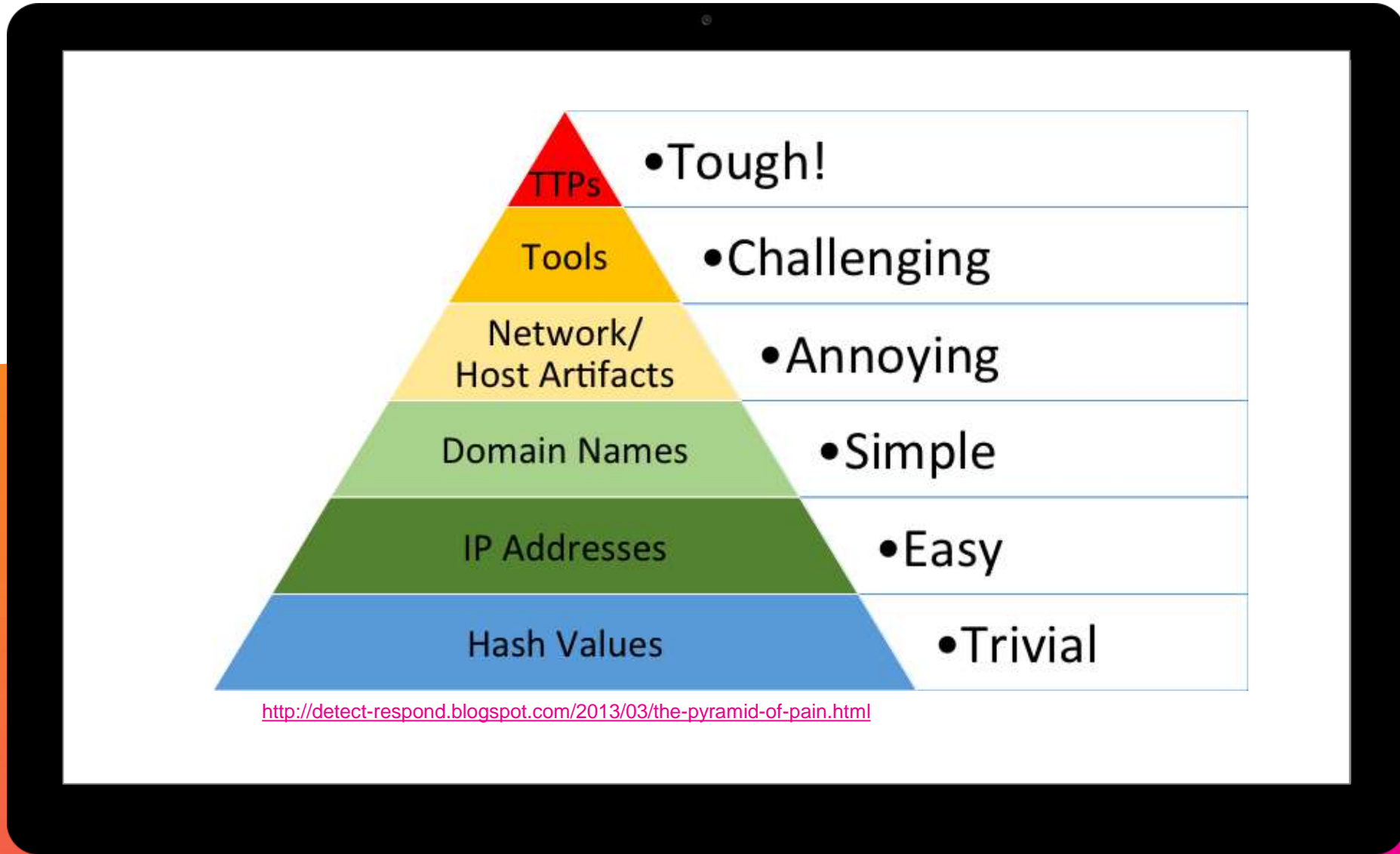
splunk > turn data into doing™

# MITRE

# ATT&CK™

Adversarial Tactics, Techniques and Common Knowledge

# The Pyramid of Pain



# MITRE ATT&CK – What is it?

- **Free, Open, Community Driven Knowledgebase**
- Describes Cyber **Adversary Behavior**
- Provides a **Common Language** (Taxonomy) for both **Offense** and **Defense**



