kapsch
challenging limits

Kapsch BusinessCom

Effiziente Abwehr von Cyber Kriminalität

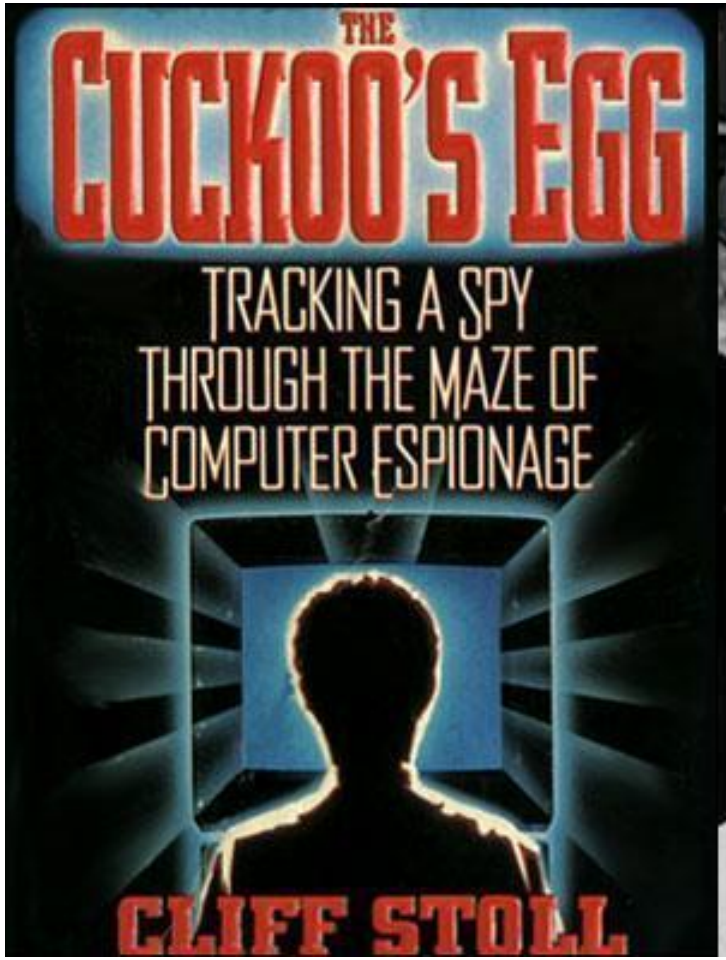
Timo Jobst
Head of Cyber Defense Center

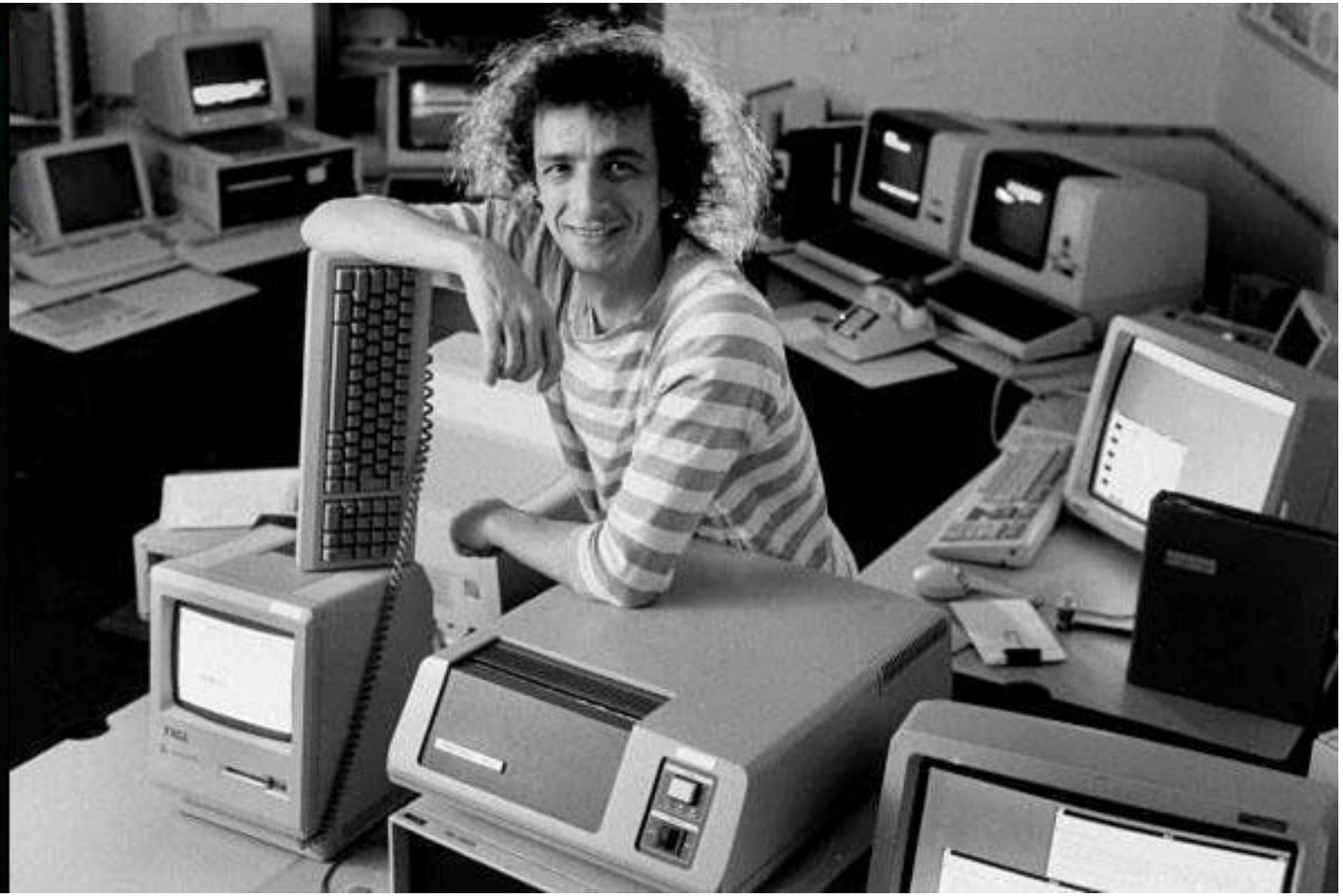
C:\whoami

- **Timo Jobst**
- Cyber Defense, Incident Response, Threat Intel
- CISSP, GCFA, GCTI, CCE,…
- >15 Jahre in Cyber Security
- Sport & Outdoor Fan

Was haben Sie 1986 gemacht?

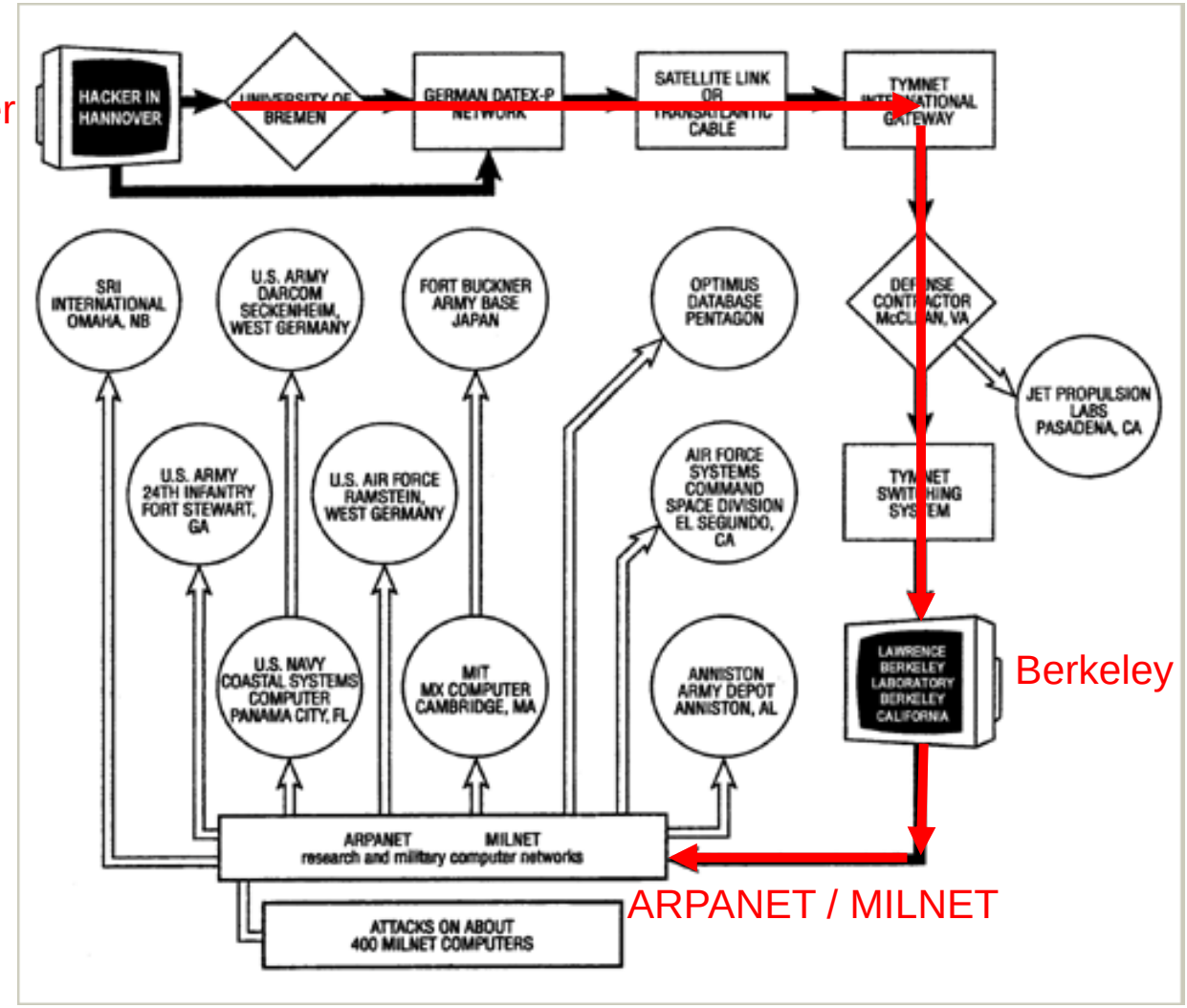
Cliff Stoll - 1986





A Long Story Short

Hacker Hannover

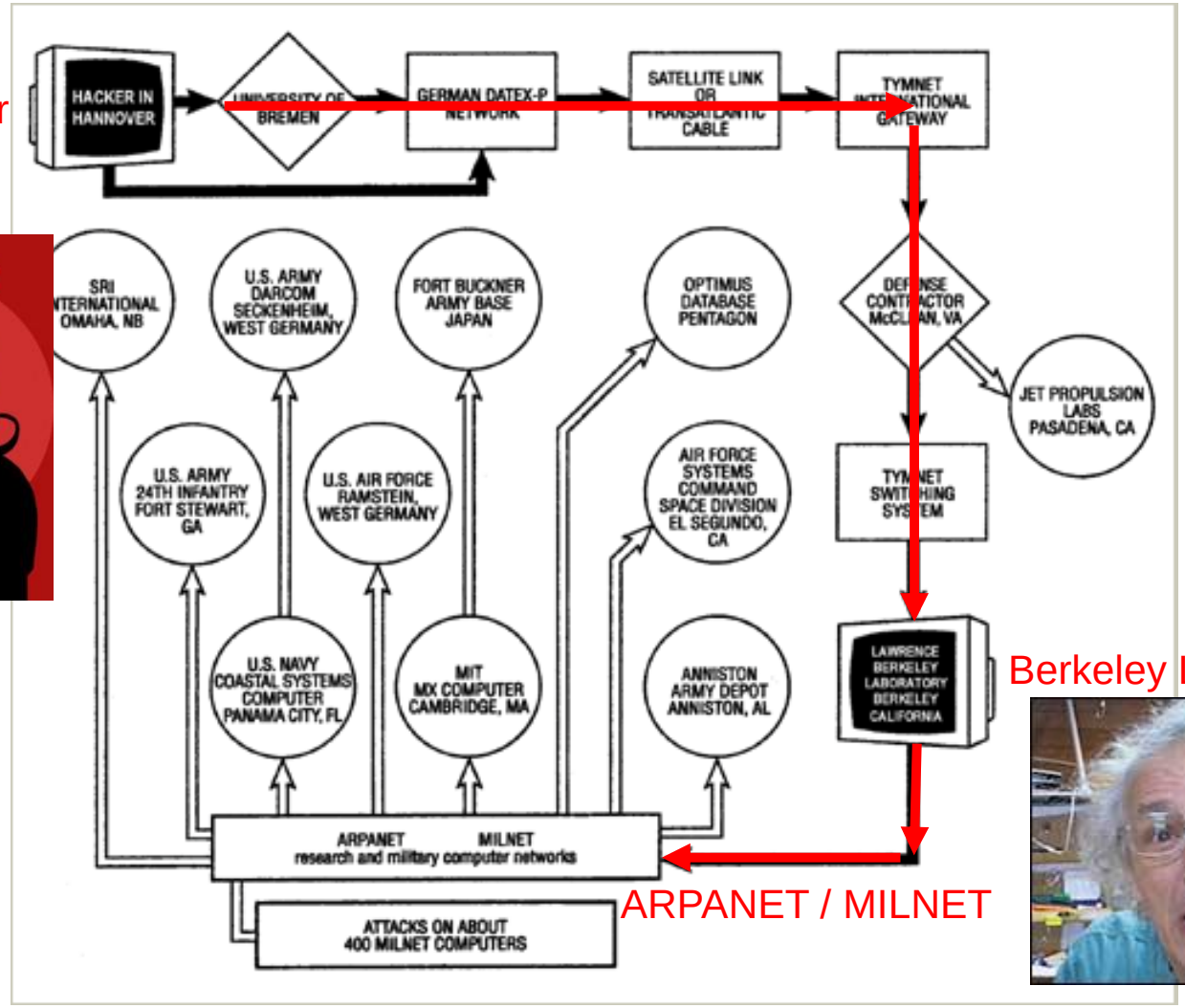


Berkeley Laboratory

ARPANET / MILNET

A Long Story Short

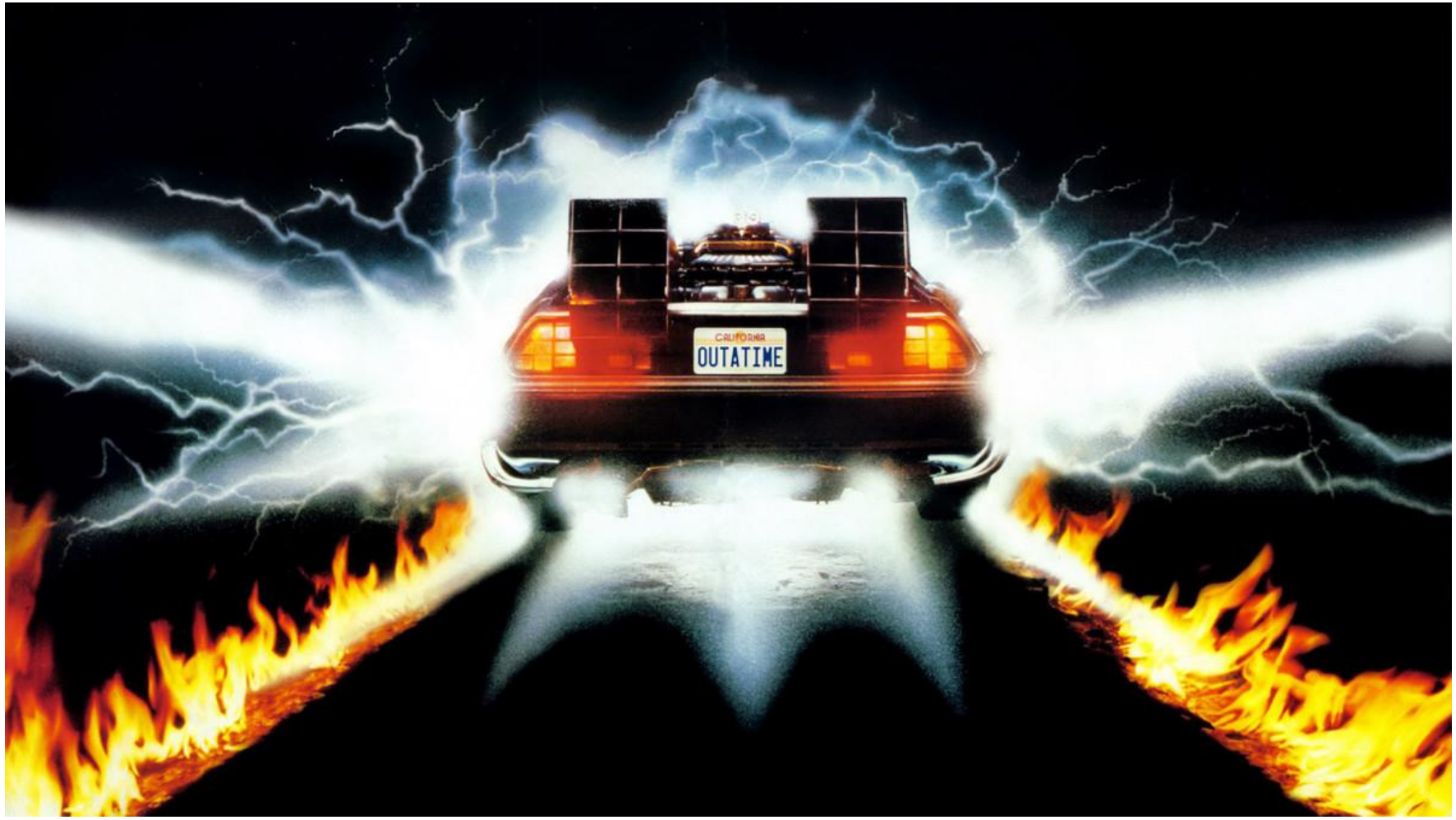
Hacker Hannover



ARPANET / MILNET

Berkeley Laborato

Back to todays Cyber Defense



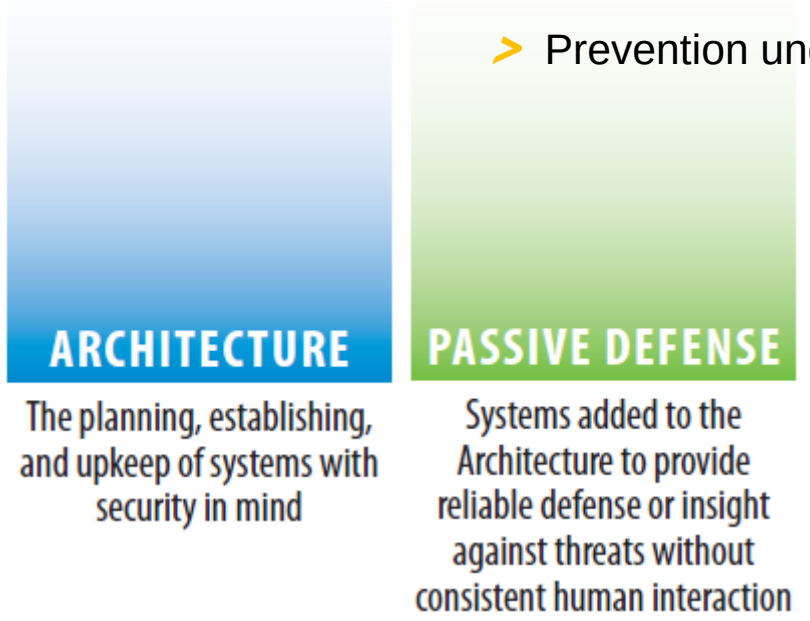
Sliding Scale of Cyber Security

- Grundbausteine
  - Planung
  - Entwicklung
  - Design
- Stellt die Basis für alles weitere her
- Solange die Basis nicht stimmt, ist ein teures Invest von Security sinnlos
- Falsch konfigurierte Hard- u. Software erzeugt viel Noise im Netzwerk
- Gewartete und gepatchte Systeme bieten dem Angreifer weniger Angriffsfläche

Quelle: https://www.sans.org/reading-room/whitepapers/ActiveDefense/paper/36240

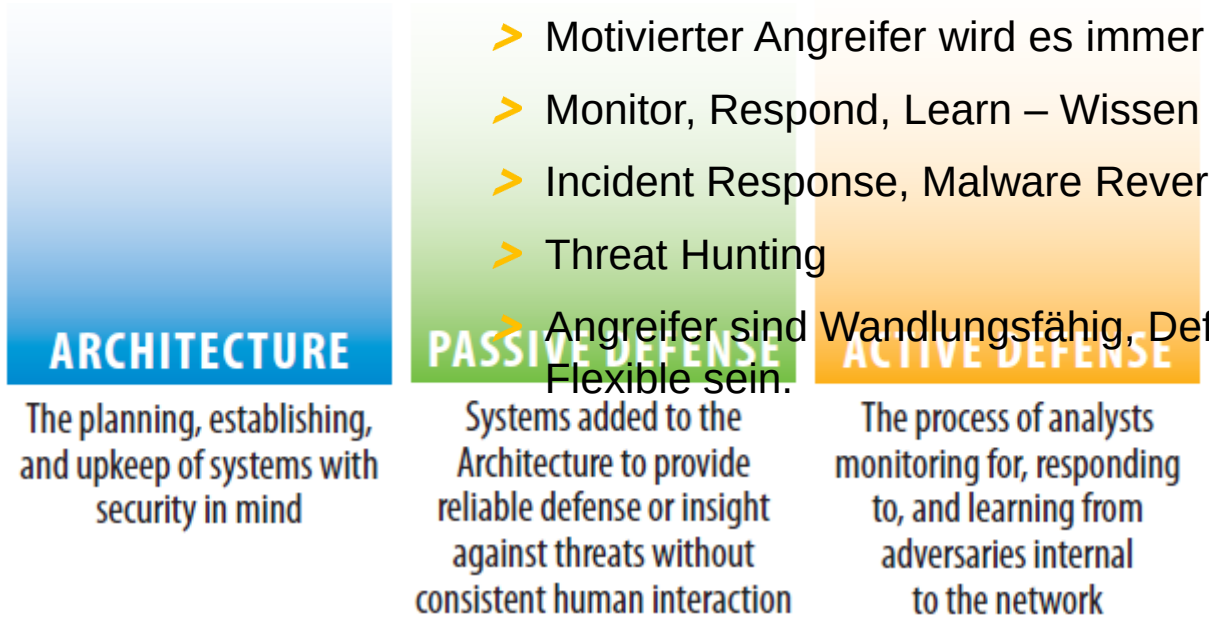
Sliding Scale of Cyber Security

- Typische Security Landschaft
  - Firwalls, Anti-Malware Systeme, IPS, AV,…
- Diese benötigen Wartung aber keine kontinuierliche menschliche Betreuung
- Prevention und Protection können meist leicht umgangen werden



Quelle: https://www.sans.org/reading-room/whitepapers/ActiveDefense/paper/36240

Sliding Scale of Cyber Security



- Gut geschulte Analysten benötigt um ebenfalls gut geschulte Angreifer zu identifizieren
- Gute Architektur und Passive Defense ist Grundvoraussetzung
- Motivierter Angreifer wird es immer schaffen ein Netz zu kompromittieren
- Monitor, Respond, Learn – Wissen auf die internen Netzwerke übertragen
- Incident Response, Malware Reverse Engineering, Threat Analyse, NSM,….
- Threat Hunting
- Angreifer sind Wandlungsfähig, Defender müssen ebenso Intelligent und Flexible sein.

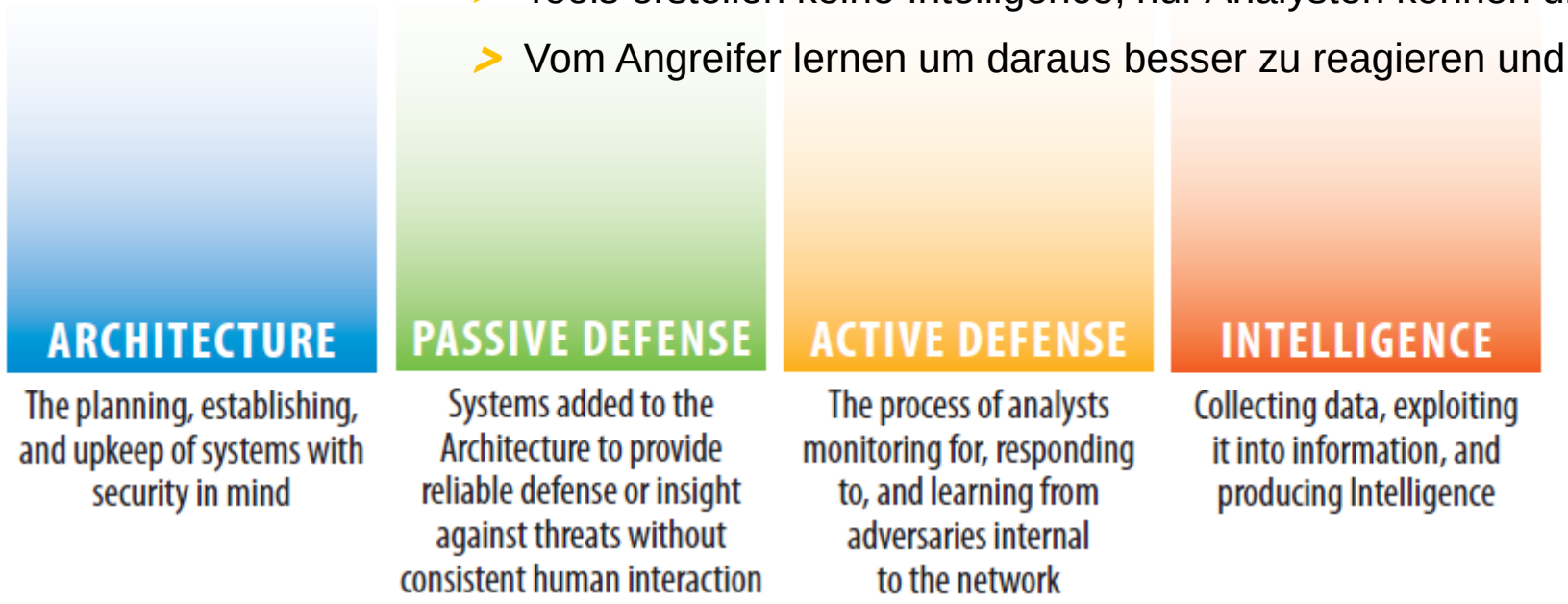
Quelle: https://www.sans.org/reading-room/whitepapers/ActiveDefense/paper/36240