- 3 Flavours: **PRE-ATT&CK™**, **Enterprise ATT&CK™**, **Mobile ATT&CK™**

# Tactics & Techniques

Actor: Angelo Brancato

Goal: Vortrag auf der ITsa halten



# Tactics Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternate Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shares	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service Execution	Execution through Module	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Algorithmic	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions Injection	Extra Window Memory Injection	Component Firmware Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware Hijacking	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshsta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services Hijacking	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Owner/User Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Folders	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Service Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Time Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		Virtualization/Sandbox Evasion			Uncommonly Used Port		
	Scripting	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification					Web Service		
	Scripting	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Scripting	Launch Agent	Startup Items	Gatekeeper Bypass							
	Scripting	Launch Daemon	Sudo	Group Policy Modification							
	Scripting	Launchctl	Sudo Caching	Hidden Files and Directories							
	Scripting	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Scripting	Local Job Scheduling	Web Shell	Hidden Window							
	Scripting	Logon Items		HISTCONTROL							
	Scripting	Logon Scripts		Image File Execution Options Injection							
	Scripting	LSASS Driver		Indicator Blocking							
	Scripting	Logon Existing Service		Indicator Removal from Tools							
	Scripting	Logon Helper DLL		Indicator Removal on Host							
	Scripting	Logon Process		Indirect Command Execution							
	Scripting	Logon Process		Install Root Certificate							
	Scripting	Logon Process		InstallUtil							
	Scripting	Logon Process		Launchctl							
	Scripting	Logon Process		LC_MAIN Hijacking							
	Scripting	Logon Process		Masquerading							
	Scripting	Logon Process		Modify Registry							
	Scripting	Logon Process		Mshsta							
	Scripting	Logon Process		Network Share Connection Removal							
	Scripting	Logon Process		NTFS File Attributes							
	Scripting	Logon Process		Obfuscated Files or Information							
	Scripting	Logon Process		Plist Modification							
	Scripting	Logon Process		Port Knocking							
	Scripting	Logon Process		Process Doppelgänger							
	Scripting	Logon Process		Process Hollowing							
	Scripting	Logon Process		Process Injection							
	Scripting	Logon Process		Redundant Access							
	Scripting	Logon Process		Regsvcs/Regasm							
	Scripting	Logon Process		Regsvr32							
	Scripting	Logon Process		Rootkit							
	Scripting	Logon Process		Rundll32							
	Scripting	Logon Process		Scripting							
	Scripting	Logon Process		Signed Binary Proxy Execution							
	Scripting	Logon Process		Signed Script Proxy Execution							
	Scripting	Logon Process		SIP and Trust Provider Hijacking							
	Scripting	Logon Process		Software Packing							
	Scripting	Logon Process		Space after Filename							
	Scripting	Logon Process		Template Injection							
	Scripting	Logon Process		Timestamp							
	Scripting	Logon Process		Trusted Developer Utilities							
	Scripting	Logon Process		Valid Accounts							
	Scripting	Logon Process		Virtualization/Sandbox Evasion							
	Scripting	Logon Process		Web Service							
	Scripting	Logon Process		XSL Script Processing							

Initial Access	Execution
Drive-by Compromise	AppleScript
Exploit Public-Facing Application	CMSTP
External Remote Services	Command-Line Interface
Hardware Additions	Compiled HTML File
Replication Through Removable Media	Control Panel Items
Spearphishing Attachment	Dynamic Data Exchange
Spearphishing Link	Execution through API
Spearphishing via Service Execution	Execution through Module
Supply Chain Compromise	Exploitation for Client Execution
Trusted Relationship	Graphical User Interface
Valid Accounts	InstallUtil



Tactics



Techniques



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternate Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drives	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Algorithmic	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions Hijacking	Extra Window Memory Injection	Component Firmware Hijacking	Input Capture	Peripheral Device Discovery	Replication Through Removable Media	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery		Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware Hijacking	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Depfuscate/Decode File of Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshhta	DL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking									
	Regsvcs/Regasm	External Remote Services									
	Regsvr32	File System Permissions Weakness									
	Rundll32	Hidden Files and Folders									
	Scheduled Task	Hooking									
	Scripting	Hypervisor									
	Scripting	Image File Execution Options Injection									
	Scripting	Kernel Modules and Extensions									
	Scripting	Launch Agent									
	Scripting	Launch Daemon									
	Scripting	Launchctl									
	Scripting	LC_LOAD_DYLIBS									

Initial Access	Ex
Drive-by Compromise	
Exploit Public-Facing Application	CMSTP
External Remote Services	Command
Hardware Additions	Compile
Replication Through Removable Media	Control
Spearphishing Attachment	Dynam
Spearphishing Link	Exe
Spearphishing via Service	F
Supply Chain Compromise	

MITRE ATT&CK    Matrices    Tactics    Techniques    Mitigations    Groups    Software    Resources    Blog    Contribute    Search site

Register to stream ATT&CKcon 2.0 October 29-30

Home > Techniques > Enterprise > Drive-by Compromise

## Drive-by Compromise

A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation.