Pew-Pew Maps


GREENLAND
CANADA
UNITED STATES
MEXICO
VUL - Vulnerability Scan

Sliding Scale of Cyber Security

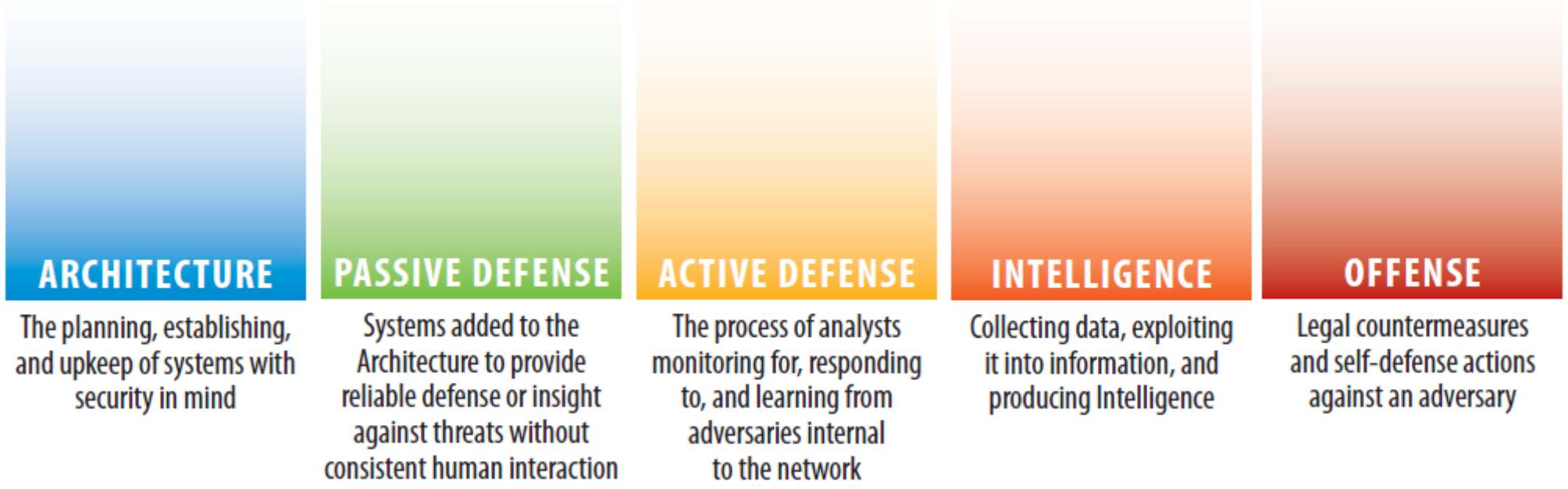
- Intelligence wird für effektive Active Defense benötigt
- Analysierte und bewertete Information führt zu Intelligence
- Tools erstellen keine Intelligence, nur Analysten können dies
- Vom Angreifer lernen um daraus besser zu reagieren und zu identifizieren



Quelle: https://www.sans.org/reading-room/whitepapers/ActiveDefense/paper/36240

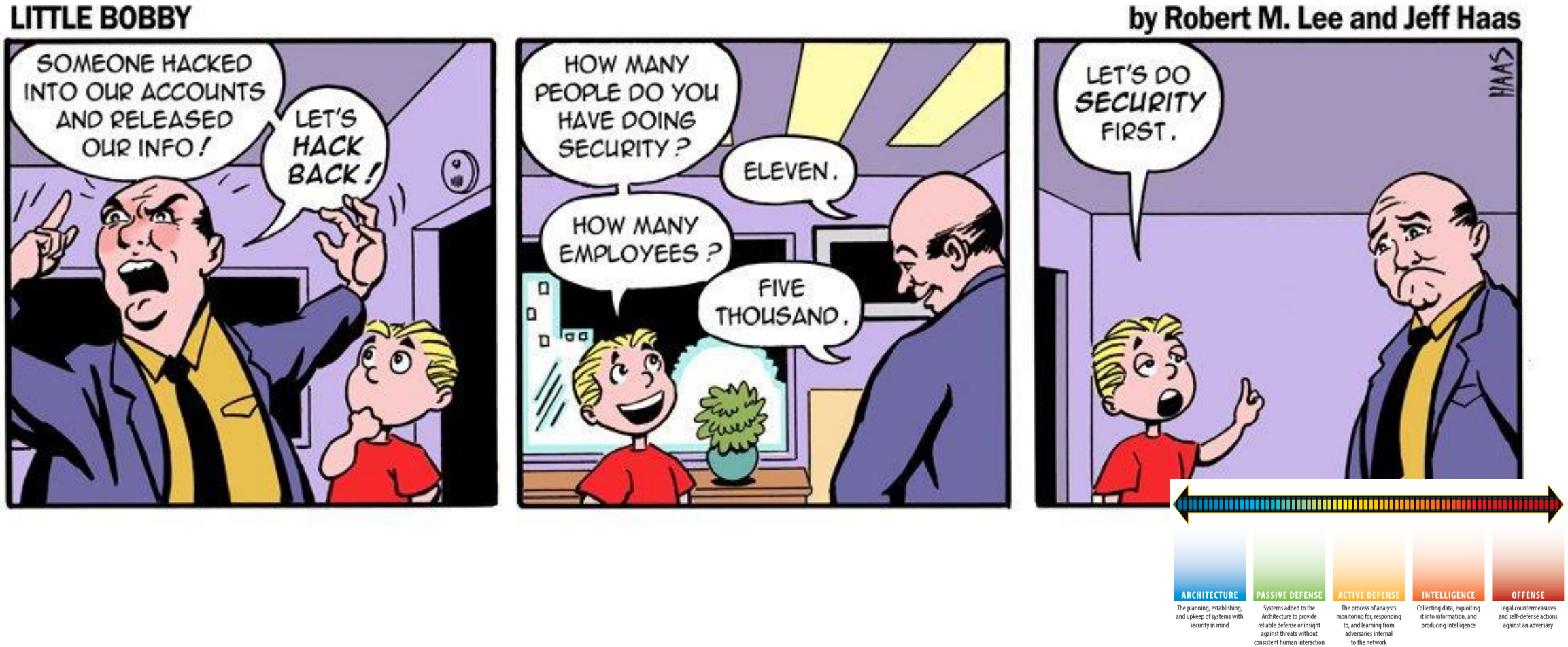
Sliding Scale of Cyber Security

- Wird eher von Militär und großen Security Unternehmen durchgeführt
- Kostenintensiv



Quelle: https://www.sans.org/reading-room/whitepapers/ActiveDefense/paper/36240

Sliding Scale of Cyber Security



Sliding Scale of Cyber Security

ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

INTELLIGENCE

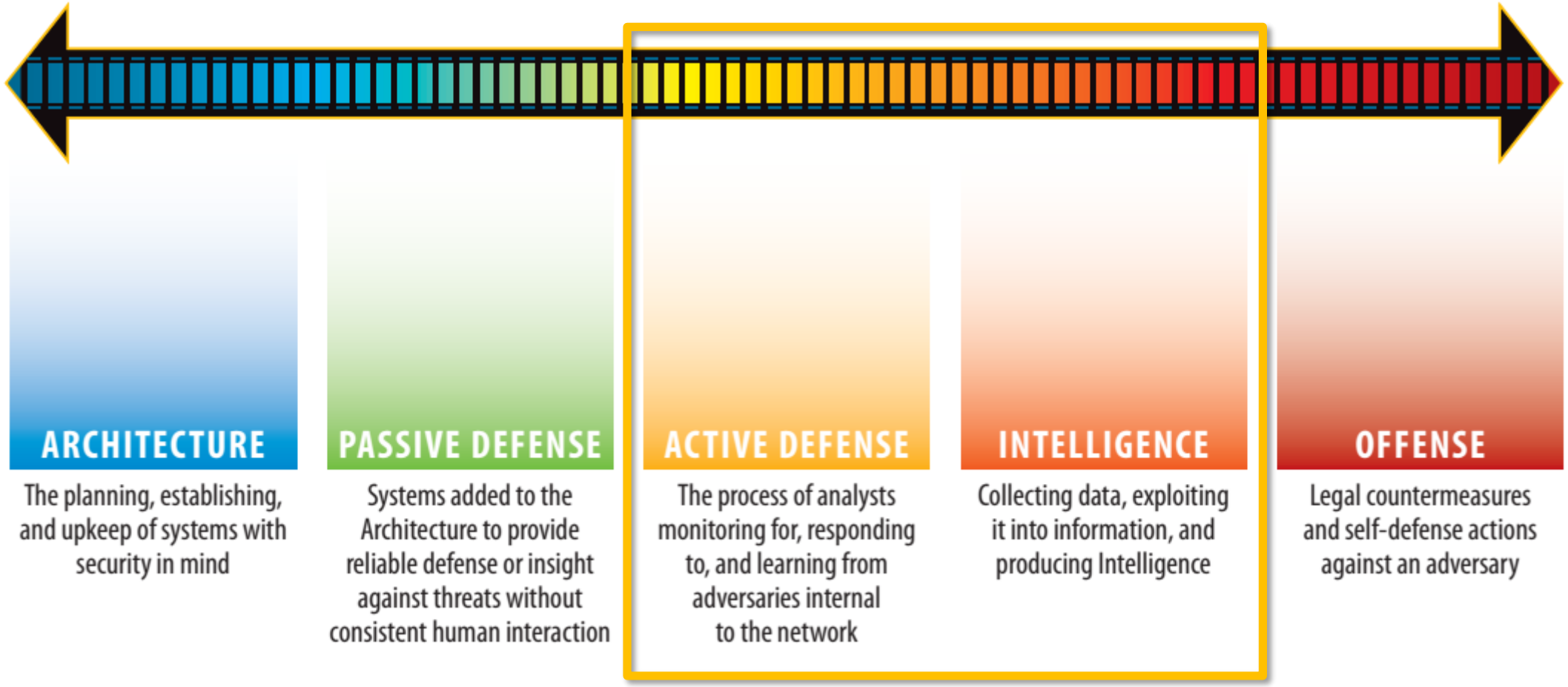
Collecting data, exploiting it into information, and producing Intelligence

OFFENSE

Legal countermeasures and self-defense actions against an adversary

Quelle: https://www.sans.org/reading-room/whitepapers/ActiveDefense/paper/36240

Sliding Scale of Cyber Security



Quelle: https://www.sans.org/reading-room/whitepapers/ActiveDefense/paper/36240

Active Defense & Intelligence

Großer Technologie Stack

Viel Open Source und einige kommerzielle Produkte

Hardware

Woher kommt die Intel?

OSINT/Kommerziell?

Wo verarbeite ich die Daten?

Wie produziere ich Intel?

Erfahrung im Security Bereich

Analytisches Denken

Netzwerk & OS Knowhow

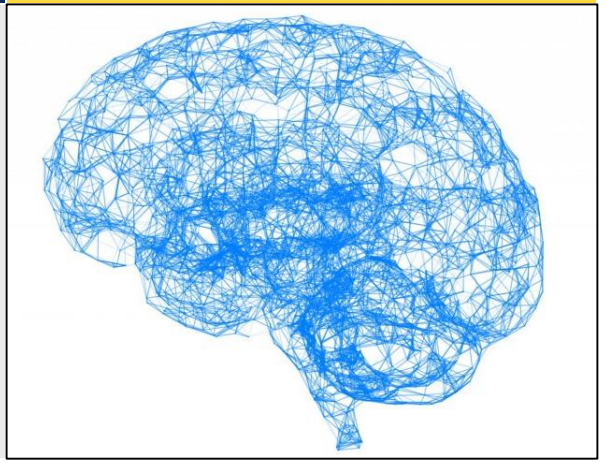
IR & Forensic Knowhow

Welche Daten braucht man?

Schwachstellen

Wie kommt man an diese Daten?

Wo speichert man sie?



Beurteilung Data Sources

Host/Network	Proactive/Live
Pivots	
Pro	
Con	

Criteria	Grade
Retention	
Context	
Search	
Acquisition	
Pivot Fields	
GRADE	

Packet Capture (PCAP)

Network	Proactive
IP, Port, Protocol Fields, Payload	
Pro	
• Highest contex network data source • Wide level of tool support • Likely already examined by IDS	
Con	
• Large disk footprint limits retention • Limited value when encryption is used • Significant extraneous data • Slow to retrieve and filter	

Criteria	Grade
Retention	D
Context	A+
Search	C
Acquisition	D
Pivot Fields	A+
GRADE	**B-**

Network Flow Data

Network	Proactive
IP, Port	
Pro	
• Possible to store for a long time • Very fast and flexible to search • Can be generated from network devices or sensors • Ideal starting point	
Con	
• Virtually no context • Several formats can produce different results	

Criteria	Grade
Retention	A+
Context	D
Search	A+
Acquisition	A
Pivot Fields	D
GRADE	**A-**

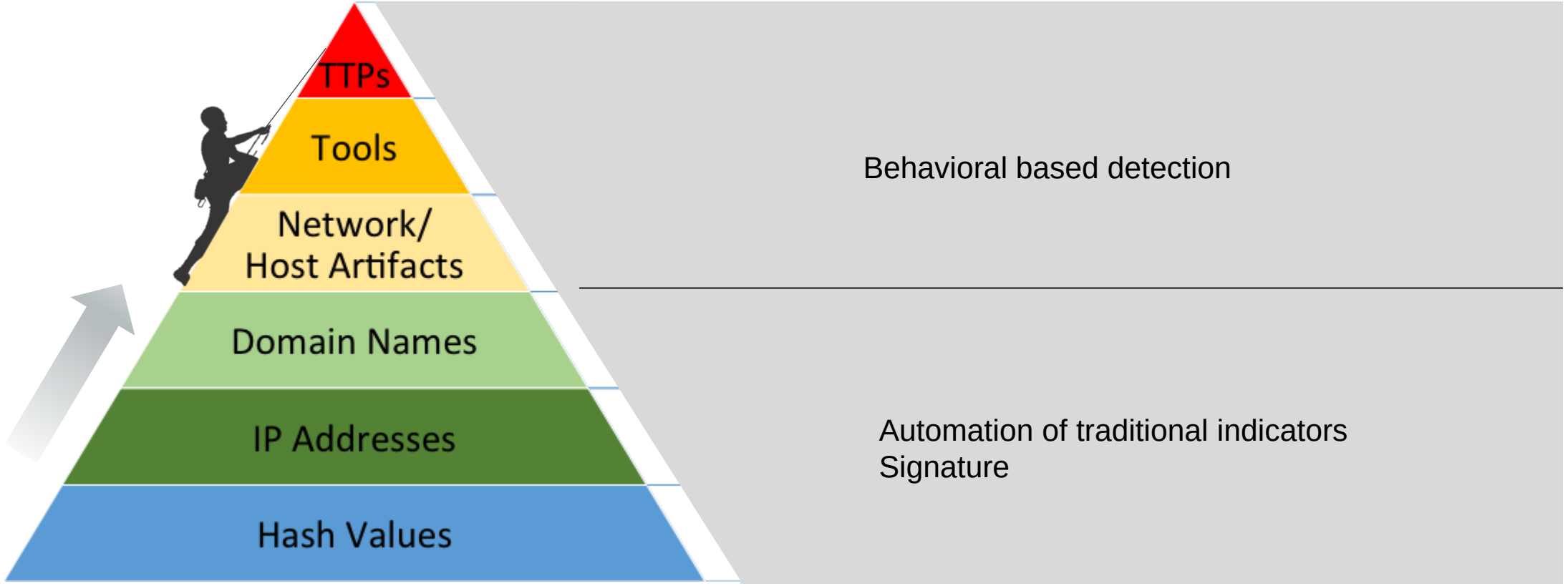
Memory Image

Host	Live
Too Many to Name	
Pro	
• Incredibly context rich • Often the only way to find certain types of malware or hidden processes • Individual dumps are easy to navigate with some tools	
Con	
• Time consuming to acquire and parse • Not feasible for proactive collection or long retention	

Criteria	Grade
Retention	F
Context	A
Search	B
Acquisition	D
Pivot Fields	A+
GRADE	**B**

Detections

Pyramid of Pain

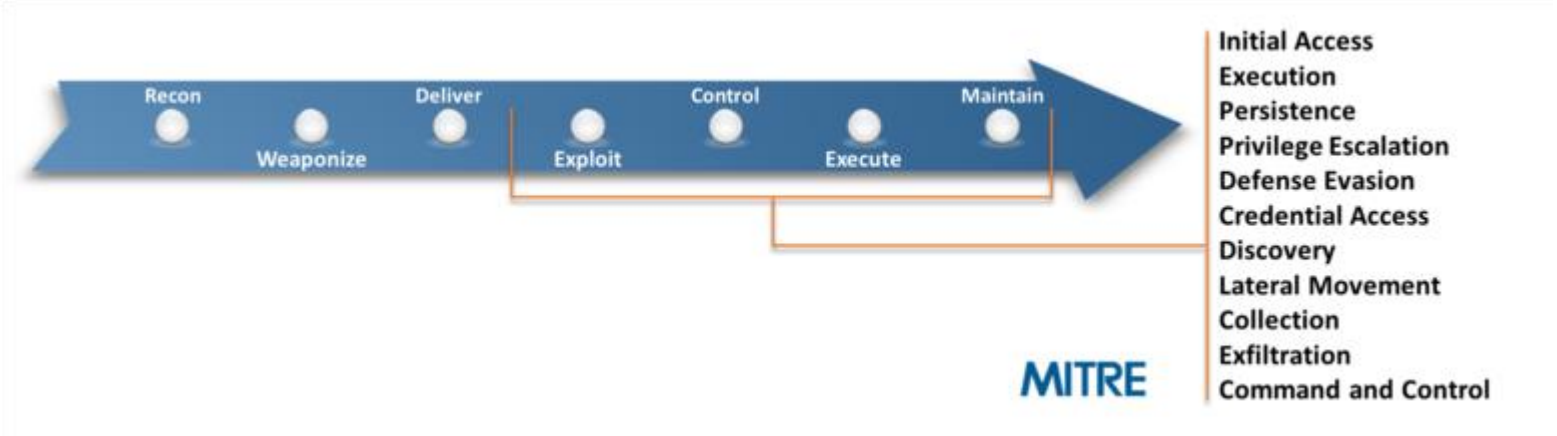


Source: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

MITRE ATT&CK

MITRE´s Adversarial Tactics, Techniques, and Common Knowledge

- An adversary model and framework for describing the actions an adversary may take to compromise and operate within an enterprise network
- Focus on the last for steps of the Cyber Attack Lifecycle



MITRE ATT&CK

- **11 Tactics**
- Derived from
control, maint
seven-stage
- Categories c
techniques a
perform that

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collecti
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Cap
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automat Collecti
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard
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	Data Sta
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data fro Informat Reposito
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Syster
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data fro Network S Drive
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data fro Removal Media
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Colle

MITRE ATT&CK

- **11 Tactics**
- Derived from later stages (expoit, control, maintain and execute) of a seven-stage Attack Lifecycle
- Categories contain list of techniques adversary could use to perform that tactic
- **~223 Techniques**
- Windows, Mac, Linux
- Techniques provide technical, description, indicators, useful defensive sensor data, detection analytics, and potentioal mitigations

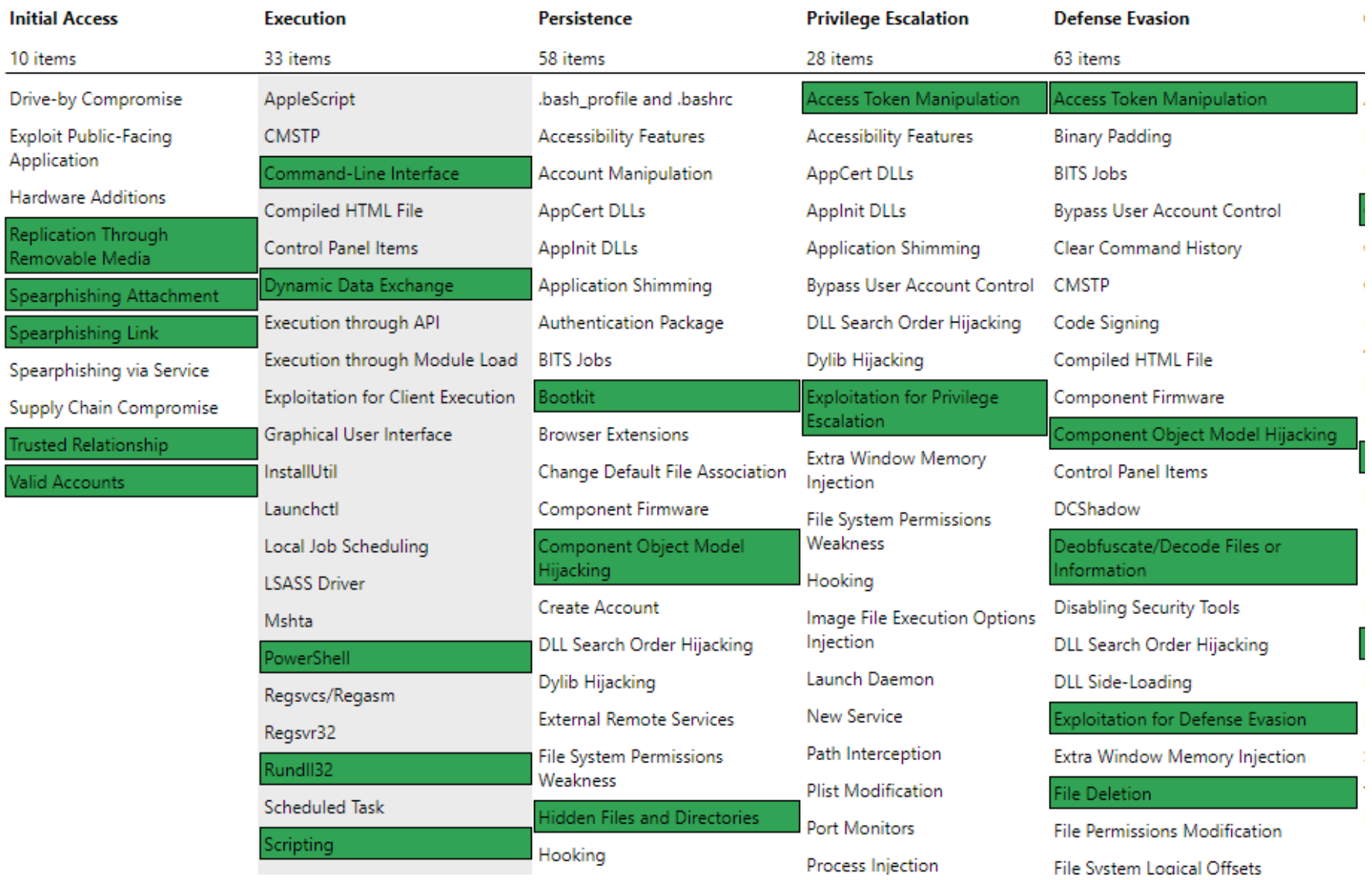
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collecti
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Cap
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automa Collecti
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard
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	Data Sta
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data fro Informat Reposito
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Syster
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data fro Network S Drive
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data fro Removal Media
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Colle

APT28, Sofacy, Fancy Bear

kapsch >>> challenging limits

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
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	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-hop Proxy
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture		Multiband Communication
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	Scheduled Task	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Scripting	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets						Web Service
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories						
	Signed Script Proxy Execution	Launch Agent	Startup Items	Hidden Users						
	Source	Launch Daemon	Sudo	Hidden Window						
	Space after Filename	Launchctl	Sudo Caching	HISTCONTROL						
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Image File Execution Options Injection						
	Trap	Local Job Scheduling	Web Shell	Indicator Blocking						
	Trusted Developer Utilities	Login Item		Indicator Removal from Tools						
	User Execution	Logon Scripts		Indicator Removal on Host						
	Windows Management Instrumentation	Windows Remote Management		Indirect Command Execution						

APT28, Sofacy, Fancy Bear



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 items	33 items	58 items	28 items	63 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items
	Launchctl	Component Firmware	Hooking	DCShadow
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion
	Scheduled Task	Hooking		File Permissions Modification
	Scripting			File System Logical Offsets

APT29, Cozy Bear

kapsch >>> challenging limits

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
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	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-hop Proxy
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture		Multiband Communication
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	Scheduled Task	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Scripting	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets						Web Service
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories						
	Signed Script Proxy Execution	Launch Agent	Startup Items	Hidden Users						
	Source	Launch Daemon	Sudo	Hidden Window						
	Space after Filename	Launchctl	Sudo Caching	HISTCONTROL						
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Image File Execution Options Injection						
	Trap	Local Job Scheduling	Web Shell	Indicator Blocking						
	Trusted Developer Utilities	Login Item		Indicator Removal from Tools						
	User Execution	Logon Scripts		Indicator Removal on Host						
	Windows Management Instrumentation									

APT29, Cozy Bear

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 items	33 items	58 items	28 items	63 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items
	Launchctl	Component Firmware	Hooking	DCShadow
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection
	Rundll32	Hidden Files and Directories		File Deletion
	Scheduled Task	Hooking		File Permissions Modification
	Scripting			

Kombination APT28/APT29

kapsch >>> challenging limits

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
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	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-hop Proxy
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture		Multiband Communication
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	Scheduled Task	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Scripting	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets						Web Service
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories						
	Signed Script Proxy Execution	Launch Agent	Startup Items	Hidden Users						
	Source	Launch Daemon	Sudo	Hidden Window						
	Space after Filename	Launchctl	Sudo Caching	HISTCONTROL						
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Image File Execution Options Injection						
	Trap	Local Job Scheduling	Web Shell	Indicator Blocking						
	Trusted Developer Utilities	Login Item		Indicator Removal from Tools						
	User Execution	Logon Scripts		Indicator Removal on Host						
	Windows Management Instrumentation			Indirect Command Execution						

Kombination APT28/APT29

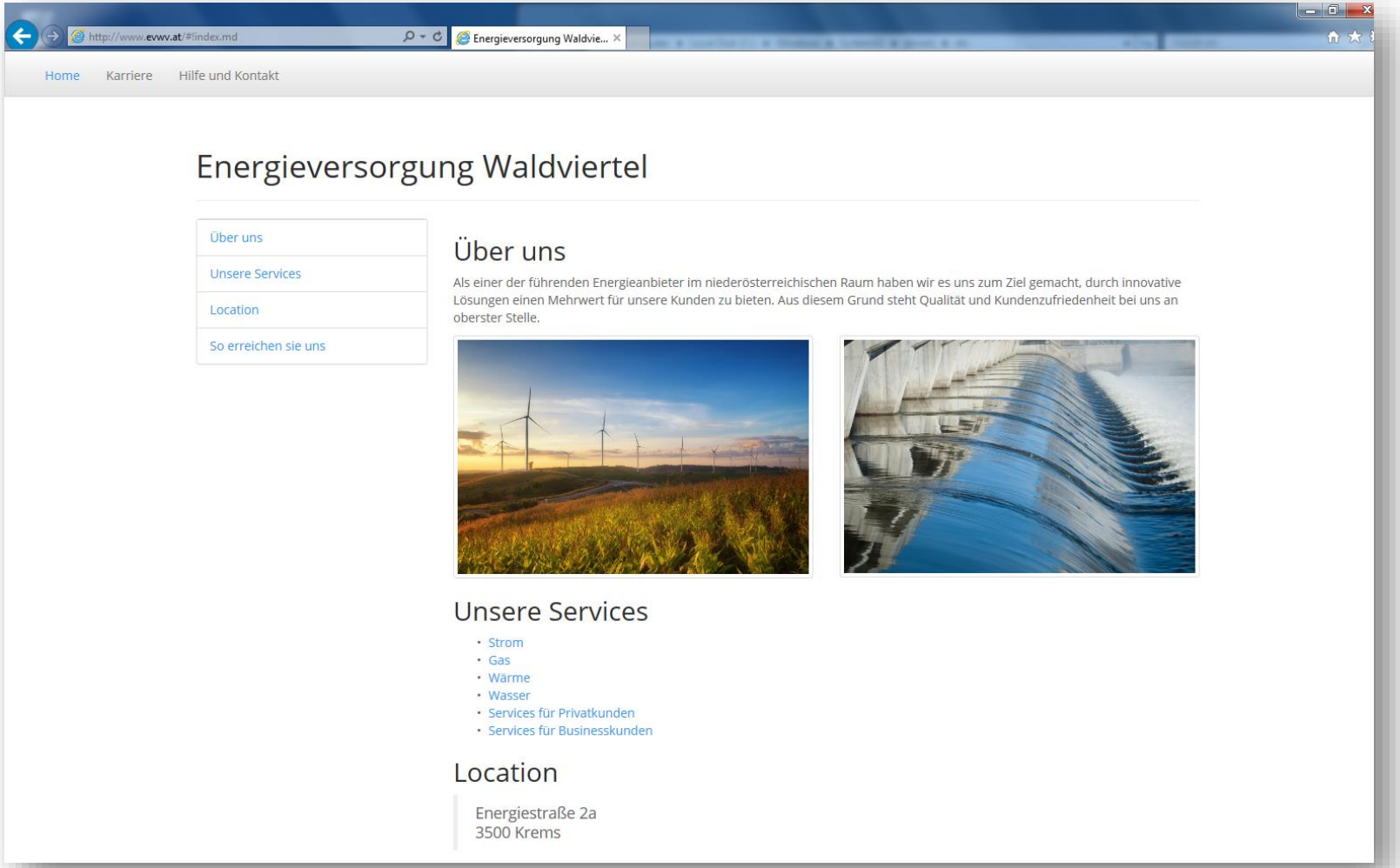
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 items	33 items	58 items	28 items	63 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items
	Launchctl	Component Firmware	Hooking	DCShadow
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection
	Rundll32	Hidden Files and Directories		File Deletion
	Scheduled Task	Hooking		File Permissions Modification
	Scripting			