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

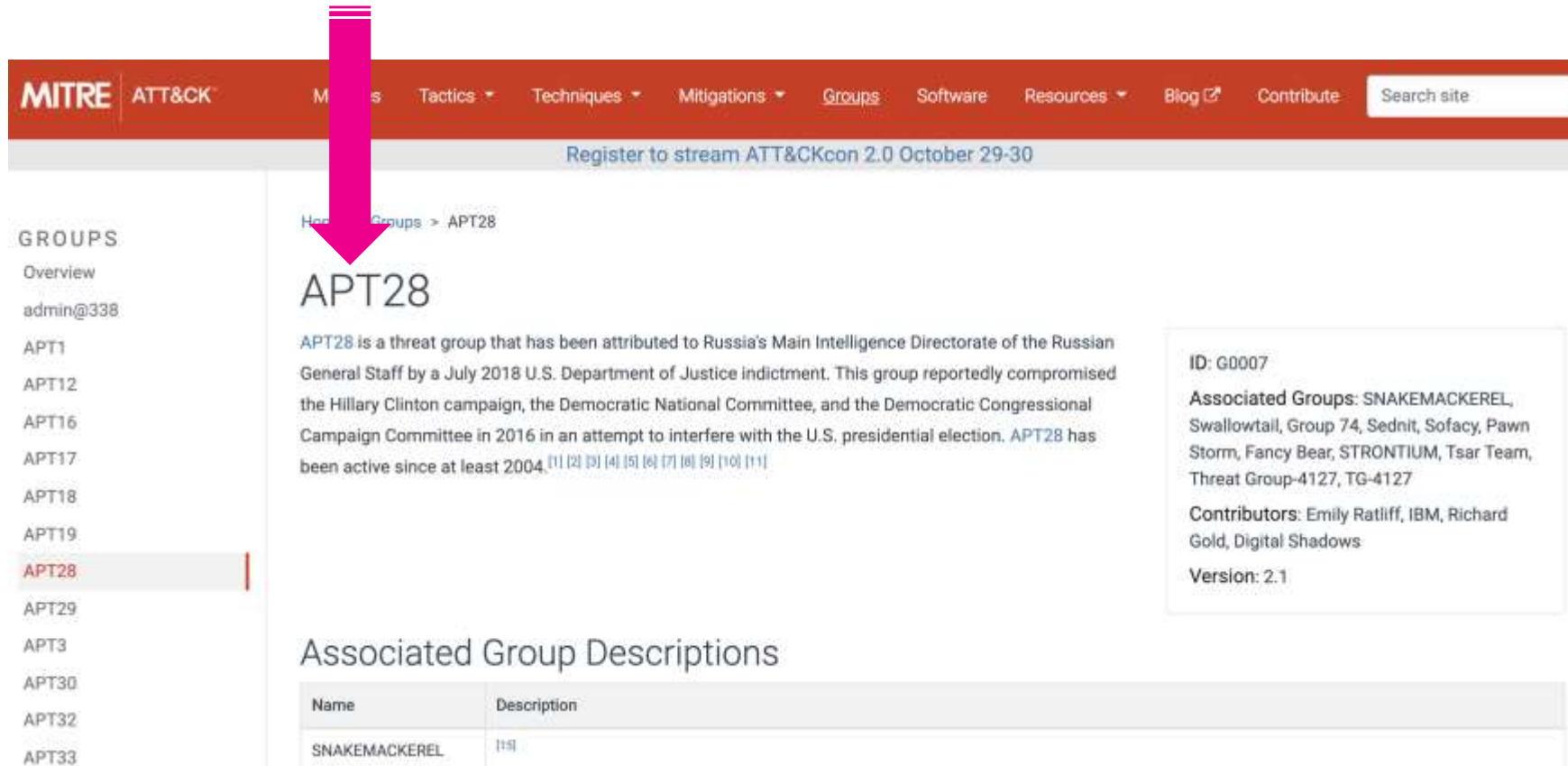
ID: T1189  
Tactic: Initial Access  
Platform: Windows, Linux, macOS  
Permissions Required: User  
Data Sources: Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection  
Version: 1.0