Die Bedrohung

Gezielte Angriffe

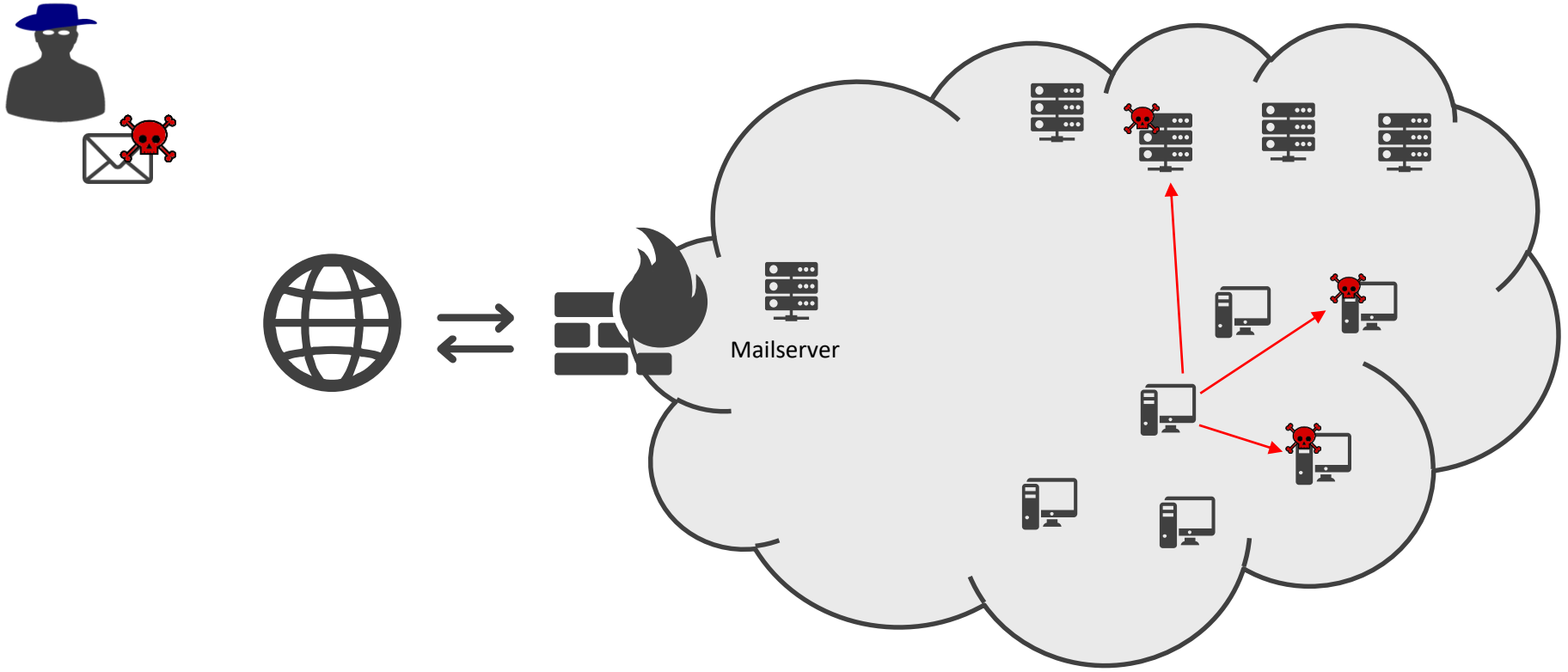
Das Ziel: Energieversorgung Waldviertel

Operation Powerhouse



Der Plan: Netzwerkzugriff

Operation Powerhouse

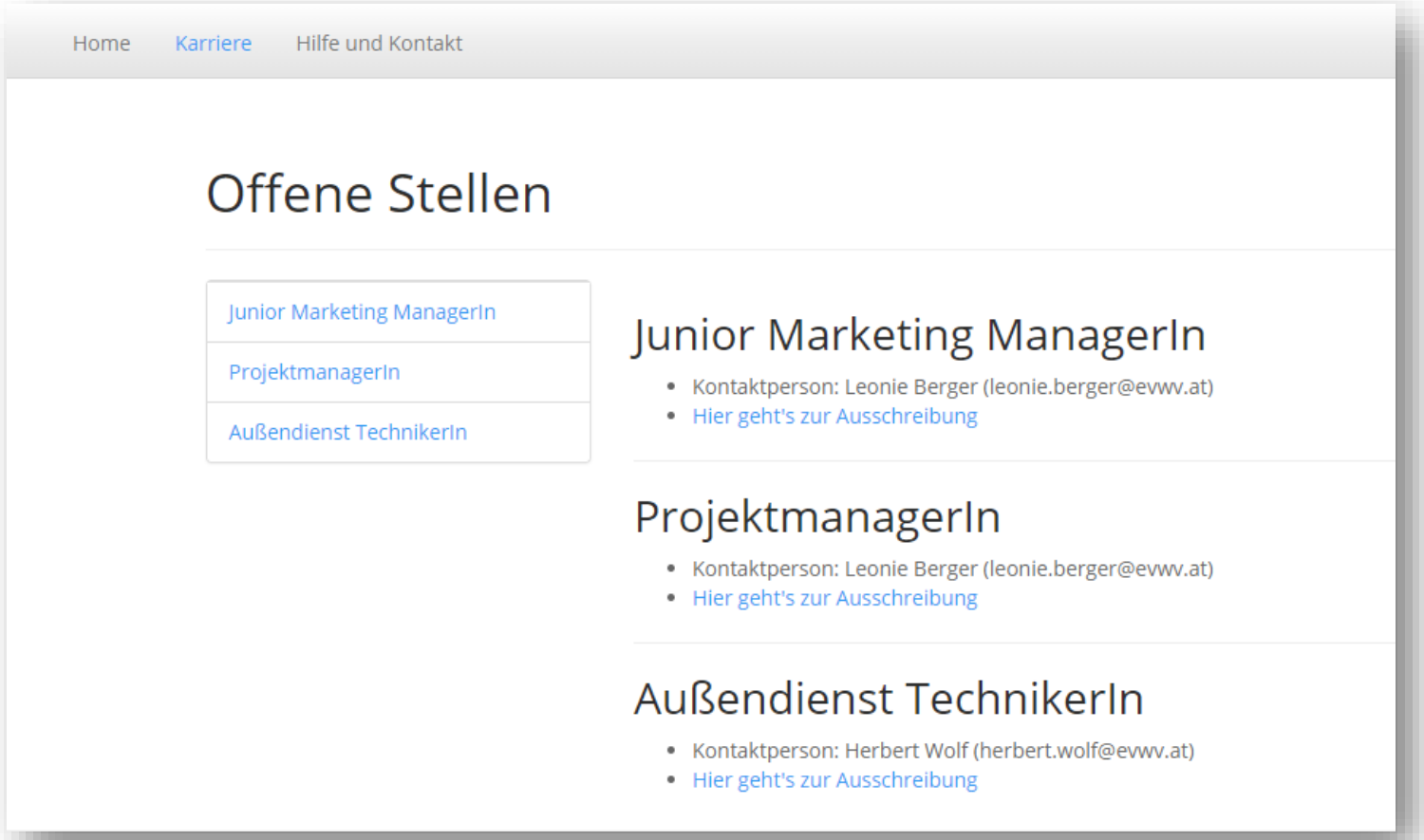


kapsch
challenging limits

Versuch #1

Versuch #1

Operation Powerhouse



Versuch #1

Operation Powerhouse

Junior Marketing ManagerIn

Dienstort: Krems

Die EVWV zählt zu den erfolgreichsten Energieversorgungsunternehmen im Osten Österreichs mit internationaler Bedeutung im Zukunftsmarkt der Smart Energy. Seit 2003 steht das Unternehmen für die konsequente Entwicklung und Implementierung richtungsweisender Technologien. Wir bieten unseren Kunden stets maßgeschneiderte Lösungen.

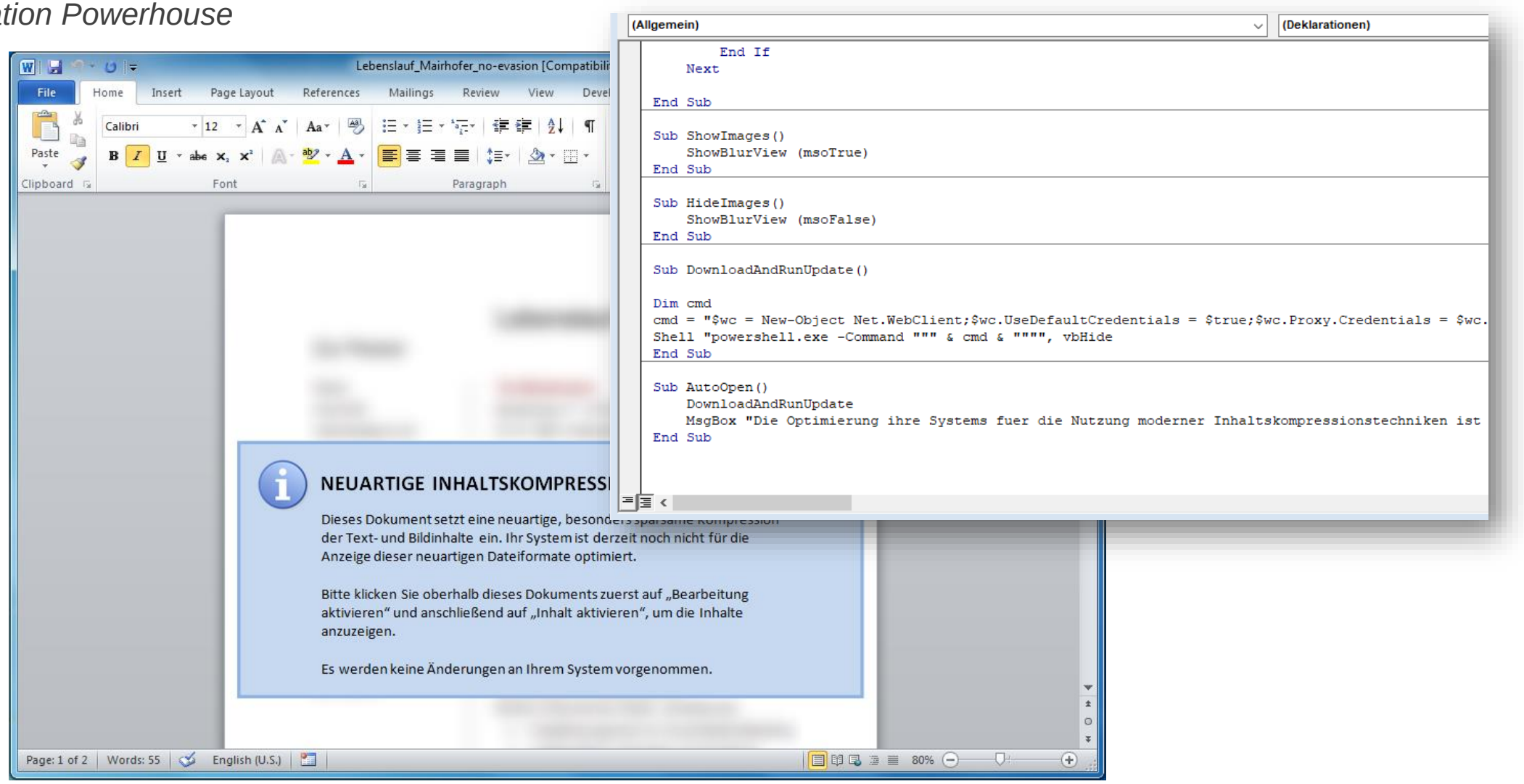
Deine Aufgaben

Wir suchen für unser Digital Media Team eine/n Mitarbeiter/in, die/der uns mit einem hohen Maß an Eigenverantwortung, organisatorischem Talent und lösungsorientiertem Denken bei folgenden Aufgaben unterstützt:

- Inhaltliche Betreuung der Website der EVWV
- Inhaltliche Betreuung des Intranets der EVWV
- Strategic Branding und digitale CI/CD Governance
- Support für digitale Aktivitäten
- Abstimmung mit Werbe-, Digital-, sowie Kommunikationsagenturen
- Mitarbeit an internationalen Kommunikationskampagnen
- Verantwortung des Social Media Auftrittes der EVWV und Abwicklung von Social Media Kampagnen, gemeinsam mit der PR-Agentur
- Mitarbeit bei einzelnen strategischen vorstandsrelevanten Projekten

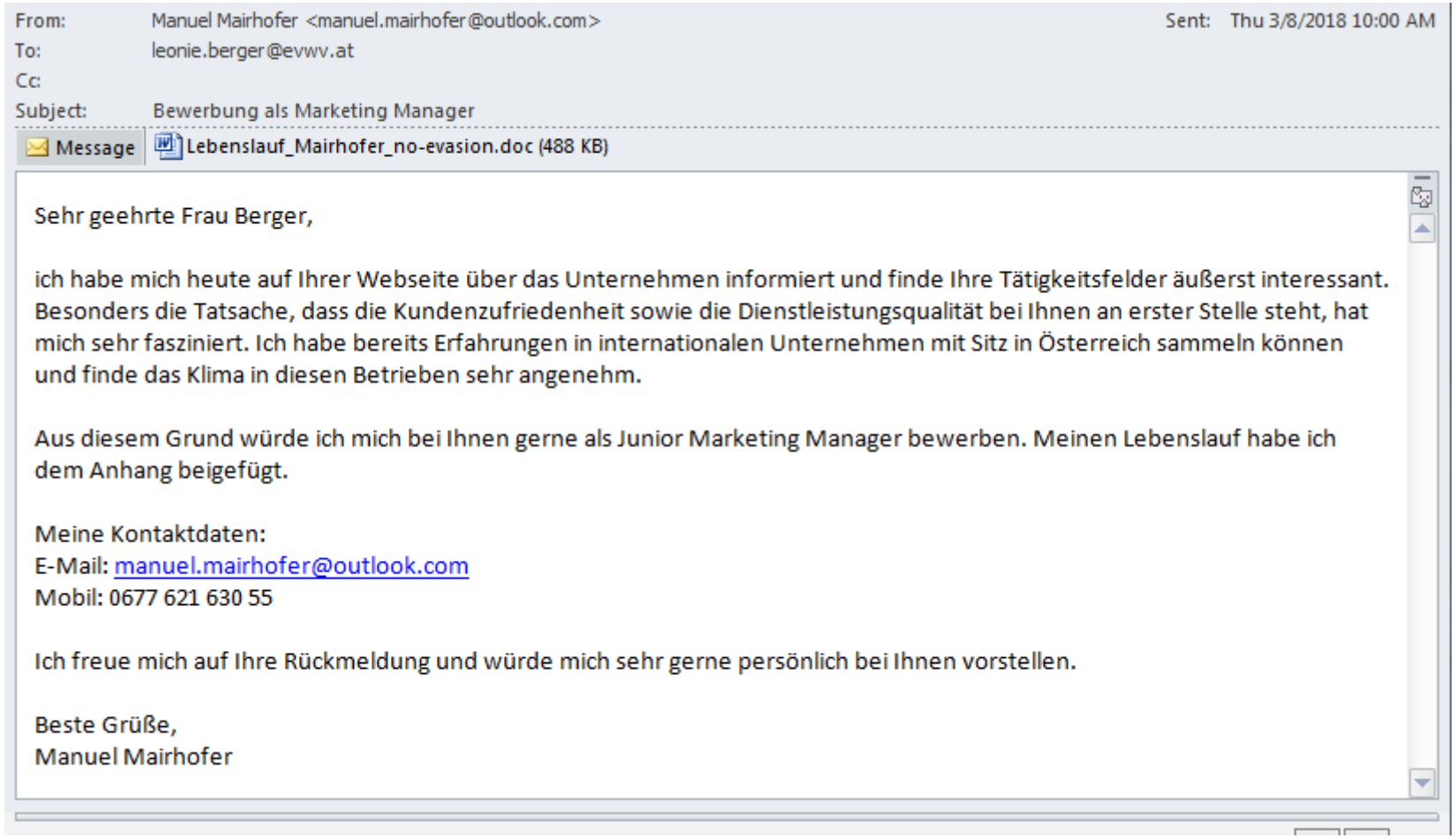
Versuch #1

Operation Powerhouse



Versuch #1

Operation Powerhouse



From: Manuel Mairhofer <manuel.mairhofer@outlook.com> Sent: Thu 3/8/2018 10:00 AM
To: leonie.berger@evwv.at
Cc:
Subject: Bewerbung als Marketing Manager
Message Lebenslauf_Mairhofer_no-evasion.doc (488 KB)

Sehr geehrte Frau Berger,

ich habe mich heute auf Ihrer Webseite über das Unternehmen informiert und finde Ihre Tätigkeitsfelder äußerst interessant. Besonders die Tatsache, dass die Kundenzufriedenheit sowie die Dienstleistungsqualität bei Ihnen an erster Stelle steht, hat mich sehr fasziniert. Ich habe bereits Erfahrungen in internationalen Unternehmen mit Sitz in Österreich sammeln können und finde das Klima in diesen Betrieben sehr angenehm.

Aus diesem Grund würde ich mich bei Ihnen gerne als Junior Marketing Manager bewerben. Meinen Lebenslauf habe ich dem Anhang beigefügt.

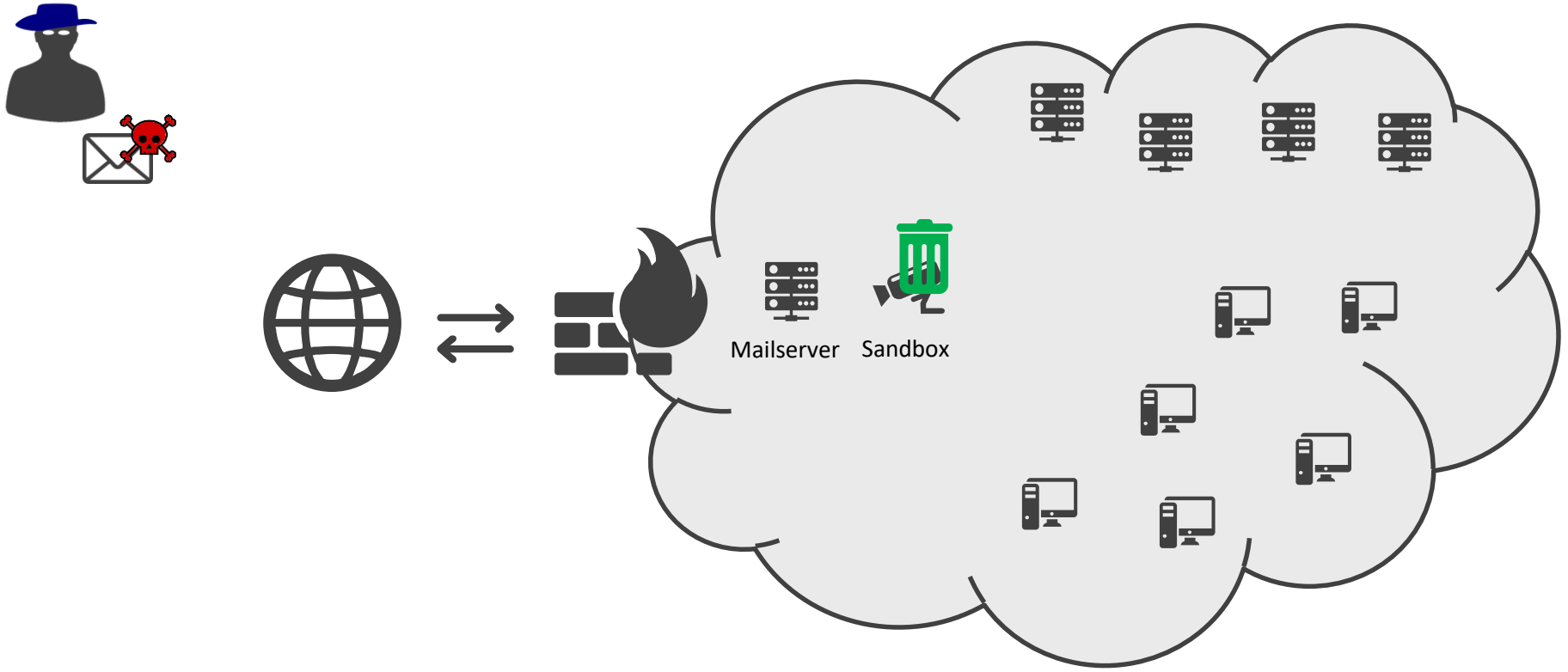
Meine Kontaktdaten:
E-Mail: manuel.mairhofer@outlook.com
Mobil: 0677 621 630 55

Ich freue mich auf Ihre Rückmeldung und würde mich sehr gerne persönlich bei Ihnen vorstellen.