ENTERPRISE

Initial Access	Process Doppelgänger
Drive-by Compromise	Process Hollowing
Exploit Public-Facing Application	Process Injection
External Remote Services	Redundant Access
Hardware Additions	Regsvcs/Regasm
Replication Through Removable Media	Regsvr32
Spearphishing	Rootkit
	Rundll32
	Scripting
	Signed Binary Proxy Execution
	Signed Script Proxy Execution
	SIP and Trust Provider Hijacking
	Software Packing
	Space after Filename
	Template Injection
	Timestamp
	Trusted Developer Utilities
	Valid Accounts
	Virtualization/Sandbox Evasion
	Web Service
	XSL Script Processing

# APT28

Goal: Cyber  
Espionage,  
Data Exfiltration



MITRE ATT&CK

Groups

Tactics

Techniques

Mitigations

Groups

Software

Resources

Blog

Contribute

Search site

Register to stream ATT&CKcon 2.0 October 29-30

Home > Groups > APT28

## APT28

APT28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. APT28 has been active since at least 2004. [\[1\]](#) [\[2\]](#) [\[3\]](#) [\[4\]](#) [\[5\]](#) [\[6\]](#) [\[7\]](#) [\[8\]](#) [\[9\]](#) [\[10\]](#) [\[11\]](#)

**ID:** G0007

**Associated Groups:** SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

**Contributors:** Emily Ratliff, IBM, Richard Gold, Digital Shadows

**Version:** 2.1

### Associated Group Descriptions

Name	Description
SNAKEMACKEREL	<a href="#">[1]</a>

GROUPS

Overview

admin@338

APT1

APT12

APT16

APT17

APT18

APT19

APT28

APT29

APT3

APT30

APT32

APT33



# APT28

## Goal: Cyber Espionage, Data Exfiltration

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Later Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	AppletScript	bash_profile and .bashrc	Access Token Manipulation	Account Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Local Public WiFi	CMSTP	Accessibility Features	Binary Patching	Account Manipulation	Account Manipulation	Application Window Discovery	Application Deployment	Automated Collection	Communication Through Remote Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	Applet DLLs	BITS Jobs	Bits Jobs	Browser Backdoor	Malicious Component	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	Applet DLLs	Applet DLLs	Browser User Account Hijacking	Credential Dumping	Domain Trust Discovery	Execution of Remote Scripts	Data from Information Reservoirs	Control Panel and Control Panel	Data Transfer Size Limits	Disk Content Wipe
Interactions through Remote Media	Control Panel Items	Applet DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	OS and System Information	Date Encoding	Endpoint Denial of Service	Endpoint Denial of Service
Specializing Attachments	Dynamic Data Exchange	Application Shimming	System User Account Hijacking	Code Signing	Credentials in Registry	Network Service Discovery	Pass the Hash	Data from Network Shares	Data Obfuscation	Exfiltration Over Command and Control Channel	Exfiltration Over Other Protocol
Specializing via Service	Extension through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Execution of Remote Scripts	Network Share Discovery	Pass the Ticket	Data from Network Shares	Data Staged	Exfiltration Over Physical Medium	Exfiltration Over Physical Medium
Supply Chain Compromise	Extension through Media	BITS Jobs	Dylib Hijacking	Complete After Delivery	Forward Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Inhibit System Recovery	Inhibit System Recovery
Trusted Relationships	Installation for Client Applications	BITS Jobs	Dylib Hijacking	Compiled HTML File	Hooking	Hooking	Remote File Copy	Email Collection	Domain Fronting	Network Denial of Service	Network Denial of Service
Valid Accounts	InstallUI	Browser Extensions	Legacy Window Memory	Component Forward	Input Capture	Input Capture	Remote Services	Input Capture	Domain Fronting	Resource Hijacking	Resource Hijacking
	LaunchUI	Component Forward	Legacy Window Memory	Component Forward	Input Prompt	Input Prompt	Remote Services	Input Capture	Domain Fronting	Runtime Data Manipulation	Runtime Data Manipulation
	Local Job Scheduling	Component Forward	Legacy Window Memory	Control Panel Items	Keyboarding	Keyboarding	Shared Webroot	Screen Capture	Domain Fronting	Service Stop	Service Stop
	LSASS Driver	Create Account	Launch Daemon	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting	Stored Data Manipulation	Stored Data Manipulation
	Maha	Create Account	Launch Daemon	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting	Unintentionally Used Port	Unintentionally Used Port
	Powercat	Dylib Hijacking	Path Interception	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting	Web Service	Web Service
	Regedit/Regasm	External Remote Services	Path Interception	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting		
	Regedit32	External Remote Services	Path Interception	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting		
	Scheduled Task	Hooking	Scheduled Task	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting		
	Spawning	Hypervisor	Scheduled Task	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting		
	Service Execution	Legacy File Execution	Service Registry	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting		
	Signed Binary Proxy	Service Registry	Service Registry	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting		
	Trusted Developer Utilities	Legacy File Execution	Service Registry	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting		
	Trap	Local Job Scheduling	Web Shell	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting		
	Trusted Developer Utilities	Legacy File Execution	Service Registry	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting		
	User Execution	Logon Scripts	Logon Scripts	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting		
	Windows Management Instrumentation	LSASS Driver	LSASS Driver	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting		
	Windows Remote Management	Modify Existing Service	Modify Existing Service	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting		
	XSL Script Processing	Netcat Helper DLL	Netcat Helper DLL	DCShadow	Keychain	Keychain	Query Registry	Video Capture	Domain Fronting		