Beste Grüße,
Manuel Mairhofer

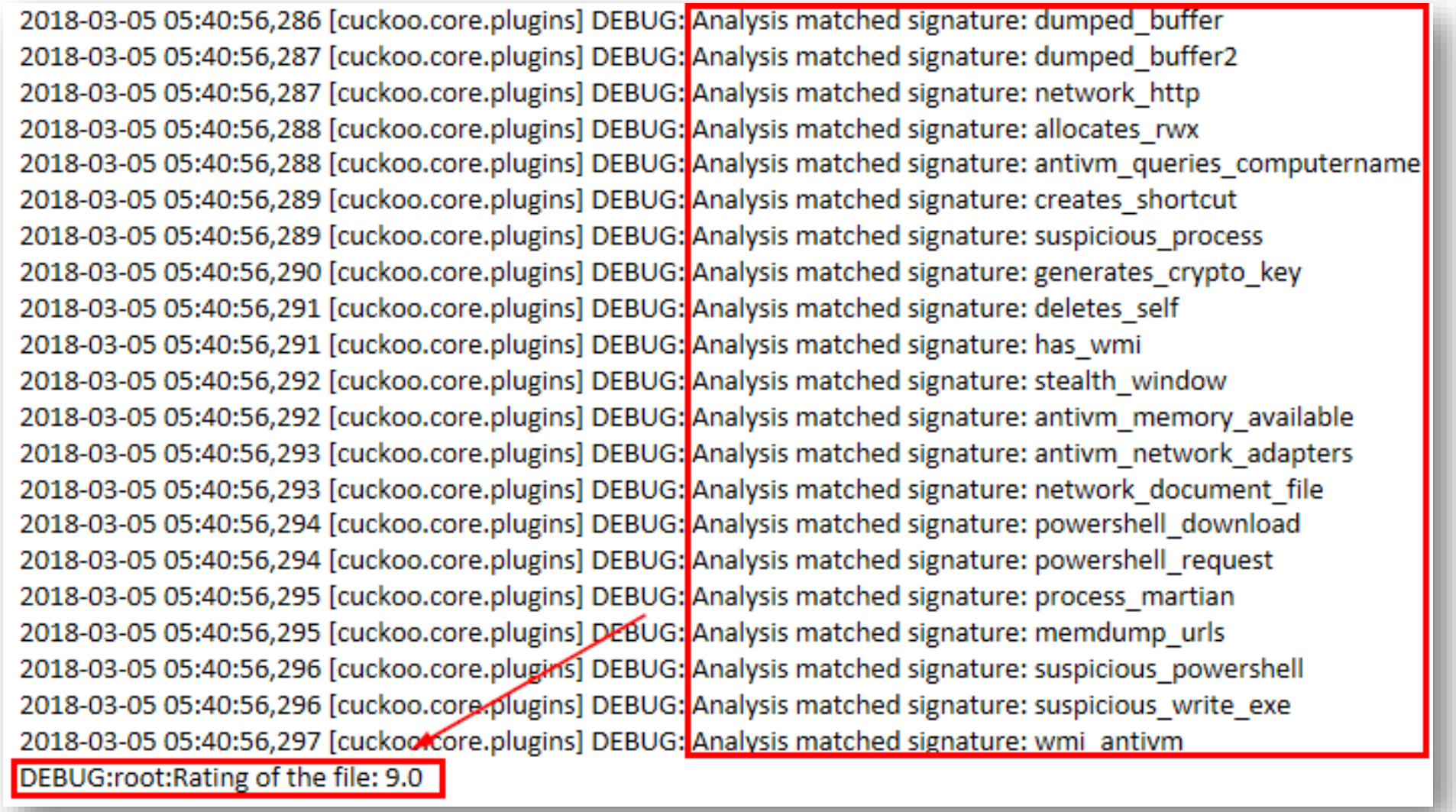
Das Problem: Die Sandbox

Operation Powerhouse



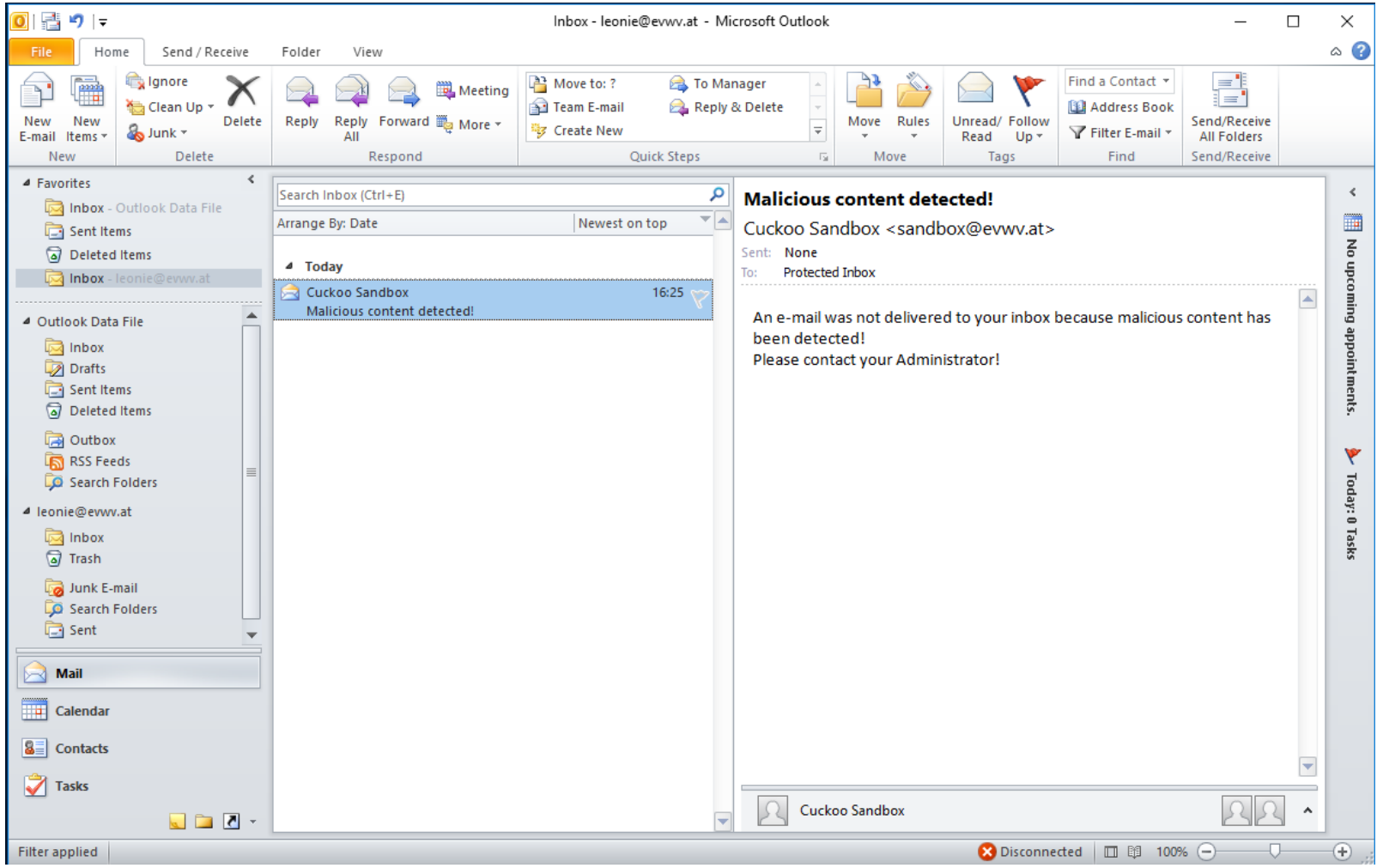
Versuch #1

Operation Powerhouse



Versuch #1

Operation Powerhouse

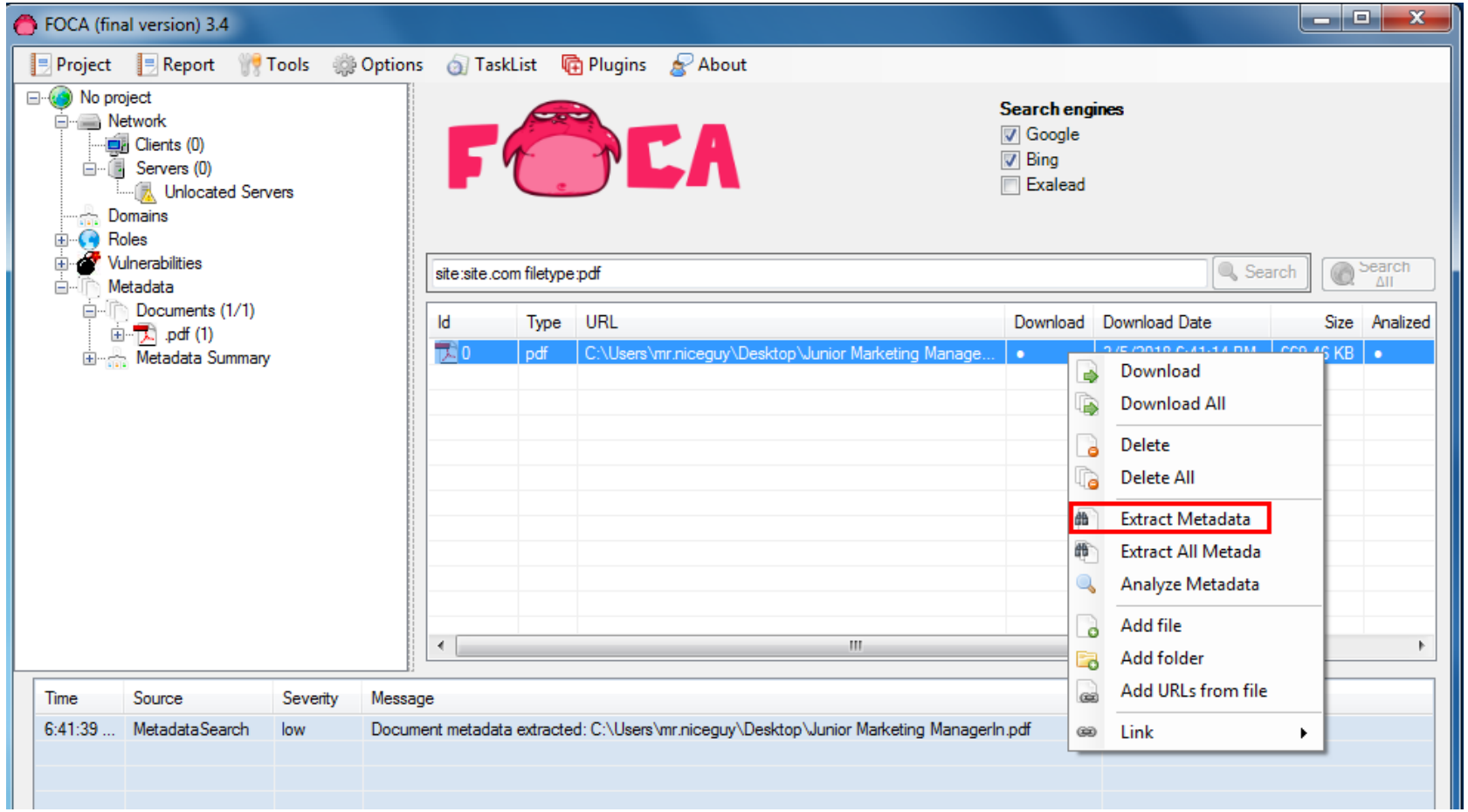


kapsch
challenging limits

Versuch #2

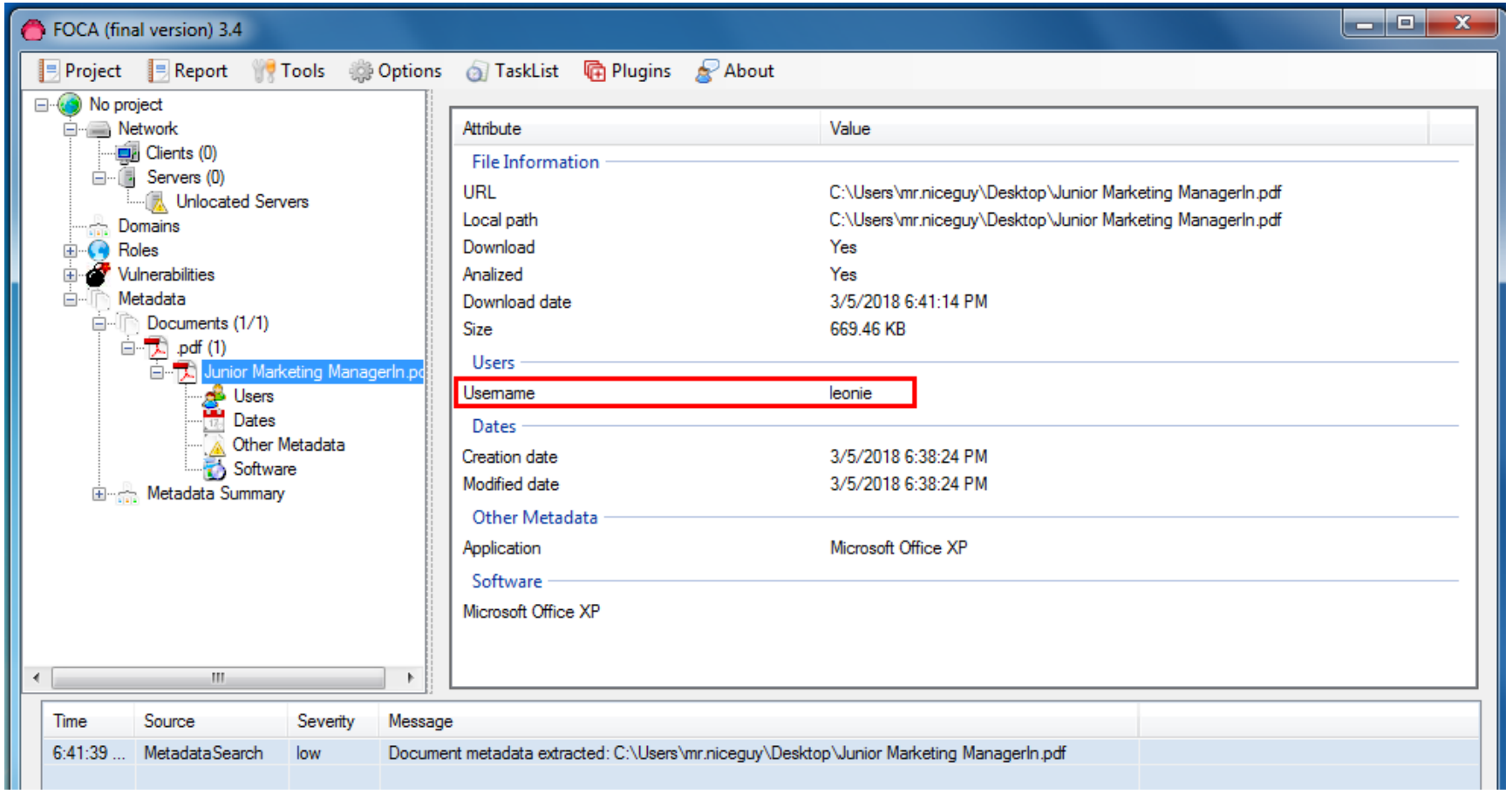
Versuch #2

Operation Powerhouse



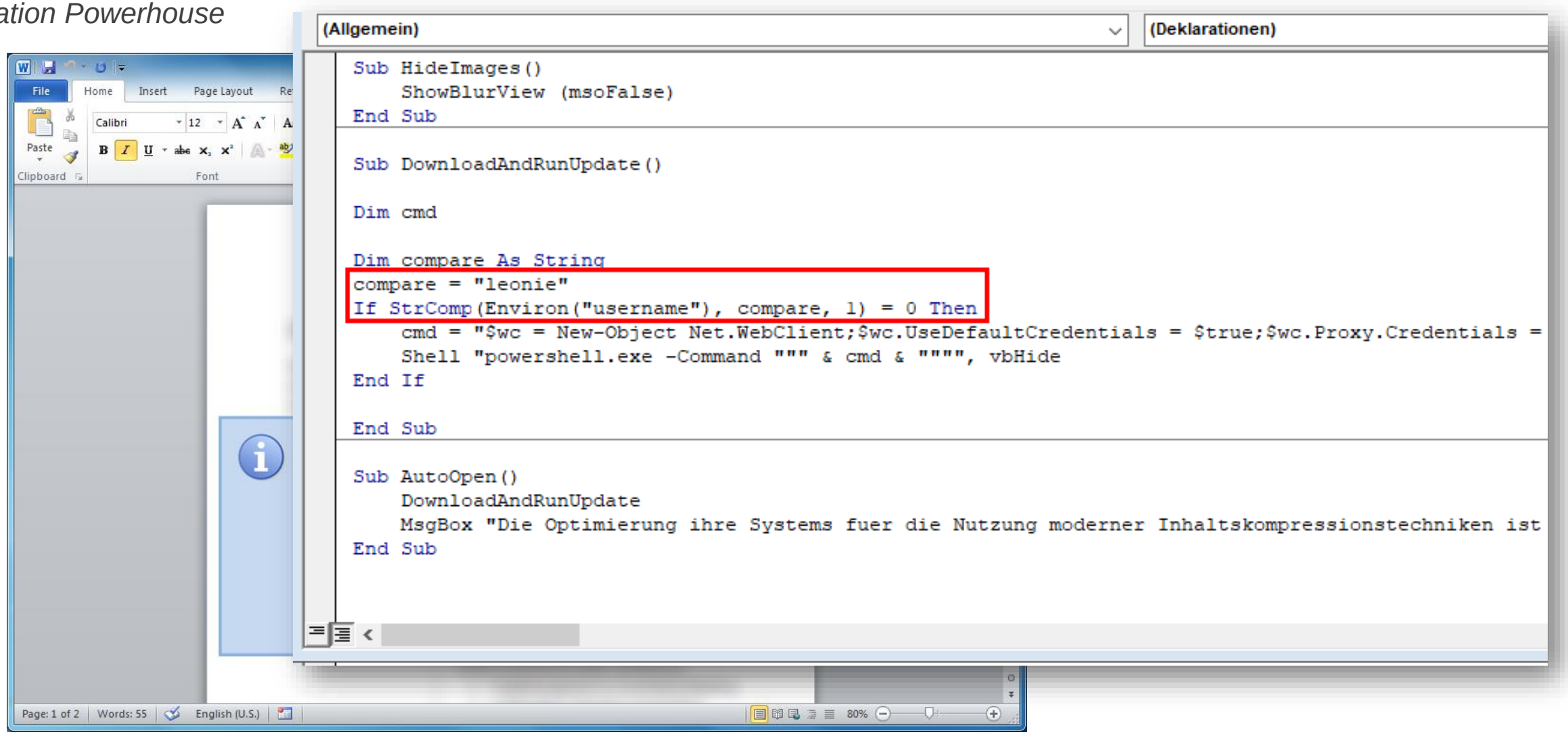
Versuch #2

Operation Powerhouse



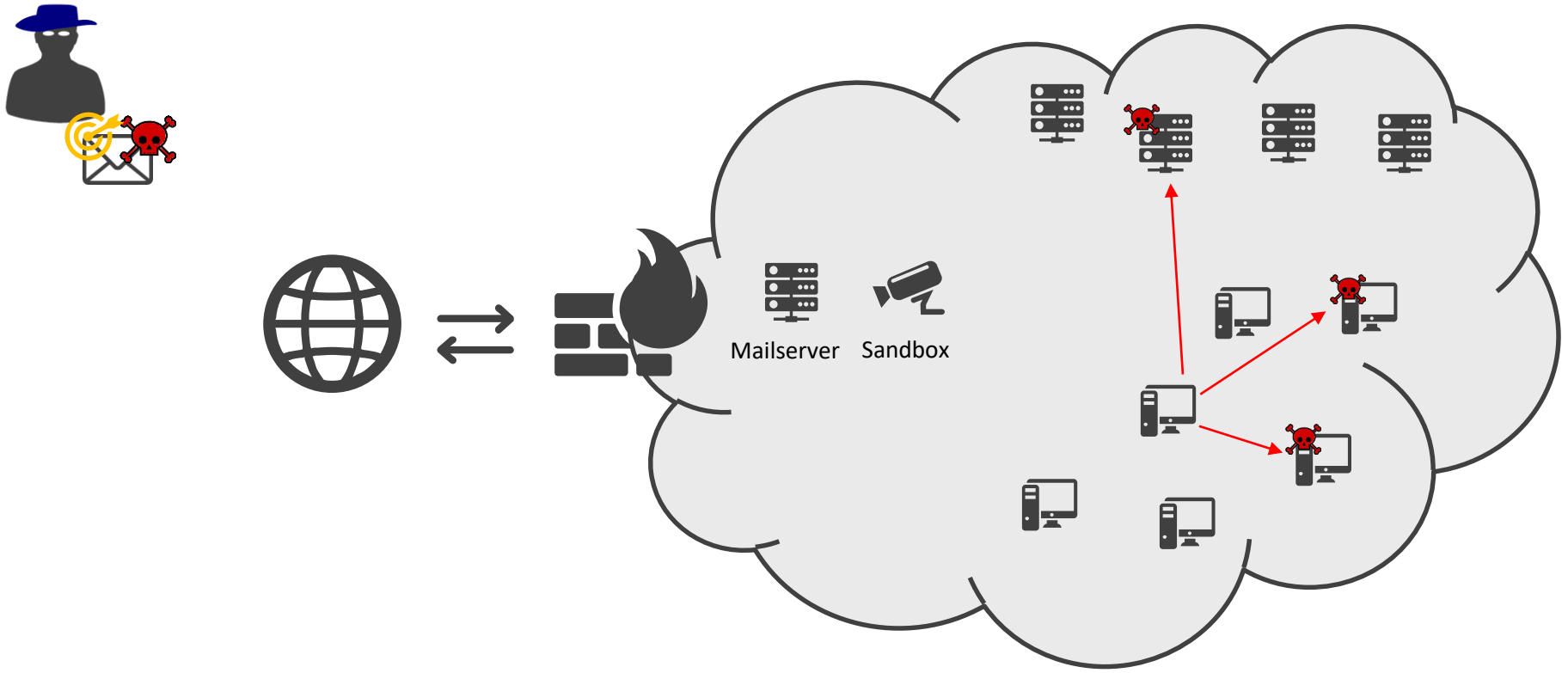
Versuch #2

Operation Powerhouse



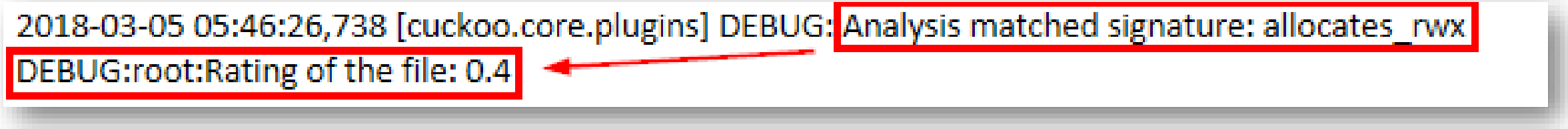
Die Lösung: Environmental Keying

Operation Powerhouse



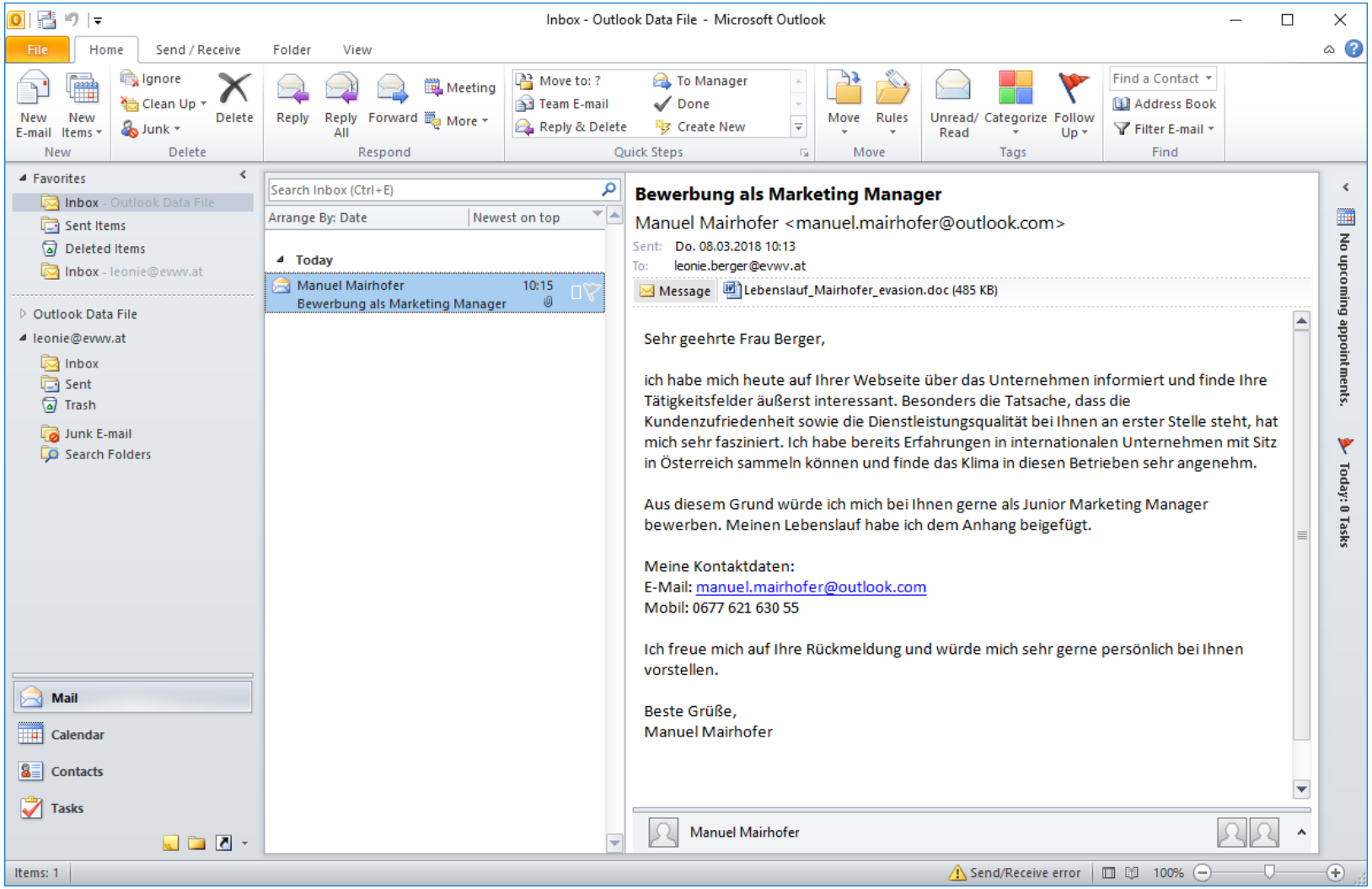
Versuch #2

Operation Powerhouse



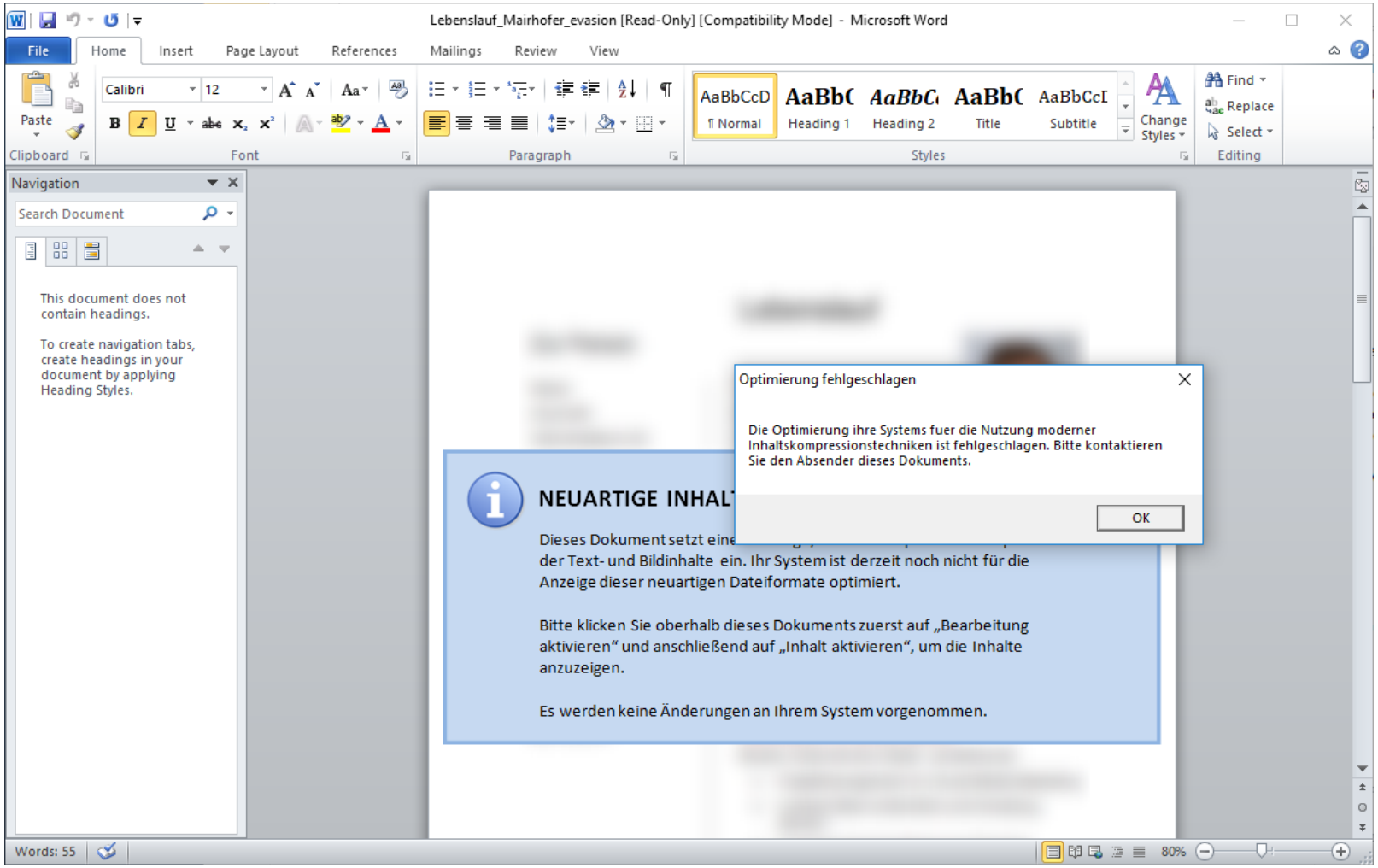
Versuch #2

Operation Powerhouse



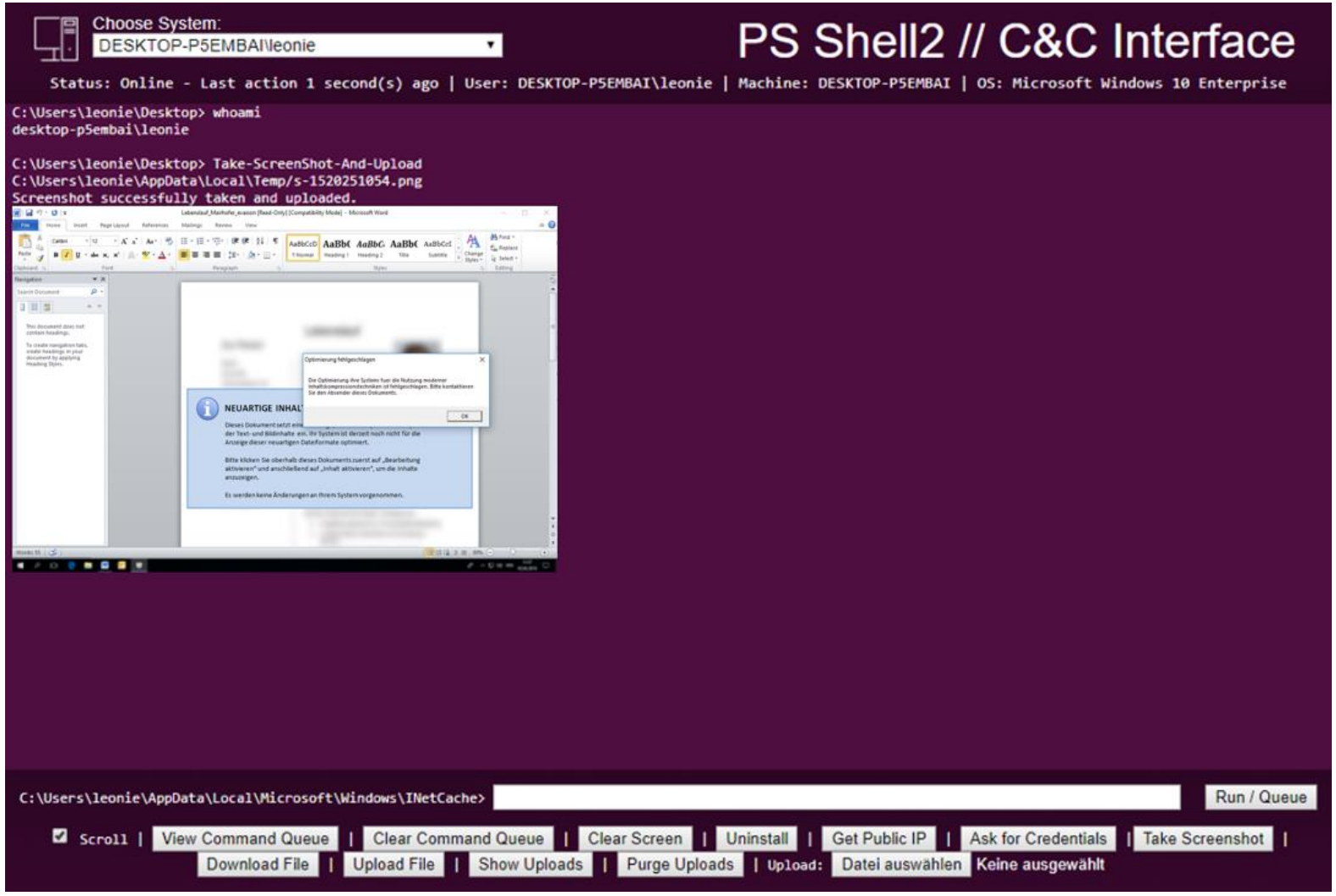
Versuch #2

Operation Powerhouse



Versuch #2

Operation Powerhouse



kapsch
challenging limits

Fazit

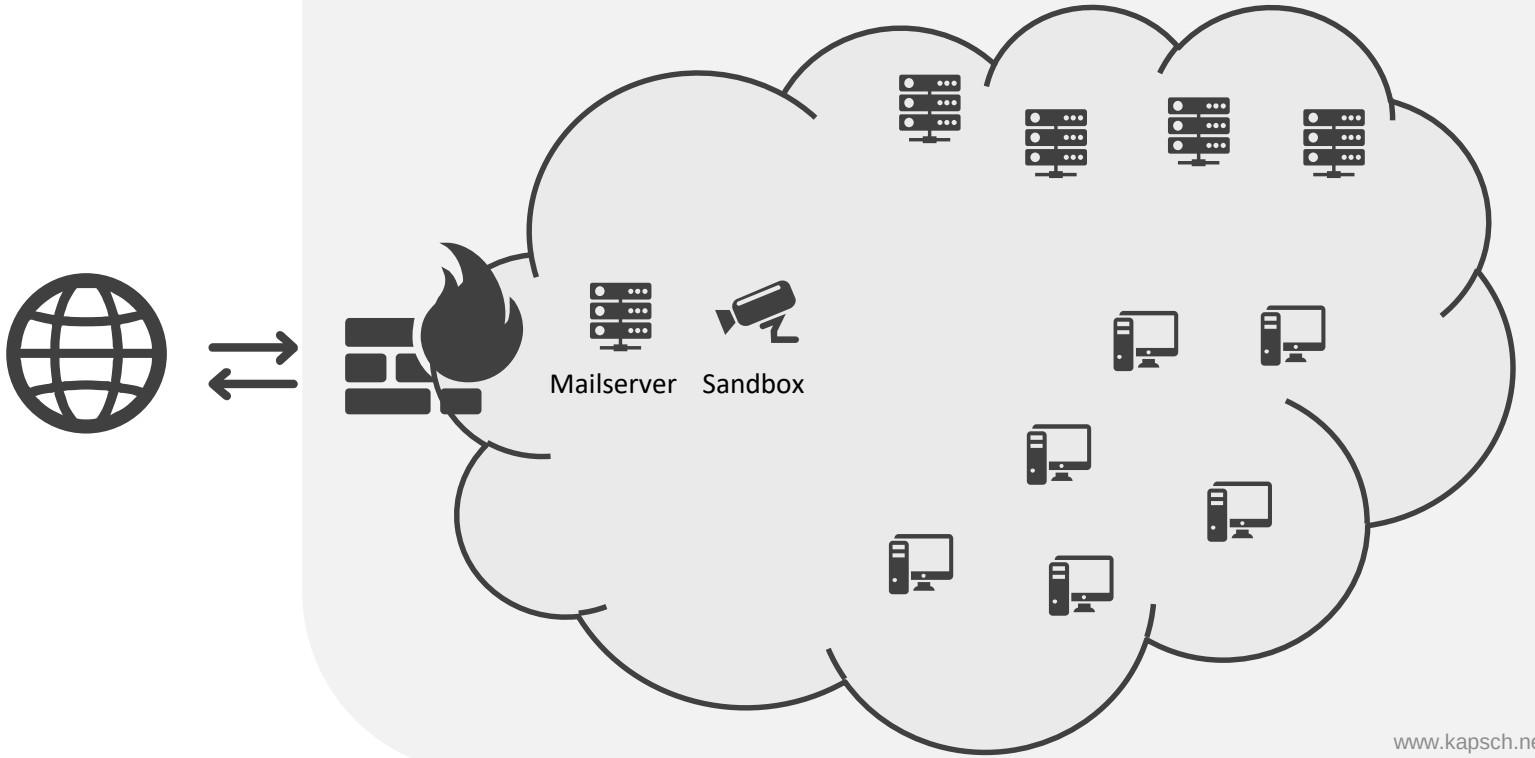
Prevention Fails


3
4

Defensible Network

- NSM
- EDR
- Log
- Vuln Scanning

Cyber Defense Technologie Stack



Defensible Network

NSM

EDR

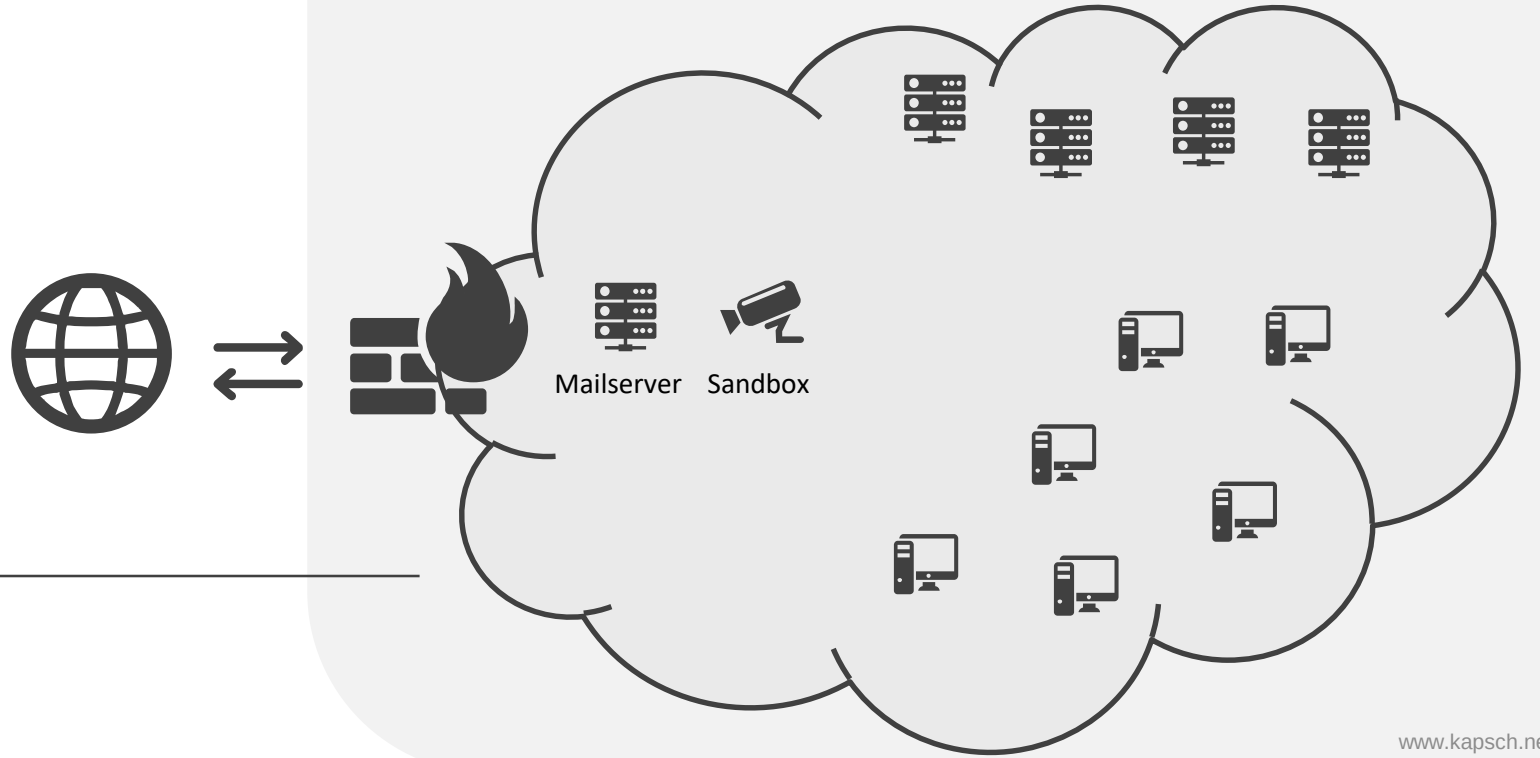
Log

Vuln Scanning

Threat Intel

Ticketing

Cyber Defense Technologie Stack



Defensible Network

NSM

EDR

Log

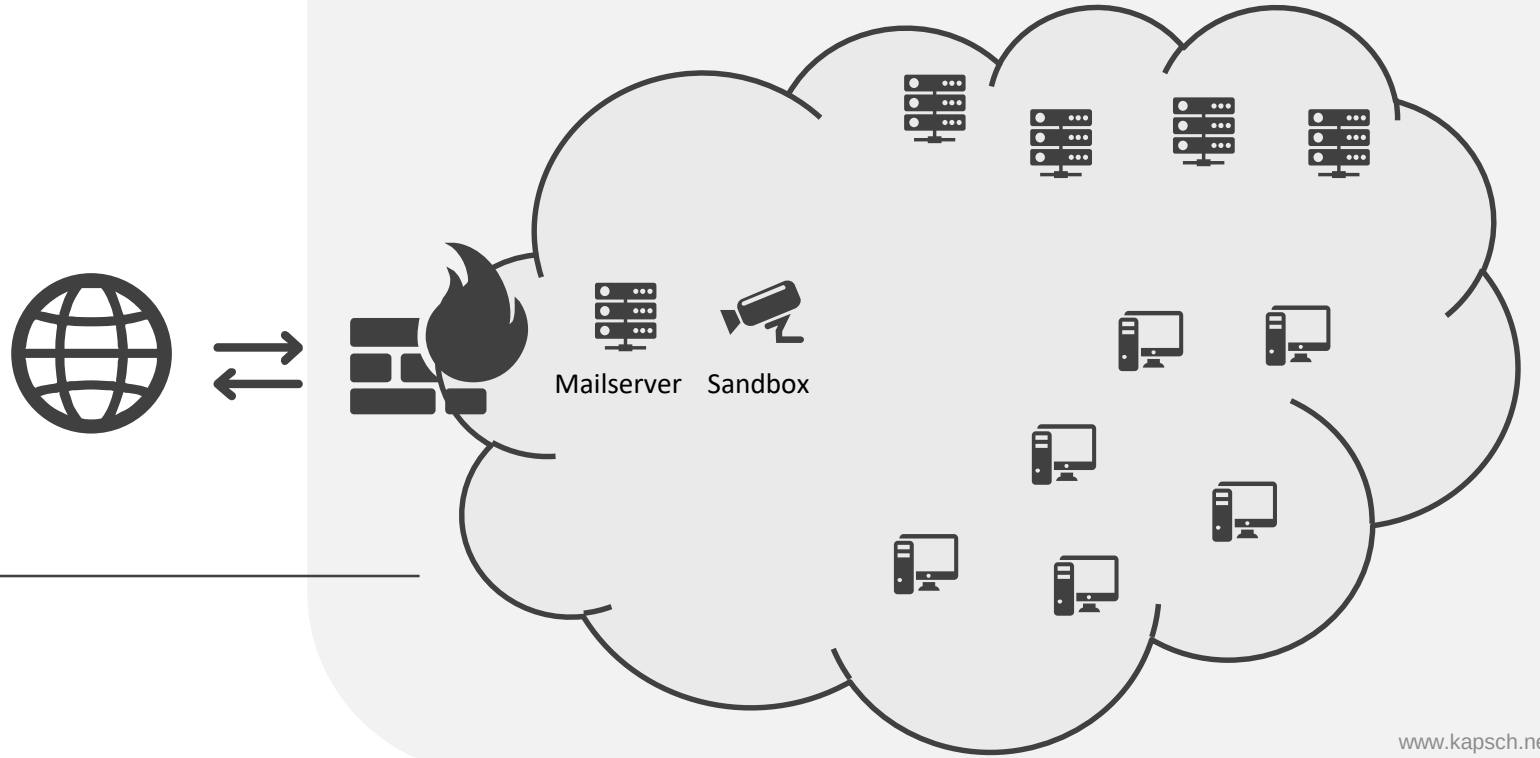
Vuln Scanning

Hunting

Threat Intel

Ticketing

Cyber Defense Technologie Stack



Defensible Network

NSM

EDR

Log

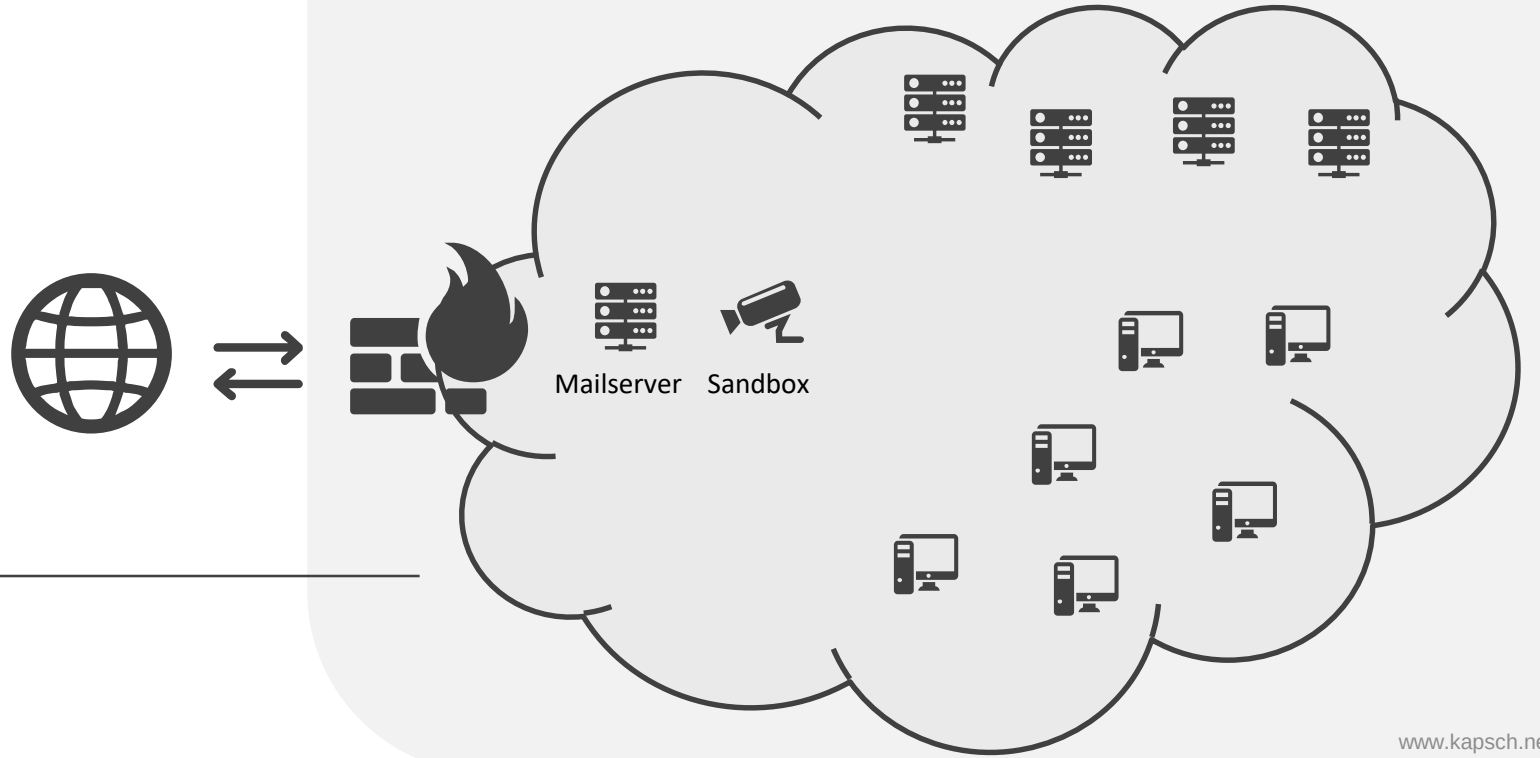
Vuln Scanning

Hunting

Threat Intel

Ticketing

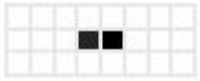
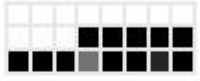
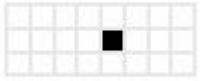
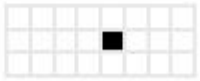
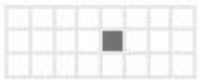
Cyber Defense Technologie Stack



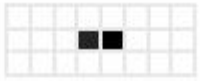
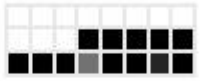
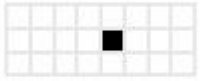
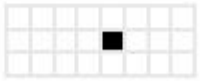
Operation Powerhouse

1. NSM - Network Monitoring
2. EDR – Endpoint
3. LOG – Logging

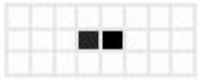
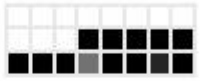
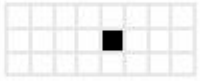
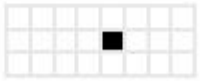
NSM Alert Overview

8	1	1		12:46:44	[BRO] Intel-ADDR - 62.218.147.233
77	7	15		12:36:26	[BRO] SSL-Invalid_Server_Cert
6	1	1		12:33:41	ET POLICY Office Document Containing AutoOpen Macro Via smtp
10	1	1		12:30:21	SURICATA HTTP unable to match response to request
2	2	1		12:14:41	ET POLICY Http Client Body contains pass= in cleartext
185	3	1		11:21:28	ET POLICY DNS Update From External net
85	2	4		06:04:31	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
2	5	1	1		13:47:51	[OSSEC] User login failed.
1	1	1		13:00:01	SURICATA zero length padN option

NSM Alert Overview

8	1	1		12:46:44	[BRO] Intel-ADDR - 62.218.147.233
77	7	15		12:36:26	[BRO] SSL-Invalid_Server_Cert
6	1	1		12:33:41	ET POLICY Office Document Containing AutoOpen Macro Via smtp
10	1	1		12:30:21	SURICATA HTTP unable to match response to request
2	2	1		12:14:41	ET POLICY Http Client Body contains pass= in cleartext
185	3	1		11:21:28	ET POLICY DNS Update From External net
85	2	4		06:04:31	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
2	5	1	1		13:47:51	[OSSEC] User login failed.
1	1	1		13:00:01	SURICATA zero length padN option

NSM Alert Overview

8	1	1		12:46:44	[BRO] Intel-ADDR - 62.218.147.233
77	7	15		12:36:26	[BRO] SSL-Invalid_Server_Cert
6	1	1		12:33:41	ET POLICY Office Document Containing AutoOpen Macro Via smtp
10	1	1		12:30:21	SURICATA HTTP unable to match response to request
2	2	1		12:14:41	ET POLICY Http Client Body contains pass= in cleartext
185	3	1		11:21:28	ET POLICY DNS Update From External net
85	2	4		06:04:31	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
2	5	1	1		13:47:51	[OSSEC] User login failed.
1	1	1		13:00:01	SURICATA zero length padN option

NSM Alert Intel-ADDR 62.218.147.233

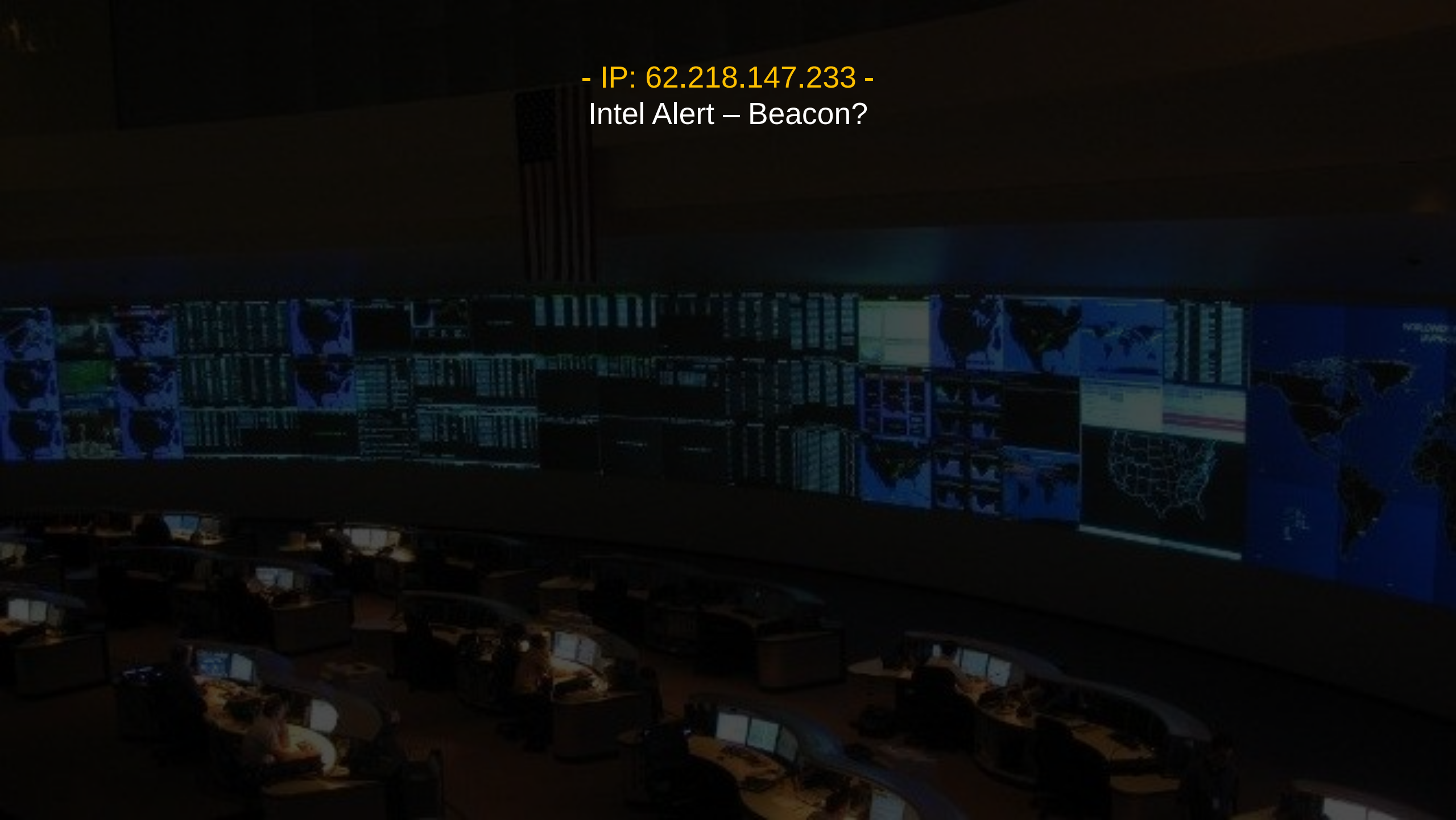
kapsch >>> challenging limits

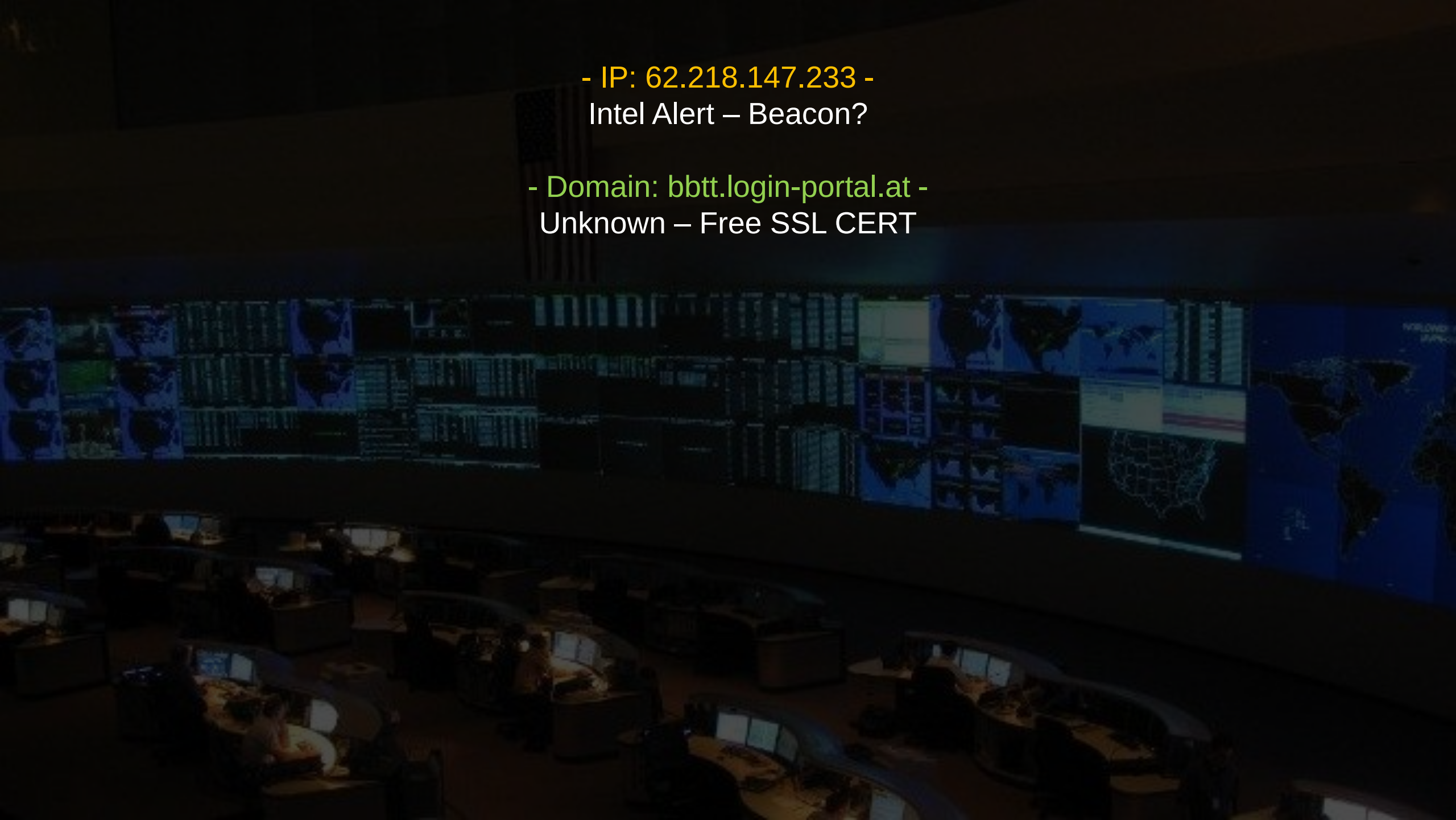
RT	2018-02-28	12:50:30	6.190	10.10.9.3	50671	62.218.147.233	443	[BRO] Intel-ADDR - 62.218.147.233
RT	2018-02-28	12:49:33	6.189	10.10.9.3	50662	62.218.147.233	443	[BRO] Intel-ADDR - 62.218.147.233
RT	2018-02-28	12:48:37	6.188	10.10.9.3	50655	62.218.147.233	443	[BRO] Intel-ADDR - 62.218.147.233
RT	2018-02-28	12:47:40	6.187	10.10.9.3	50647	62.218.147.233	443	[BRO] Intel-ADDR - 62.218.147.233
RT	2018-02-28	12:46:44	6.186	10.10.9.3	50639	62.218.147.233	443	[BRO] Intel-ADDR - 62.218.147.233
RT	2018-02-28	12:45:48	6.185	10.10.9.3	50630	62.218.147.233	443	[BRO] Intel-ADDR - 62.218.147.233
RT	2018-02-28	12:44:48	6.184	10.10.9.3	50620	62.218.147.233	443	[BRO] Intel-ADDR - 62.218.147.233

NSM Alert SSL Connection

Src IP: 10.10.9.3
Dst IP: 62.218.147.233
Src Port: 50340
Dst Port: 443
OS Fingerprint: 10.10.9.3:50340 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint: -> 62.218.147.233:443 (distance 0, link: ethernet/modem)

SRC: ..........Z....KA.~b.ct9~`R..O..M.....b..........9.3.5./.
SRC: ...8.2.
SRC: .....:.....bbtt.login-portal.at.
SRC: ....#..........
DST: ....A...=...../.|3.....$..7..7;.7Ba
DST: ....#.............0...0.....'.6.+..)...8?..0
DST: ..*.H..
DST: .....0J1.0...U....US1.0...U.
DST: .
DST: Let's Encrypt1#0!..U...Let's Encrypt Authority X30..