MITRE ATT&CK

MITRE ATT&CK

Groups

Tactics

Techniques

Blog

Contribute

Search site

- GROUPS
- Overview
  - admin@338
  - APT1
  - APT12
  - APT16
  - APT17
  - APT18
  - APT19
  - APT28**
  - APT29
  - APT3
  - APT30
  - APT32
  - APT33

Home Groups > APT28

## APT28

APT28 is a threat group that has been attributed to Russian intelligence Directorate 13, this group reported to be active since at least 2004. [1] [2] [3] [4] [5] [6] [7] [8] [9] [10]

APT28 is a threat group that has been attributed to Russian intelligence Directorate 13, this group reported to be active since at least 2004. [1] [2] [3] [4] [5] [6] [7] [8] [9] [10]

### Associated Group Descriptions

Name	Description
SNAKEMACKEREL	[15]

ID: G0007

Associated Groups: SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

Contributors: Emily Ratliff, IBM, Richard Gold, Digital Shadows

Version: 2.1

# APT28

## Goal: Cyber Espionage, Data Exfiltration

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	Aggrebot	bash_profile and .bashrc	Access Token Manipulation	Account Manipulation	Account Manipulation	Account Discovery	AppleBorg	Audio Capture	Community User Port	Automated Exfiltration	Data Destruction
External Remote Services	CMSTP	Accessibility Features	Accessibility Features	Binary Packing	Binary History	Application Window Hiding	Application Deployment	Automated Collection	Connection Through	Data Compression	Data Encrypted for Impact
Hardware Additions	Completed HTML File	Account Manipulation	Account Manipulation	BITS Jobs	BITS Jobs	Browser Backdoor	Clipboard Component	Clipboard Data	Connection Policy	Data Encrypted	Deployment
Hardware Additions	Completed HTML File	Applet DLLs	Applet DLLs	Browser User Account Hijacking	Browser User Account Hijacking	Clipboard Discovery	Clipboard Component	Clipboard Data	Connection Policy	Data Encrypted	Deployment
Hardware Additions	Completed HTML File	Applet DLLs	Applet DLLs	Clipboard Discovery	Clipboard Discovery	Clipboard Component	Clipboard Component	Clipboard Data	Connection Policy	Data Encrypted	Deployment
Hardware Additions	Completed HTML File	Applet DLLs	Applet DLLs	Clipboard Discovery	Clipboard Discovery	Clipboard Component	Clipboard Component	Clipboard Data	Connection Policy	Data Encrypted	Deployment
Hardware Additions	Completed HTML File	Applet DLLs	Applet DLLs	Clipboard Discovery	Clipboard Discovery	Clipboard Component	Clipboard Component	Clipboard Data	Connection Policy	Data Encrypted	Deployment
Hardware Additions	Completed HTML File	Applet DLLs	Applet DLLs	Clipboard Discovery	Clipboard Discovery	Clipboard Component	Clipboard Component	Clipboard Data	Connection Policy	Data Encrypted	Deployment
Hardware Additions	Completed HTML File	Applet DLLs	Applet DLLs	Clipboard Discovery	Clipboard Discovery	Clipboard Component	Clipboard Component	Clipboard Data	Connection Policy	Data Encrypted	Deployment
Hardware Additions	Completed HTML File	Applet DLLs	Applet DLLs	Clipboard Discovery	Clipboard Discovery	Clipboard Component	Clipboard Component	Clipboard Data	Connection Policy	Data Encrypted	Deployment

# Can we detect this?

# Is the attacker already in our network?

MITRE ATT&CK

Groups

Tactics

Techniques

Reg

- GROUPS
- Overview
  - admin@338
  - APT1
  - APT12
  - APT16
  - APT17
  - APT18
  - APT19
  - APT28
  - APT29
  - APT3
  - APT30
  - APT32
  - APT33

Home Groups > APT28

APT28

Associated Group Description

Name	Description
SNAKEMACKEREL	118

Groups: SNAKEMACKEREL, SWANOWAN, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

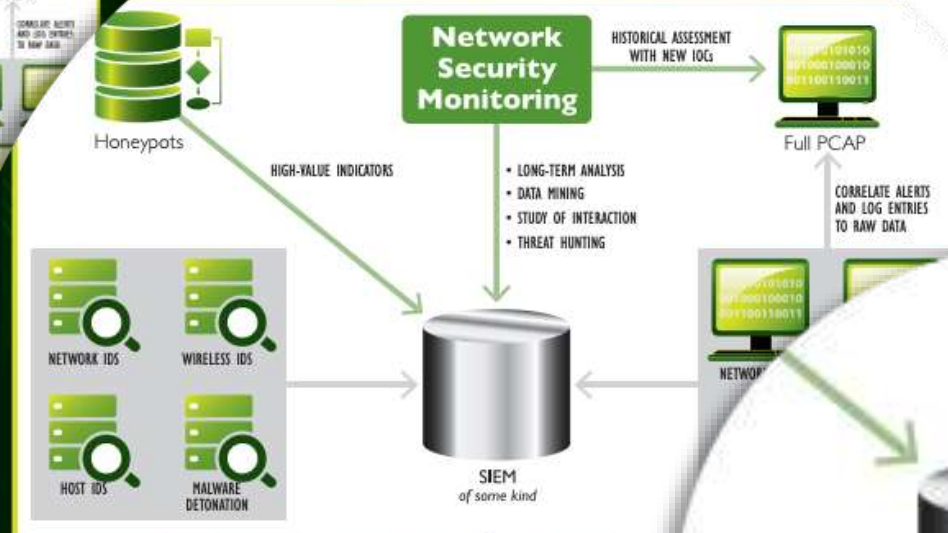
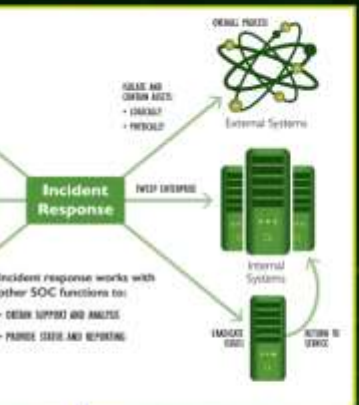
Contributors: Emily Ratliff, IBM, Richard Gold, Digital Shadows

Version: 2.1



# Security Operations Center (SOC) Essential Functions

# Center (SOC)



- ISP Onboarding Checklist**
- Hiring Practices**
    - Drug tests
    - Criminal background checks
  - Suppliers, Partners, and Resellers**
    - Access to customer data
    - Connections to network
  - Communication Tools**
    - 24/7 and follow-up capability
  - Reports**
    - Metrics and dashboards
    - Status delivery frequency
    - MITD, MITR
  - Organizational Stability**
    - Staff in business
    - Financially stable
    - ILLc and follow-up capability



<https://www.sans.org/security-resources/posters/security-leadership-poster/135/download>

# Security Operations Center (SOC) Essential Functions

**Incident Response**

Incident response works with other SOC functions for:

- Identify threats and analyze
- Monitor threat and activities

**Forensics**

Full Network, Source Forensics

**SP Onboarding Checklist**

- Wiring Practices
- Tagging
- Inventory
- Suppliers, Partners, and Resellers
- Access to customer data
- Connectivity to network
- Communication Tools

⊙

**Emotet Malware (DHS Report TA18-201A)**

Malware

Detect rarely used executables, specific registry paths that may confer malware survivability and persistence, instances where cmd.exe is used to launch script interpreters, and other indicators that the Emotet financial malware has compromised your environment.