- IP: 62.218.147.233 -
Intel Alert – Beacon?

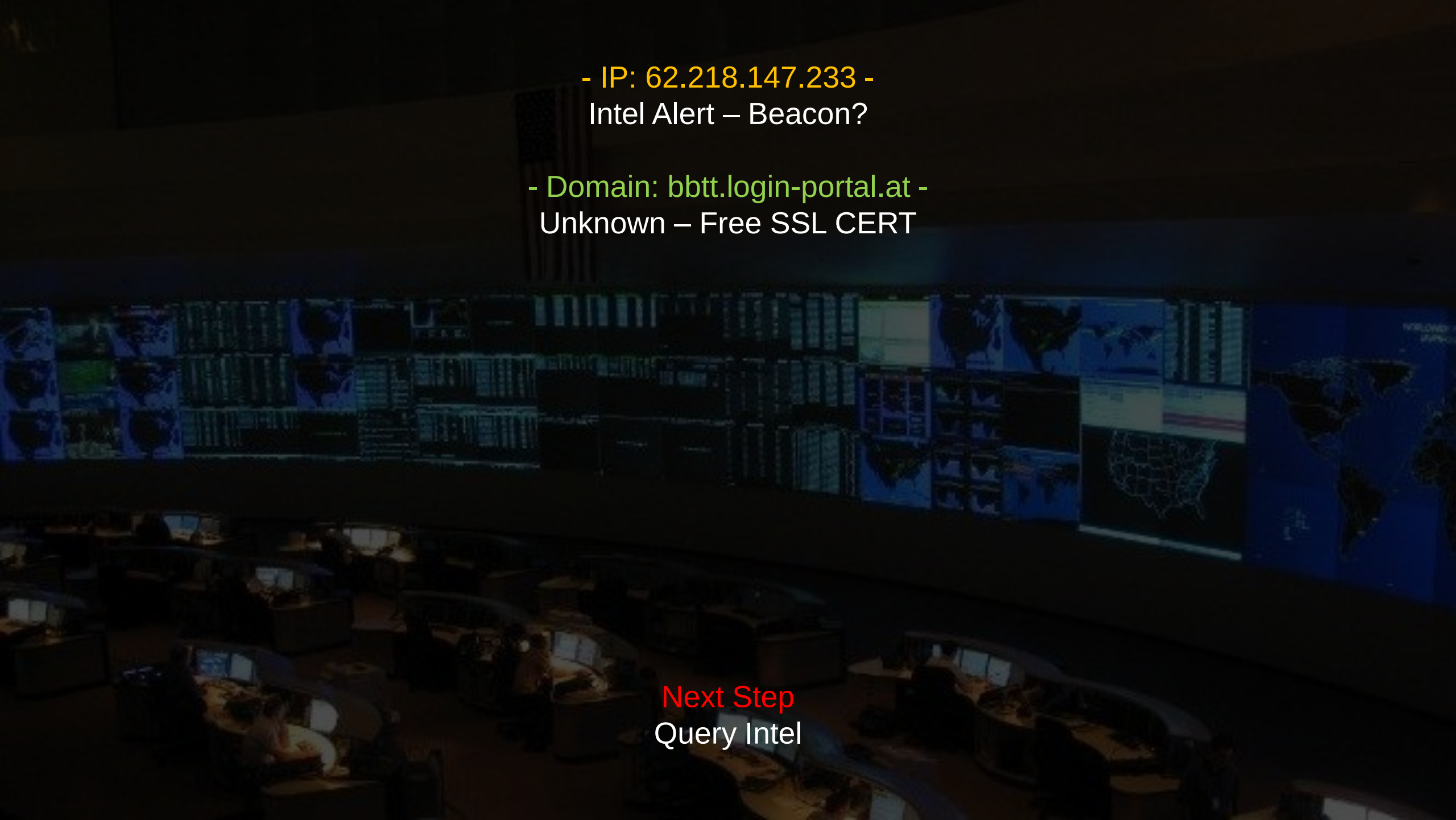


- IP: 62.218.147.233 -

Intel Alert – Beacon?

- Domain: bbtt.login-portal.at -

Unknown – Free SSL CERT


- IP: 62.218.147.233 -
Intel Alert – Beacon?
- Domain: bbtt.login-portal.at -
Unknown – Free SSL CERT
Next Step
Query Intel

Intel Check – login-portal.at

kapsch >>> challenging limits

login-portal[.]at

Unknown

OTX:Pulses="0" VT:Score="0 detected_url(s)" PT:Malware="False" Umbrella:Sec-Category="[]"
PT:OSINT="False" Umbrella:Content-Category="[]" PhishTank:In_Database="False" Domain:Updated="2018-02-26"
Umbrella:Sec-Rank="0.0" CIRCL:PassiveDNS="0 record" Autofocus:Samples="0" Umbrella:First-Seen="2018-02-26"
Shodan:IPs="0" Shodan:Domains="0" Shodan:ASNs="0" Shodan:ISPs="0" MISP:Search="No events"

Intel Check – 62.218.147.233

62[.]218[.]147[.]233

APT Waldviertel

VT:Score="18 detected_url(s)" PT:OSINT="False" Umbrella:Content-Category="[]" Umbrella:Sec-Category="[]"
CIRCL:PassiveSSL="3 records" MISP:Search="1 event(s)"

Intel Check – Known Domains

kapsch >>> challenging limits

Score	Scan Date	URL
7/67	2018-02-23 20:10:08	hxxp://secure-login[.]at/secnight2017/hidden-tear[.]exe[.]txt
5/67	2018-02-08 20:08:31	hxxp://secure-login[.]at/
5/66	2017-12-19 12:10:27	hxxps://secure-login[.]at/secnight2017/decrypt-log[.]php?info=,Pattern
2/66	2017-12-19 12:10:27	hxxps://www[.]sslv3[.]at/secnight2017/msg[.]htm
8/64	2017-11-08 13:35:08	hxxp://sslv3[.]at/tools/ps_shell2_hxxps[.]ex_[.]html
8/63	2017-10-26 03:19:16	hxxp://www[.]sslv3[.]at/cryptolocker/encrypt2[.]exe
2/64	2017-10-25 20:13:16	hxxp://secure-login[.]at/secnight2017
3/64	2017-10-11 12:58:37	hxxps://secure-login[.]at/secnight2017/launcher[.]ps1[.]txt

Intel Check – Shared Events

EventID: 155441

Event info: Operation Powerhouse

UUID: 5a9526d0-c544-40af-bc86-5527ac12306d

Tags: misp-galaxy:mitre-tool="PsExec"

Cluster: : PsExec

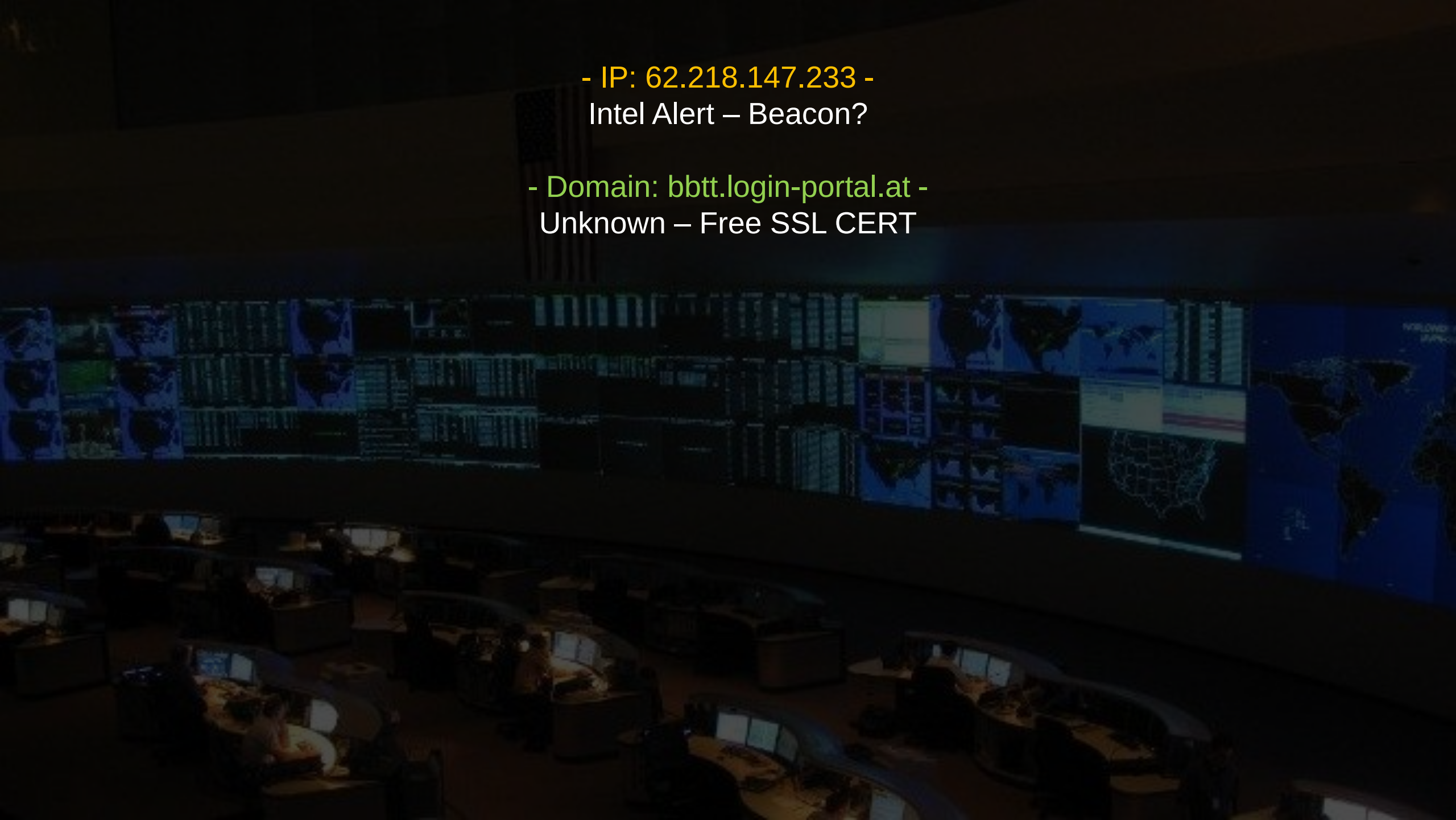
Related events:

Dridex of the day (2016-02-01) - botnet 123

APT1 - Mandiant - http://intelreport.mandiant.com/

Intel Check – Shared Events

Category	Type	Value
Artifacts dropped	filename	a.exe
External analysis	link	https://www.virustotal.com/#/url/b2778d2b100d7ae768ffe64da58a2f0ac68fb62eb63a86689939ecaded9379ae/detection
Network activity	ip-dst	62.218.147.233
Network activity	domain	secure-login.at
Network activity	domain	sslv3.at
Other	comment	Threat Actor: APT Waldviertel
Targeting data	target-org	Power-Plants

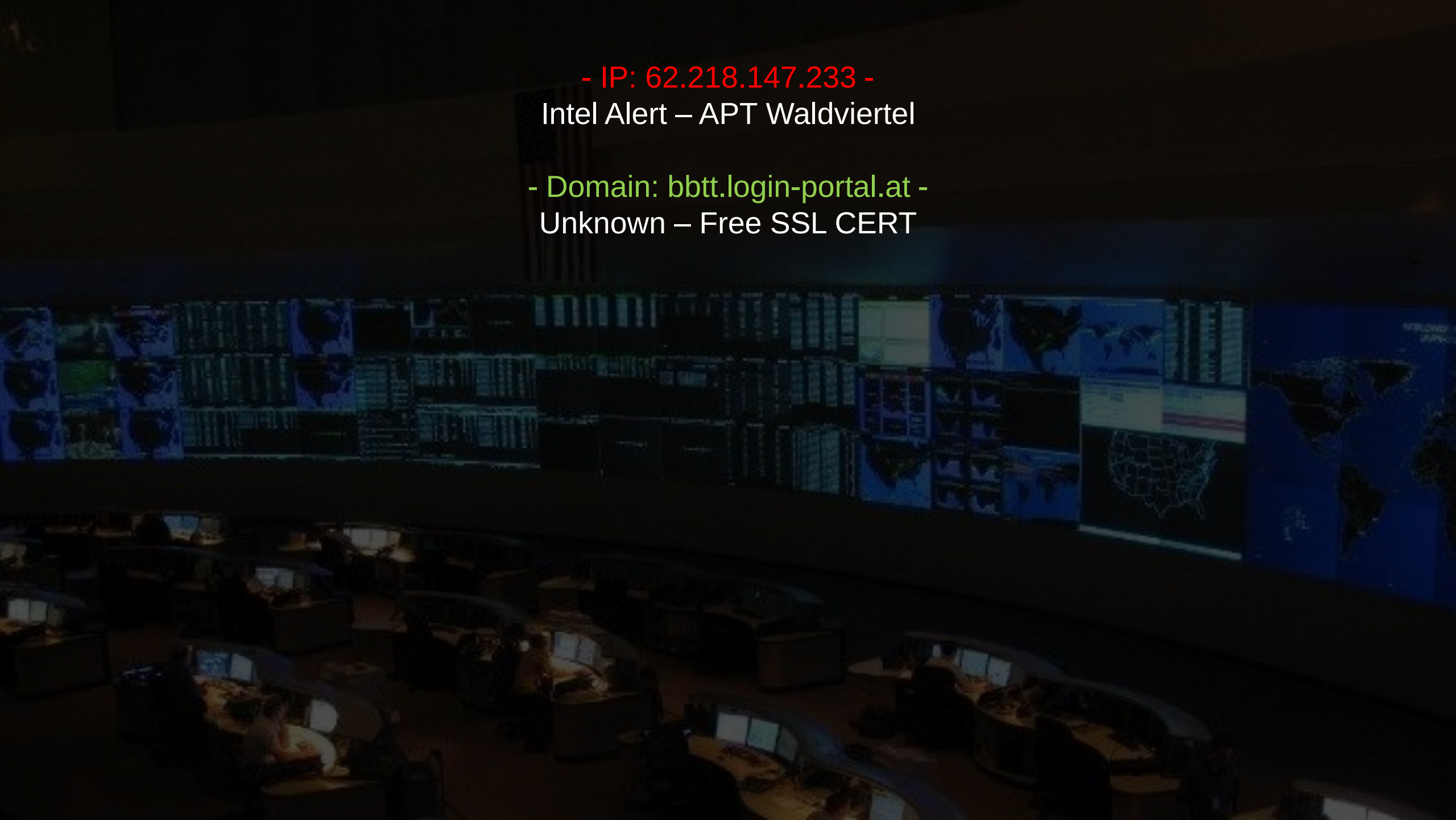


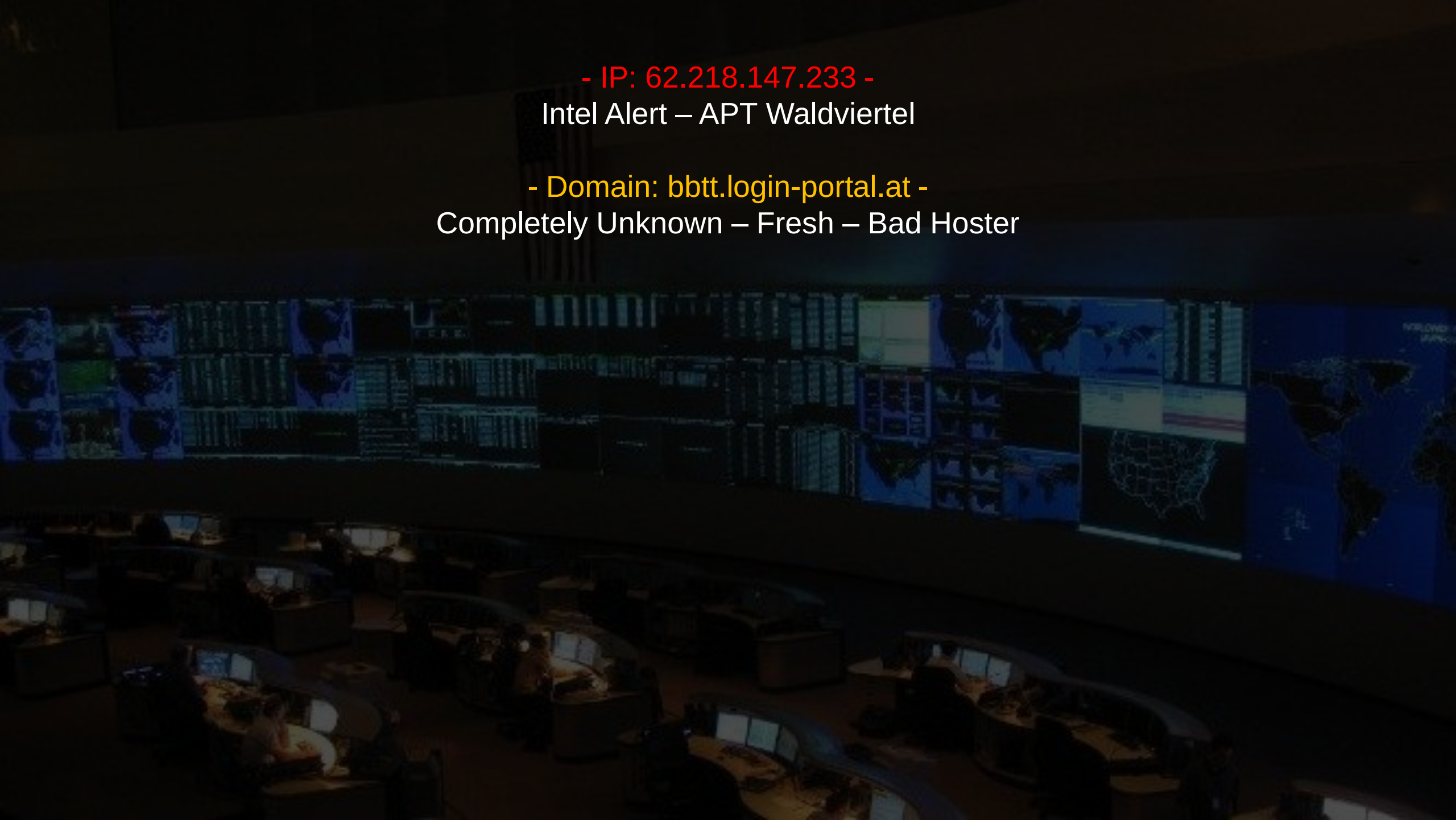
- IP: 62.218.147.233 -

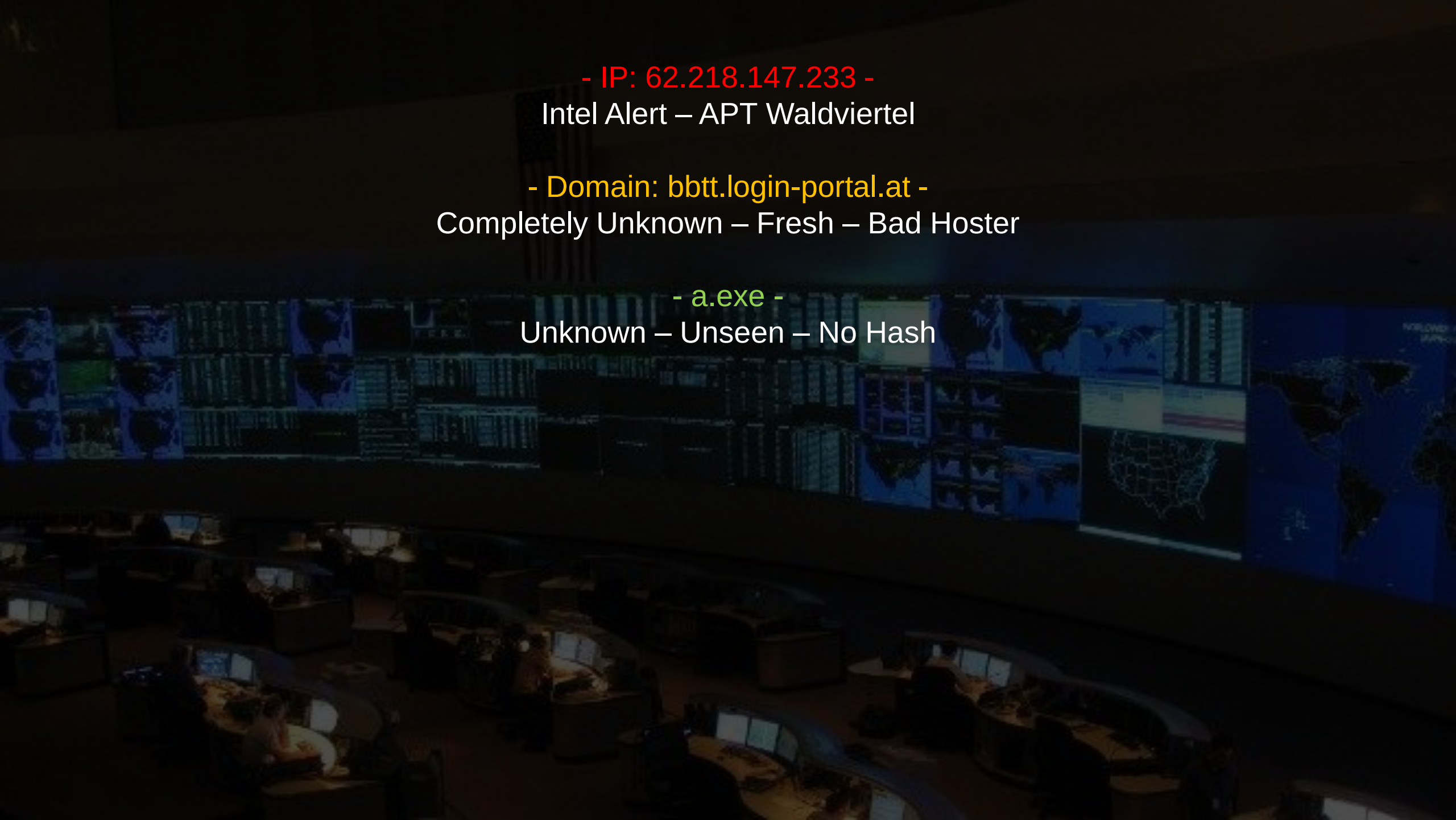
Intel Alert – Beacon?

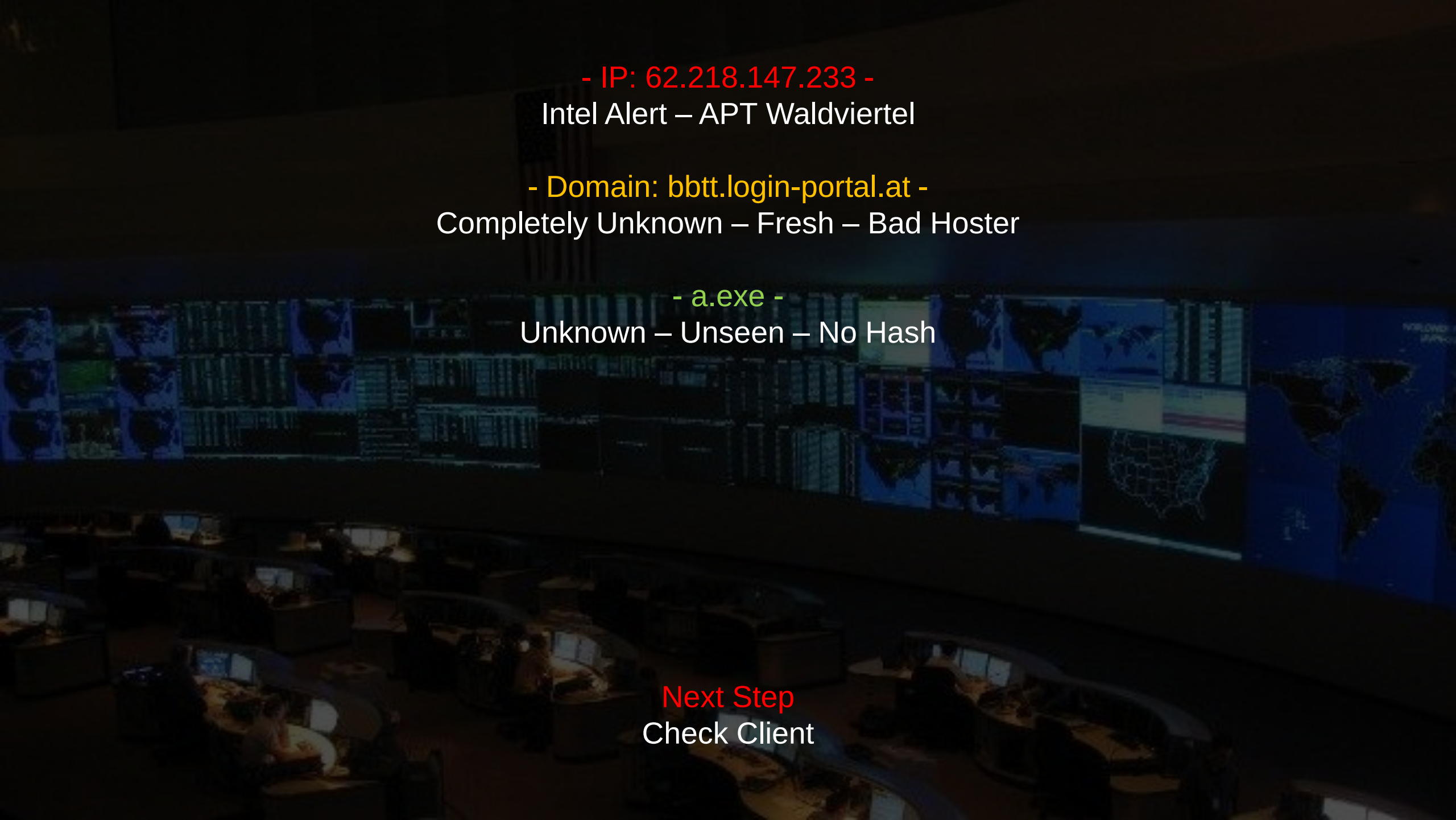
- Domain: bbtt.login-portal.at -

Unknown – Free SSL CERT


- IP: 62.218.147.233 -
Intel Alert – APT Waldviertel
- Domain: bbtt.login-portal.at -
Unknown – Free SSL CERT


- IP: 62.218.147.233 -
Intel Alert – APT Waldviertel
- Domain: bbtt.login-portal.at -
Completely Unknown – Fresh – Bad Hoster


- IP: 62.218.147.233 -
Intel Alert – APT Waldviertel
- Domain: bbtt.login-portal.at -
Completely Unknown – Fresh – Bad Hoster
- a.exe -
Unknown – Unseen – No Hash


- IP: 62.218.147.233 -
Intel Alert – APT Waldviertel
- Domain: bbtt.login-portal.at -
Completely Unknown – Fresh – Bad Hoster
- a.exe -
Unknown – Unseen – No Hash
Next Step
Check Client

EDR Alert

kapsch
challenging limits

1
total hosts
with alerts

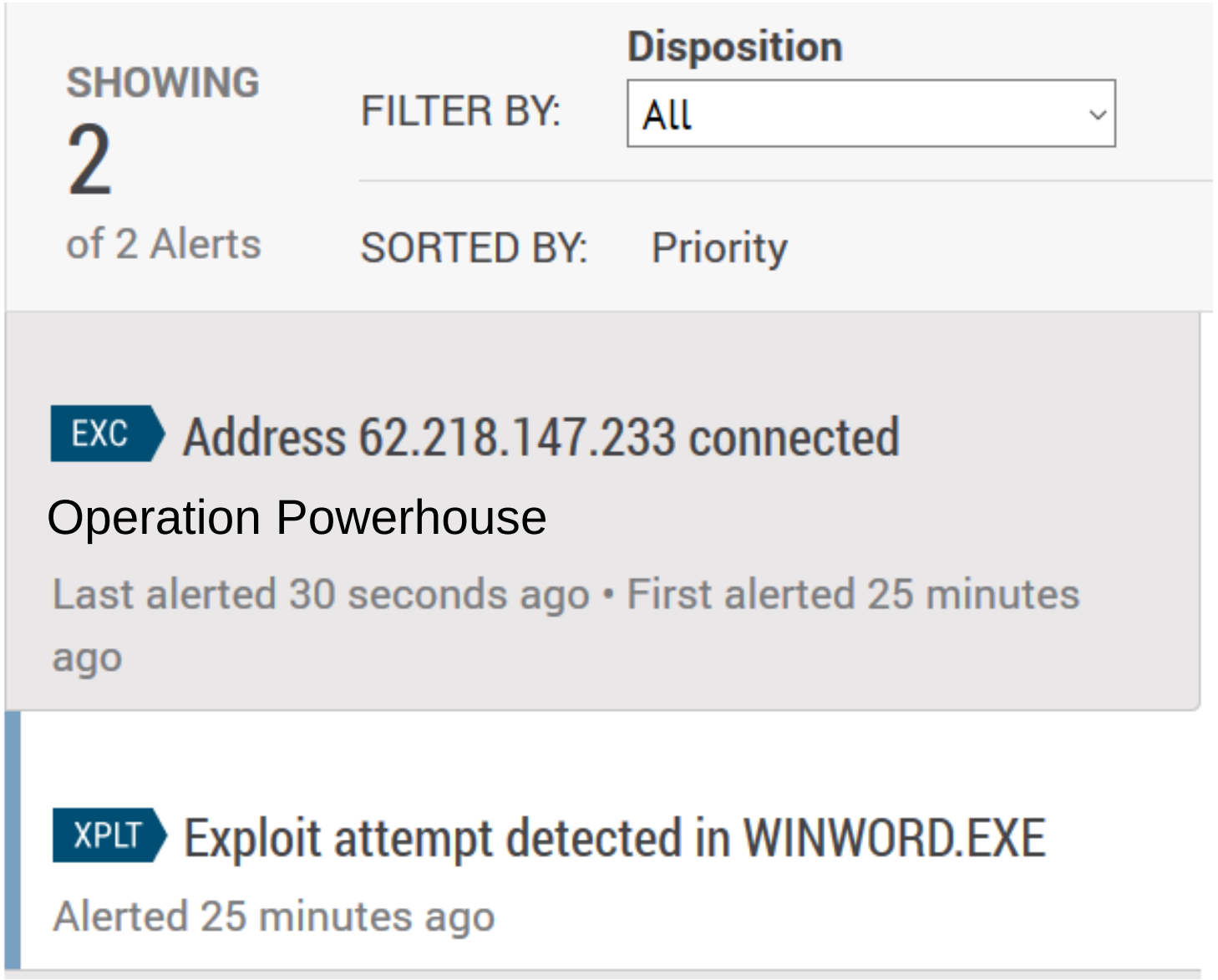
All Exploits blocked on
0 hosts

Alerts detected on
0 high-value hosts

Exploits on
1 host

Malware on
0 hosts

EDR Alert – Overview



EDR Alert – Connection Overview

kapsch
challenging limits

62.218.147.233

Alerted	26 seconds ago
ipv4NetworkEvent/timestamp	2018-02-28 13:15:29Z
ipv4NetworkEvent/remoteIP	62.218.147.233
ipv4NetworkEvent/remotePort	443
ipv4NetworkEvent/localIP	10.10.9.3
ipv4NetworkEvent/localPort	50884
ipv4NetworkEvent/protocol	TCP
ipv4NetworkEvent/pid	5608
ipv4NetworkEvent/process	Microsoft Word Updater.exe
ipv4NetworkEvent/processPath	C:\Users\Leonie.SLOTH\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
ipv4NetworkEvent/username	SLOTH\leonie

EDR Alert – Exploit Overview - Origin

kapsch >>> challenging limits

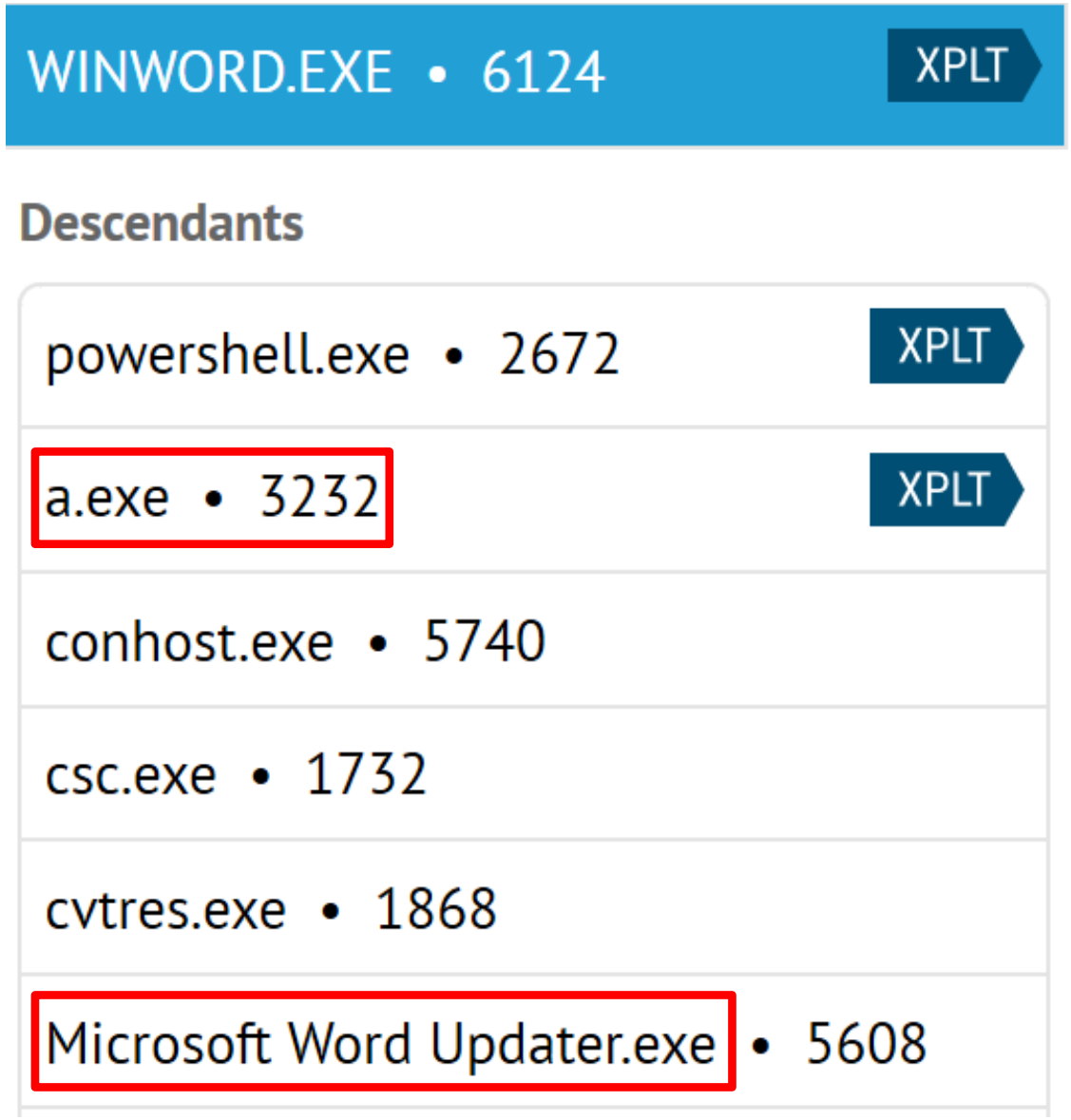
Initial Exploit Process

Exploit detection time	2018-02-28 12:46:49Z
Process path	WINWORD.EXE
Process ID	6124

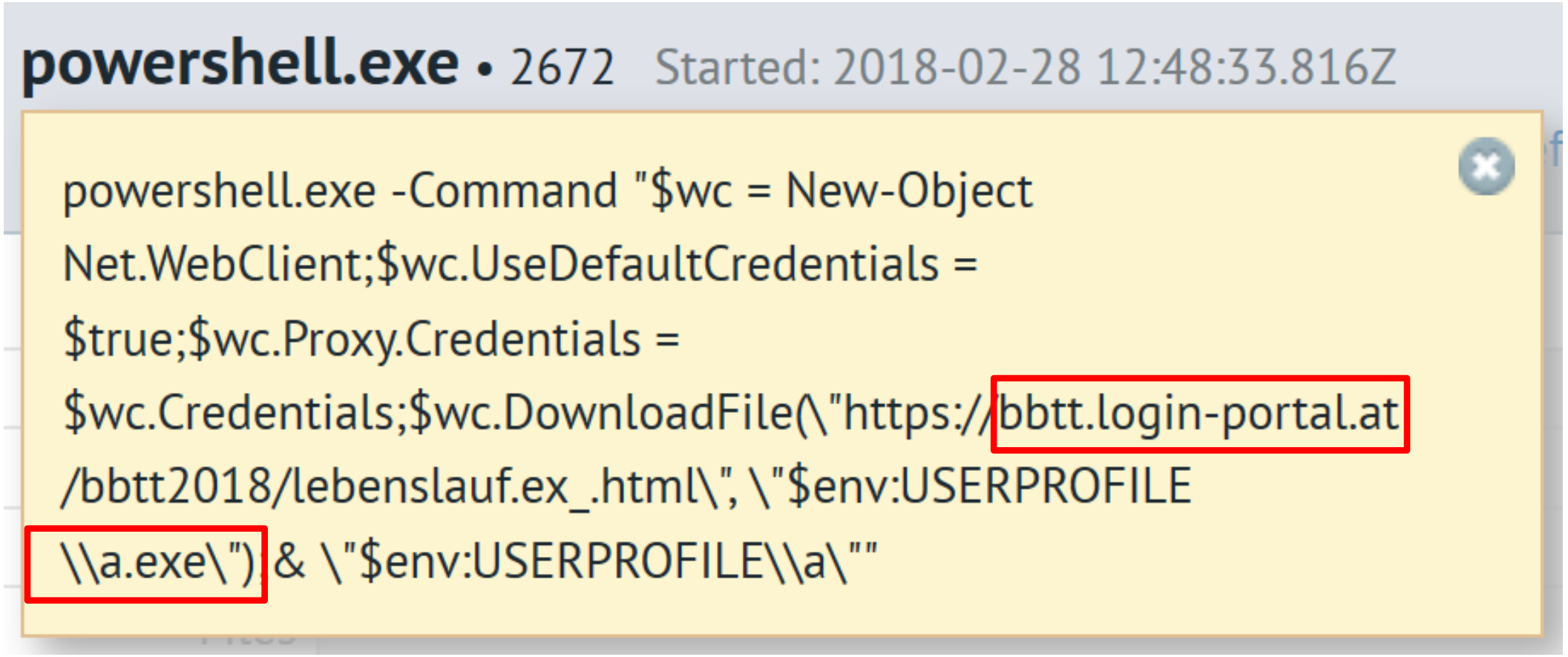
Exploit Documents

- C:\Users\Leonie.SLOTH\AppData\Roaming\Microsoft\Templates\Normal.dotm
- C:\Users\Leonie.SLOTH\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\BJRZQNNO\lebenslauf14.doc

EDR Alert – Exploit Overview – Process Tree



EDR Alert – Powershell – 2nd Stage Download



EDR Alert – a.exe

kapsch challenging limits

1 Registry Keys

From 2018-02-26 06:59:18.731Z to 2018-02-28 12:49:13.997Z

XPLT HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

9 Files

From 2018-02-26 08:10:25.387Z to 2018-02-28 12:49:06.028Z

Path

XPLT ▸ C:\Users\Leonie.SLOTH\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Word Updater.exe

dll ▸ C:\Users\Leonie.SLOTH\AppData\Local\Temp\-jdh14sl.dll

▸ C:\Users\Leonie.SLOTH\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\a.exe.log

▸ C:\Users\Leonie.SLOTH\AppData\Local\Temp\-jdh14sl.0.cs

▸ C:\Users\Leonie.SLOTH\AppData\Local\Temp\-jdh14sl.cmdline

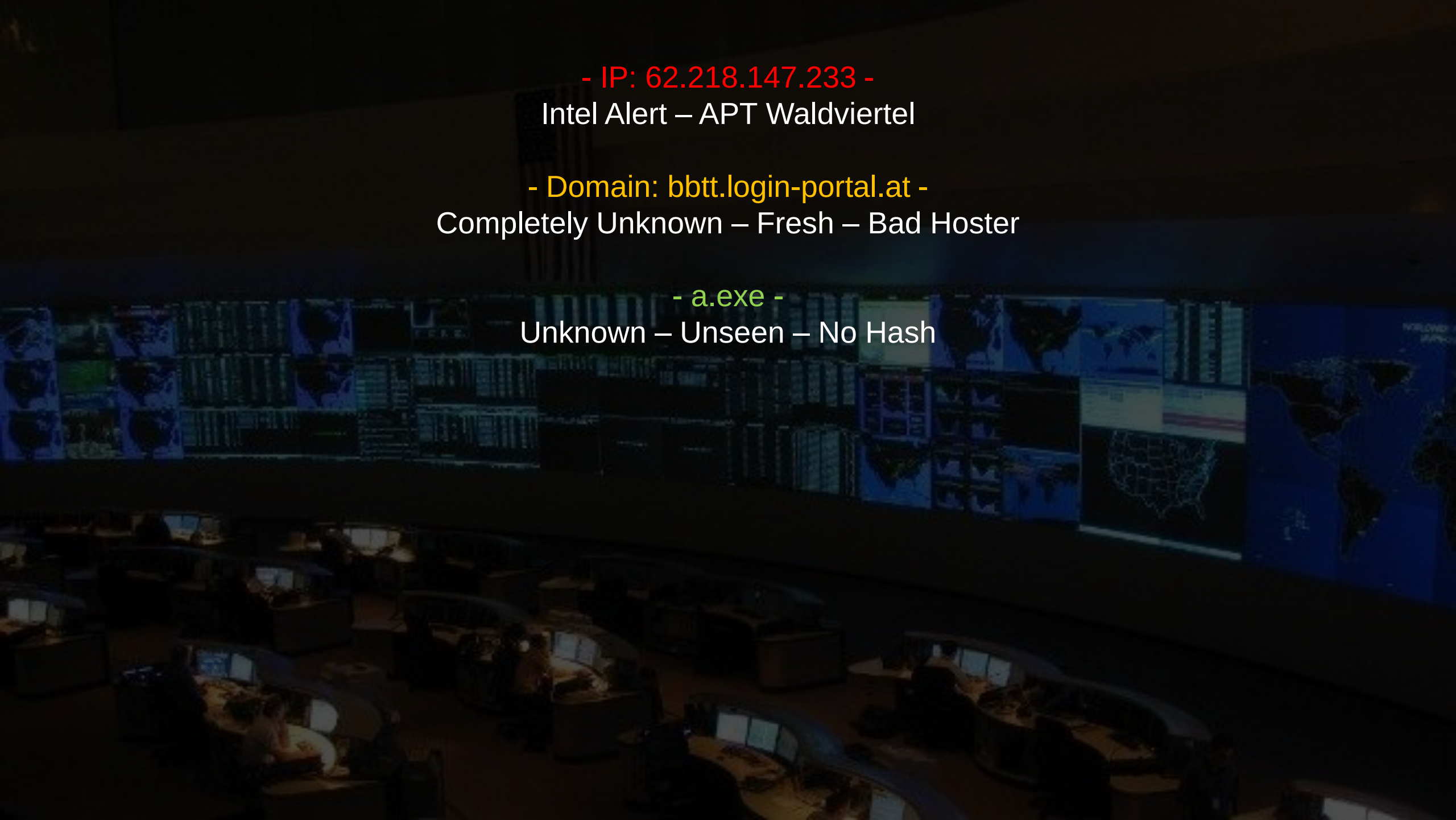
EDR Alert – Microsoft Word Updater.exe

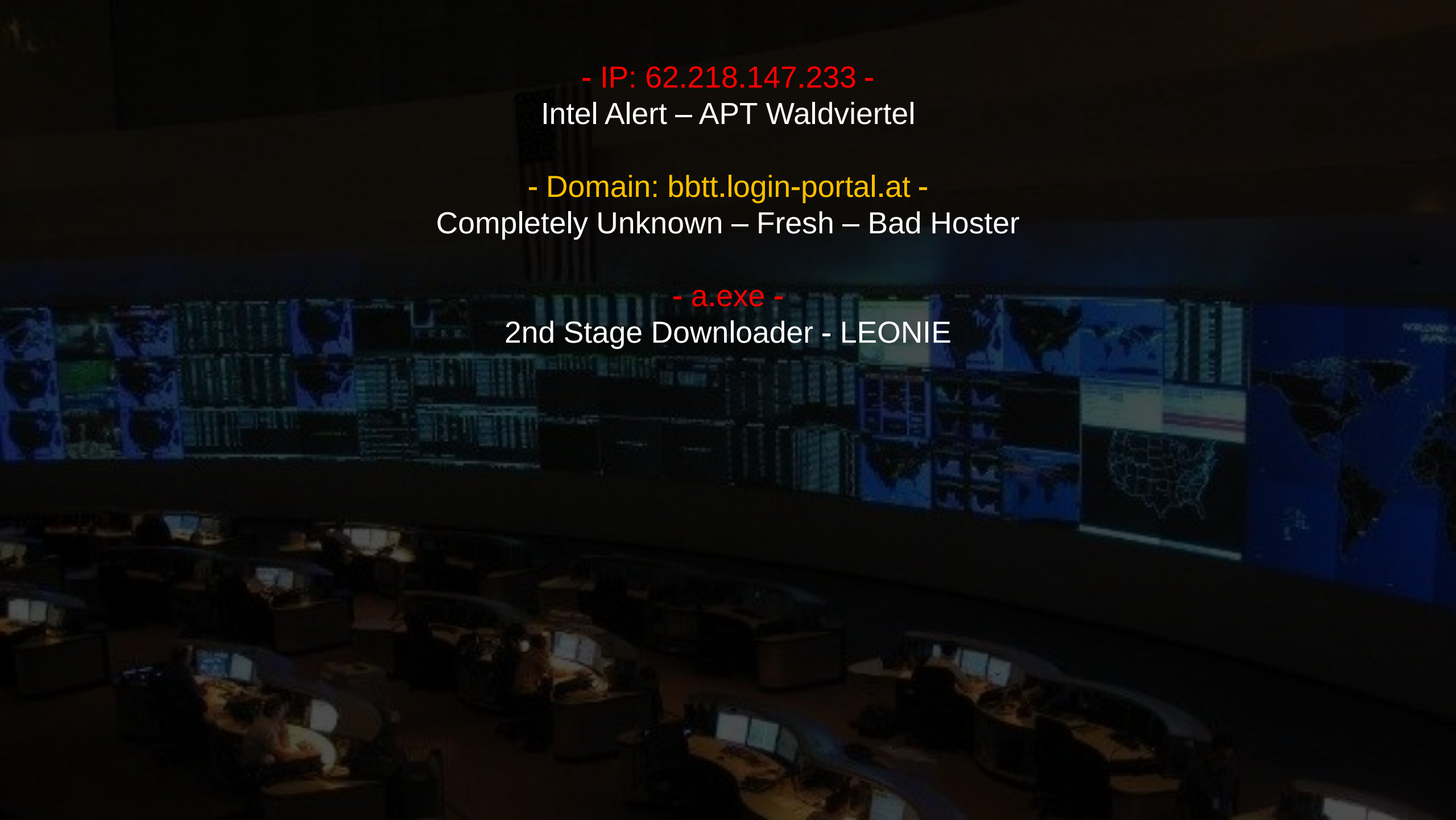
kapsch >>> challenging limits

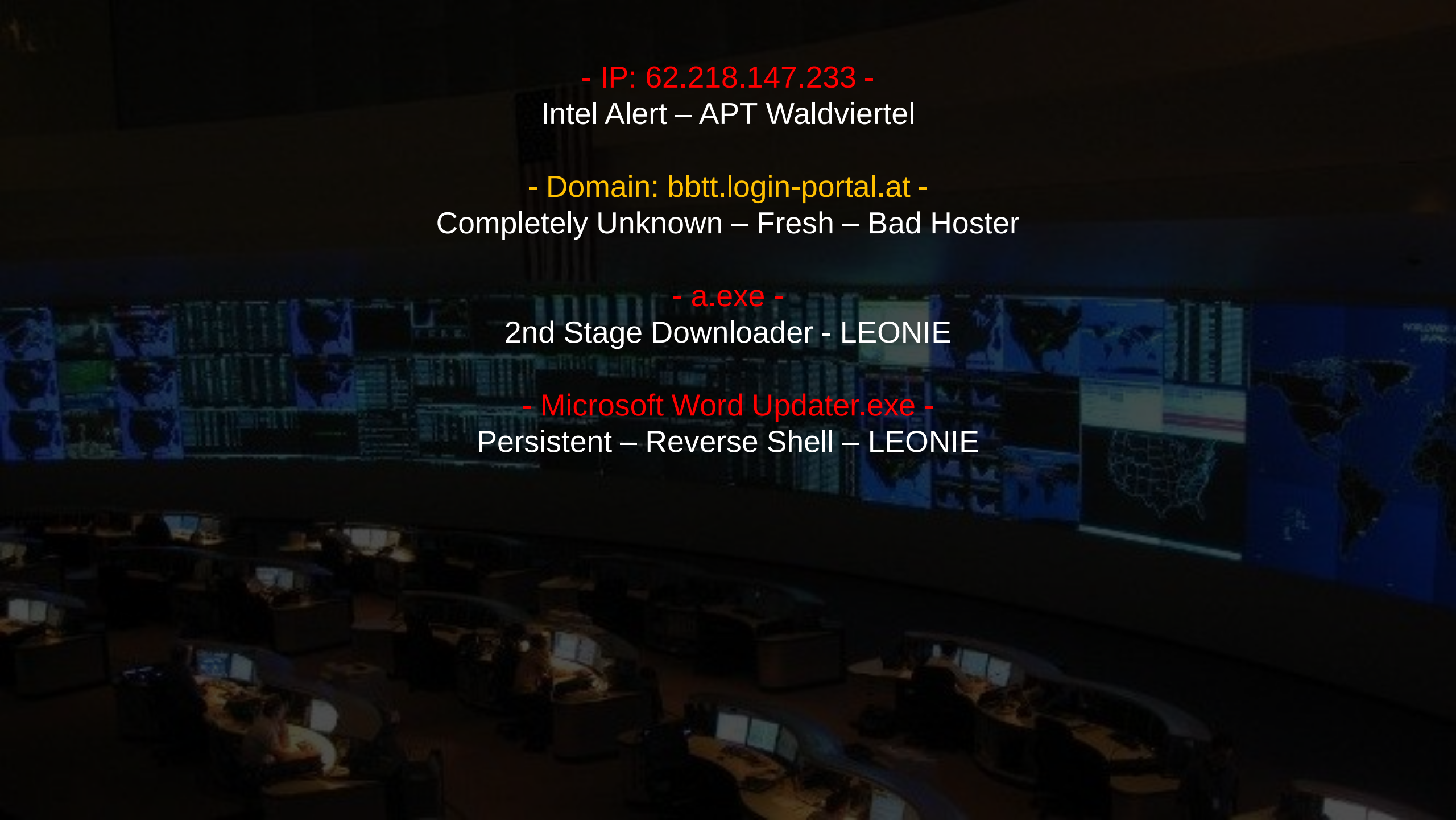
7 Processes

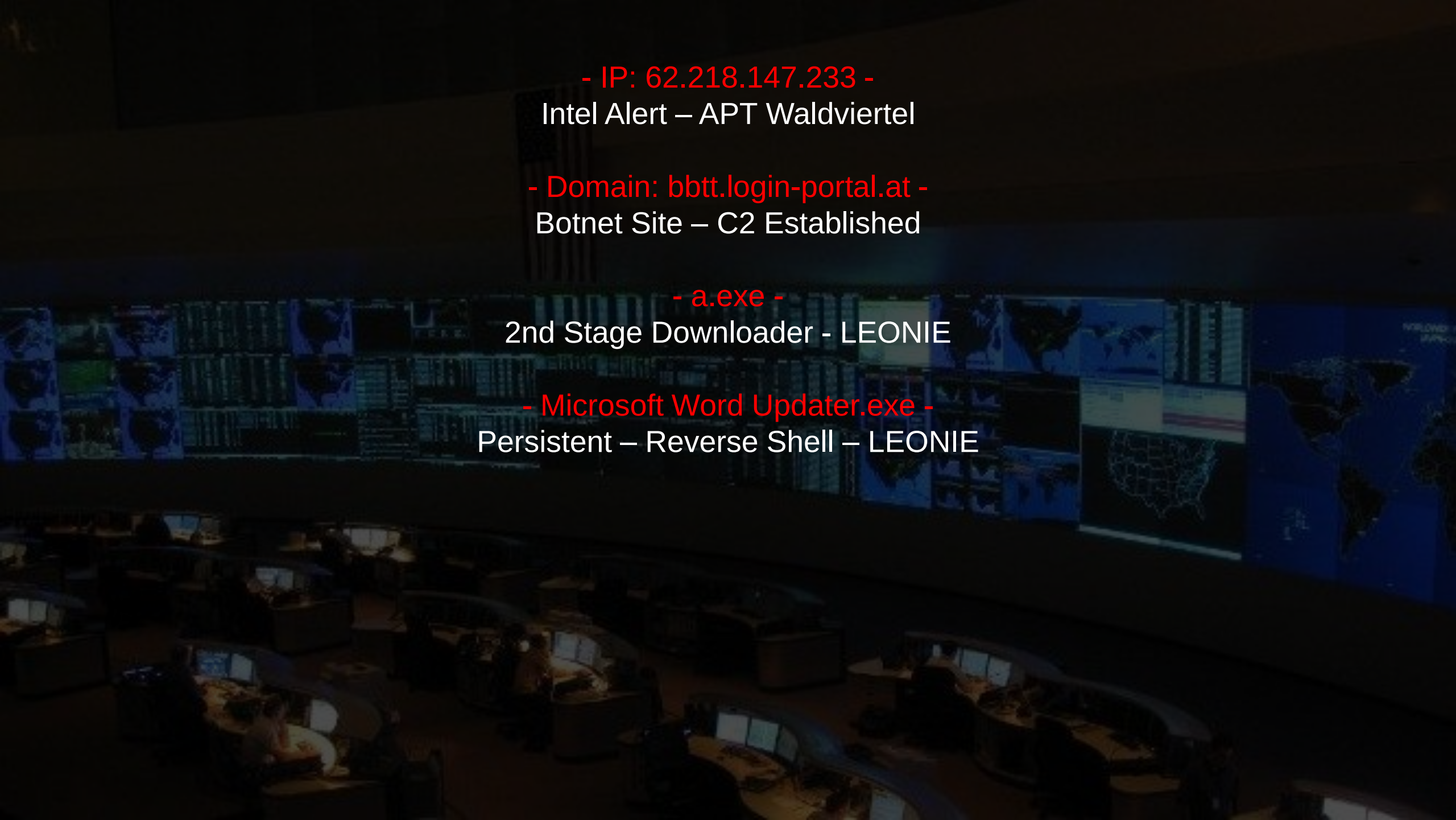
From 2018-02-17 10:46:46.265Z to 2018-02-28 13:03:00.303Z