ES Content Updates

11 Sep 2018

---

### Detection Searches

- ⊙ ESCU - Detect Rare Executables - Rule - [edit](#)
- ⊙ ESCU - Registry Keys Used For Persistence - Rule - [edit](#)
- ⊙ ESCU - Detect Use of cmd.exe to Launch Script Interpreters - Rule - [edit](#)
- ⊙ ESCU - Prohibited Software On Endpoint - Rule - [edit](#)
- ⊙ ESCU - SMB Traffic Spike - Rule - [edit](#)
- ⊙ ESCU - SMB Traffic Spike - MLTK - Rule - [edit](#)
- ⊙ ESCU - Suspicious Email Attachment Extensions - Rule - [edit](#)
- ⊙ ESCU - Email Attachments With Lots Of Spaces - Rule - [edit](#)
- ⊙ ESCU - Detection of tools built by NirSoft - Rule - [edit](#)

### Recommended Data Sources

- Carbon Black Response
- CrowdStrike Falcon
- Sysmon
- Tanium
- Ziften

See all 9 Data Sources

### Sourcetypes

No items found.

### Data Models

- Endpoint
- Network\_Traffic
- Email

### Lookups

- interesting\_processes\_lookup
- isSuspiciousFileExtension\_lookup

---

### Framework Mapping

CIS 20

CIS 2
CIS 8
CIS 3
CIS 7
CIS 12

KILL CHAIN PHASES

Installation
Command and Control
Actions on Objectives
Exploitation
Delivery

ATT&CK

Execution
Persistence
Registry Run Keys / Start Folder
Applnit DLLs
Authentication Package
Command-Line Interface
Lateral Movement
Command and Control

Commonly Used Port
Defense Evasion
Discovery
Third-party Software
Account Discovery

NIST

ID.AM
PR.PT
PR.DS
DE.CM
DE.AE
PR.IP

[https://www.splunk.com/en\\_us/blog/2019/09/11/splunk-soc-essential-functions.html](https://www.splunk.com/en_us/blog/2019/09/11/splunk-soc-essential-functions.html)







Color by

Total

MITRE ATT&CK Threat Group

APT28

Highlight Data Source

None

Show Only Available Content

Yes

Show Only Popular Techniques

Yes

We have no use case.

MITRE ATT&CK Matrix

We're good.

We have the use case but no log-data.

Initial Access	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Later Stages	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Common Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Commun
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Through
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Remov
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Media
Spearphishing	Dynamic Data	Application	Bypass User	Clear Command	Credentials in Network Service	Conne
						Proxy
						Custom
						and Co
						Proto
						Crypto
						Proto
						Data

# 10 WAYS TO TAKE MITRE ATT&CK FROM PLAN TO ACTION

A Guide to Creating a  
Threat-Informed Defense  
for Your Organization



[https://www.splunk.com/de\\_de/form/10-ways-to-take-the-mitre-att-and-ck-framework-from-plan-to-action.html](https://www.splunk.com/de_de/form/10-ways-to-take-the-mitre-att-and-ck-framework-from-plan-to-action.html)

1. Establish a Detect, Response, Prevent Strategy	Head of Security Ops
2. Respond with a short analytics turnaround	Sec. Content Developer (Blue Team)
3. Validate Coverage	SIEM Architect
4. Justify need for Data Sources	SOC Engineer
5. Document decisions based on risk evaluation	Head of Security Ops
6. Justify Investment and define roadmap	CISO
7. Risk Based Alerting Model	SOC Analysts
8. Measure Quality of Data Sources and Coverage	SIEM Admin
9. Document and Communicate Improvement Efforts	Penetration Tester (Red Team)
10. Third Party Suppliers	IT Leaders and Purchase Dep.

# Dankeschön!

Besuchen Sie uns gerne am Splunk Stand.  
Halle 10.0 / 10.0-116

**Angelo Brancato, Splunk**

**splunk** > turn data into doing™