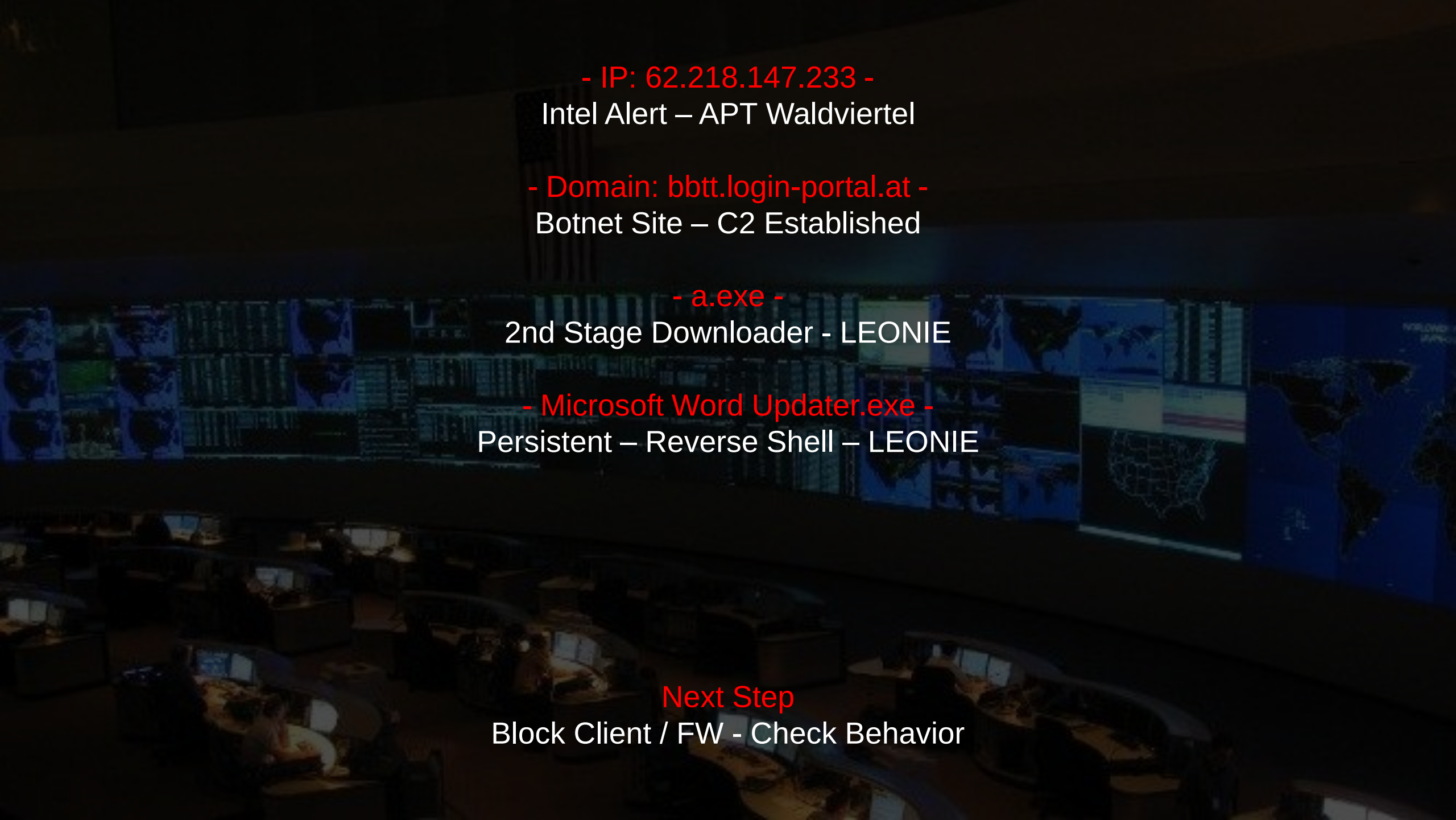
PID	Path
4240	C:\Windows\system32\conhost.exe
4220	csc.exe
5428	csc.exe
5924	ipconfig.exe
5720	systeminfo.exe
5124	tasklist.exe
5636	whoami.exe


- IP: 62.218.147.233 -
Intel Alert – APT Waldviertel
- Domain: bbtt.login-portal.at -
Completely Unknown – Fresh – Bad Hoster
- a.exe -
Unknown – Unseen – No Hash


- IP: 62.218.147.233 -
Intel Alert – APT Waldviertel
- Domain: bbtt.login-portal.at -
Completely Unknown – Fresh – Bad Hoster
- a.exe -
2nd Stage Downloader - LEONIE


- IP: 62.218.147.233 -
Intel Alert – APT Waldviertel
- Domain: bbtt.login-portal.at -
Completely Unknown – Fresh – Bad Hoster
- a.exe -
2nd Stage Downloader - LEONIE
- Microsoft Word Updater.exe -
Persistent – Reverse Shell – LEONIE


- IP: 62.218.147.233 -
Intel Alert – APT Waldviertel
- Domain: bbtt.login-portal.at -
Botnet Site – C2 Established
- a.exe -
2nd Stage Downloader - LEONIE
- Microsoft Word Updater.exe -
Persistent – Reverse Shell – LEONIE



- IP: 62.218.147.233 -

Intel Alert – APT Waldviertel

- Domain: bbtt.login-portal.at -

Botnet Site – C2 Established

- a.exe -

2nd Stage Downloader - LEONIE

- Microsoft Word Updater.exe -

Persistent – Reverse Shell – LEONIE

Next Step

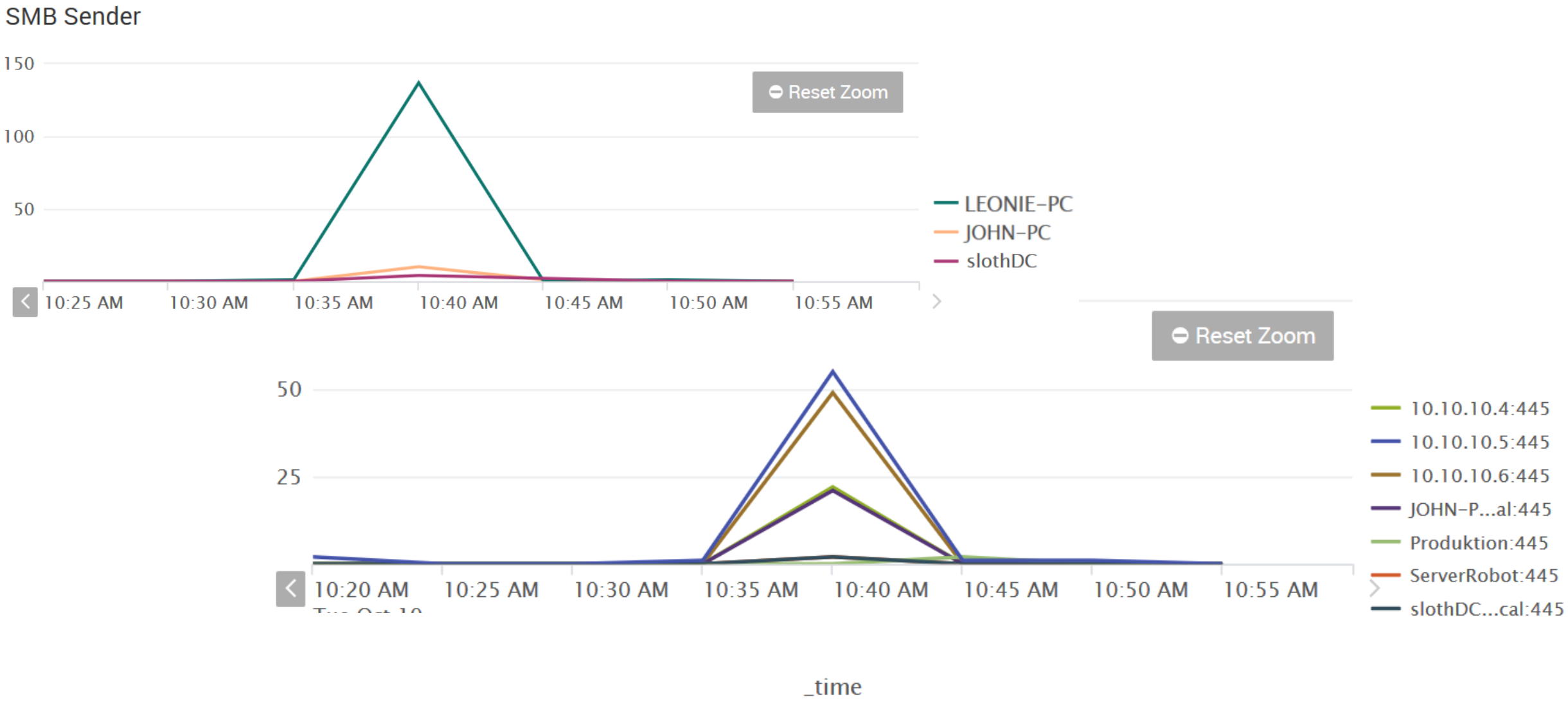
Block Client / FW - Check Behavior

Splunk - Logging Active Directory Alerts

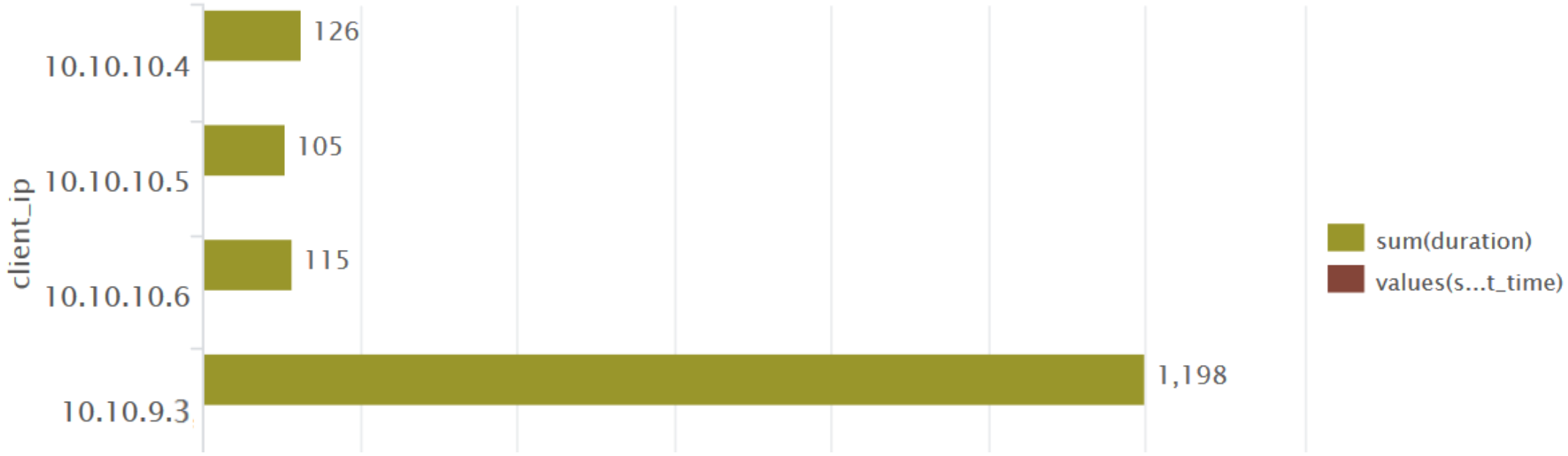
kapsch >>> challenging limits

Error_Code	count	Description
0xC0000064	29110	user name does not exist
0xC0000234	1697	user is currently locked out
0xC0000071	1443	expired password

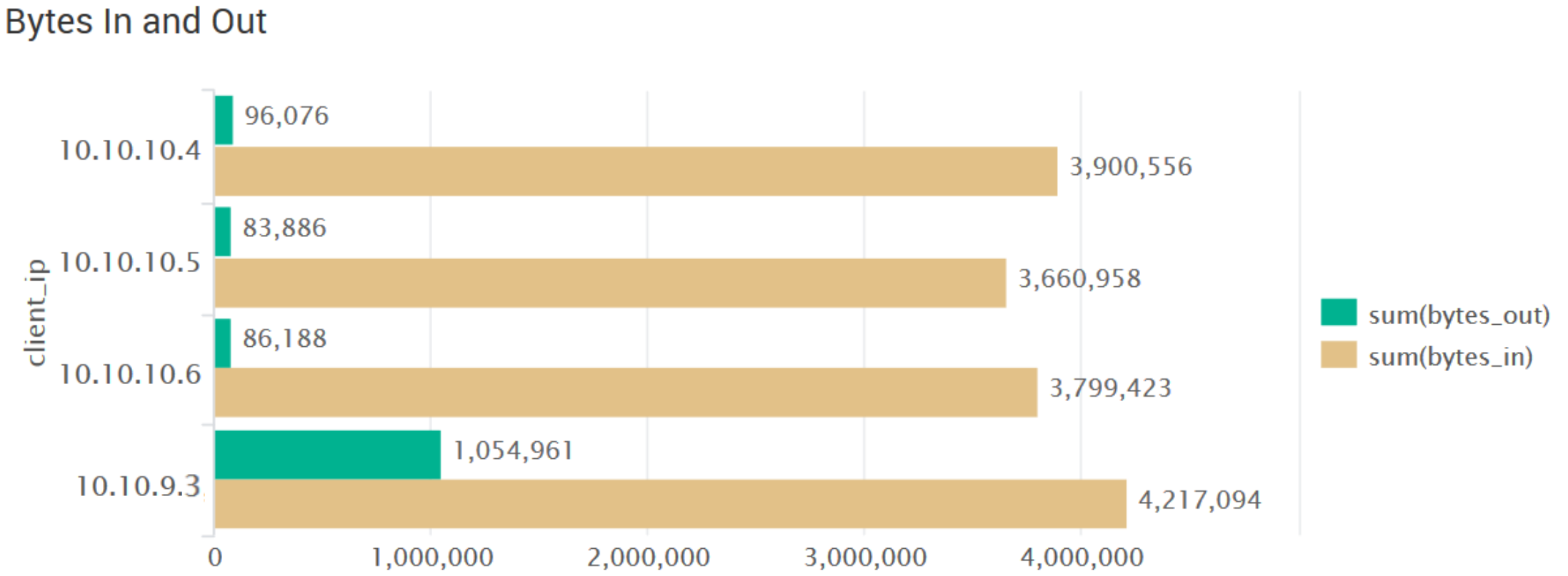
Splunk - Logging Internal Network Behavior

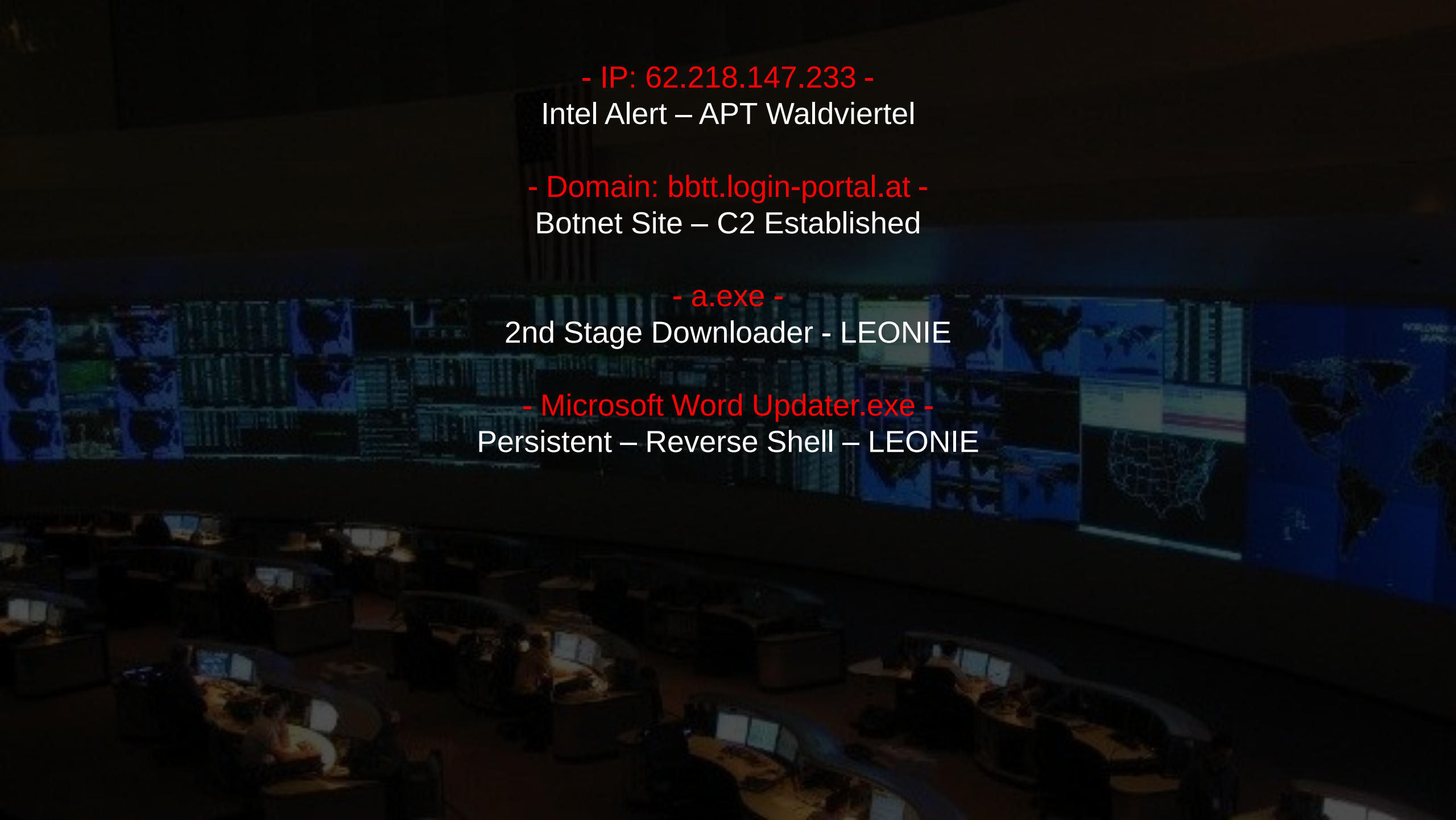


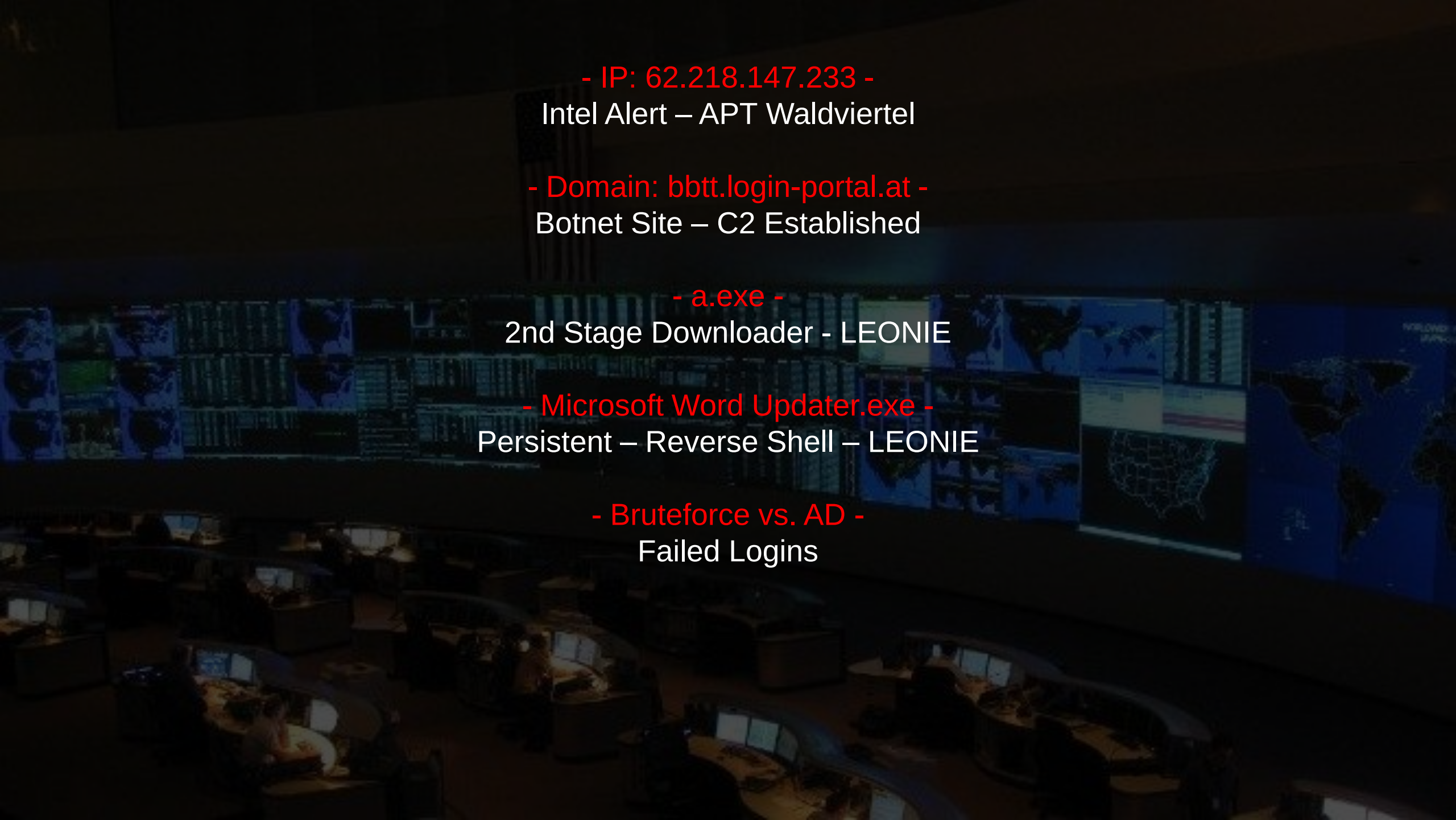
Splunk - Logging Rev. Shell Indikator (Time)

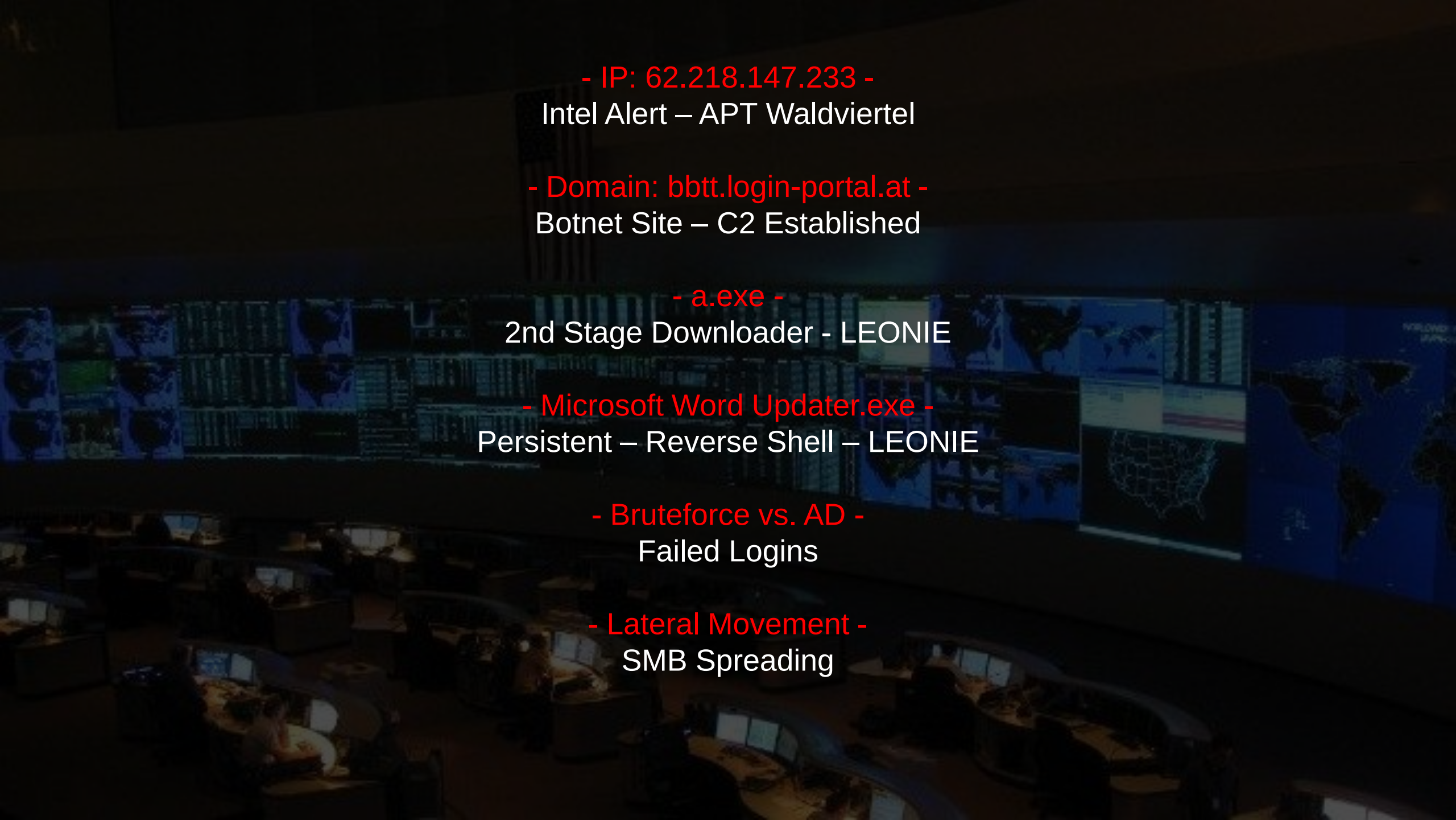


Splunk - Logging Rev. Shell Indikator (Bytes)




- IP: 62.218.147.233 -
Intel Alert – APT Waldviertel
- Domain: bbtt.login-portal.at -
Botnet Site – C2 Established
- a.exe -
2nd Stage Downloader - LEONIE
- Microsoft Word Updater.exe -
Persistent – Reverse Shell – LEONIE


- IP: 62.218.147.233 -
Intel Alert – APT Waldviertel
- Domain: bbtt.login-portal.at -
Botnet Site – C2 Established
- a.exe -
2nd Stage Downloader - LEONIE
- Microsoft Word Updater.exe -
Persistent – Reverse Shell – LEONIE
- Bruteforce vs. AD -
Failed Logins


- IP: 62.218.147.233 -
Intel Alert – APT Waldviertel
- Domain: bbtt.login-portal.at -
Botnet Site – C2 Established
- a.exe -
2nd Stage Downloader - LEONIE
- Microsoft Word Updater.exe -
Persistent – Reverse Shell – LEONIE
- Bruteforce vs. AD -
Failed Logins
- Lateral Movement -
SMB Spreading


WE ARE
HIRING!
Kapsch Cyber Defense Center
cdc@kapsch[.]net

Questions?

Timo Jobst
Head of Cyber Defense Center

Kapsch BusinessCom

Kapsch BusinessCom
Wienerbergstrasse 53
1120 Wien, Österreich
Phone: +43 50 811 5791
E-Mail: timo.jobst@kapsch.net
www.kapsch.net