31ST ANNUAL FIRST CONFERENCE

EDINBURGH
JUNE 16-21
2019

ATT&CKing the Castle

Chip Greene

Conrad Layne

Introductions

Chip Greene

Director, Cyber Security GE CIRT
ICS SecOps, Operational Readiness
Veterans Network Lead

MS Disaster Science
Alumni Board of Directors

BS Information Systems
Cyber Security Advisory Board

USS Richard E. Byrd DDG-23
NAVSTA Norfolk Brig

Conrad Layne

Senior Cyber Intelligence Analyst,
ATT&CK Czar

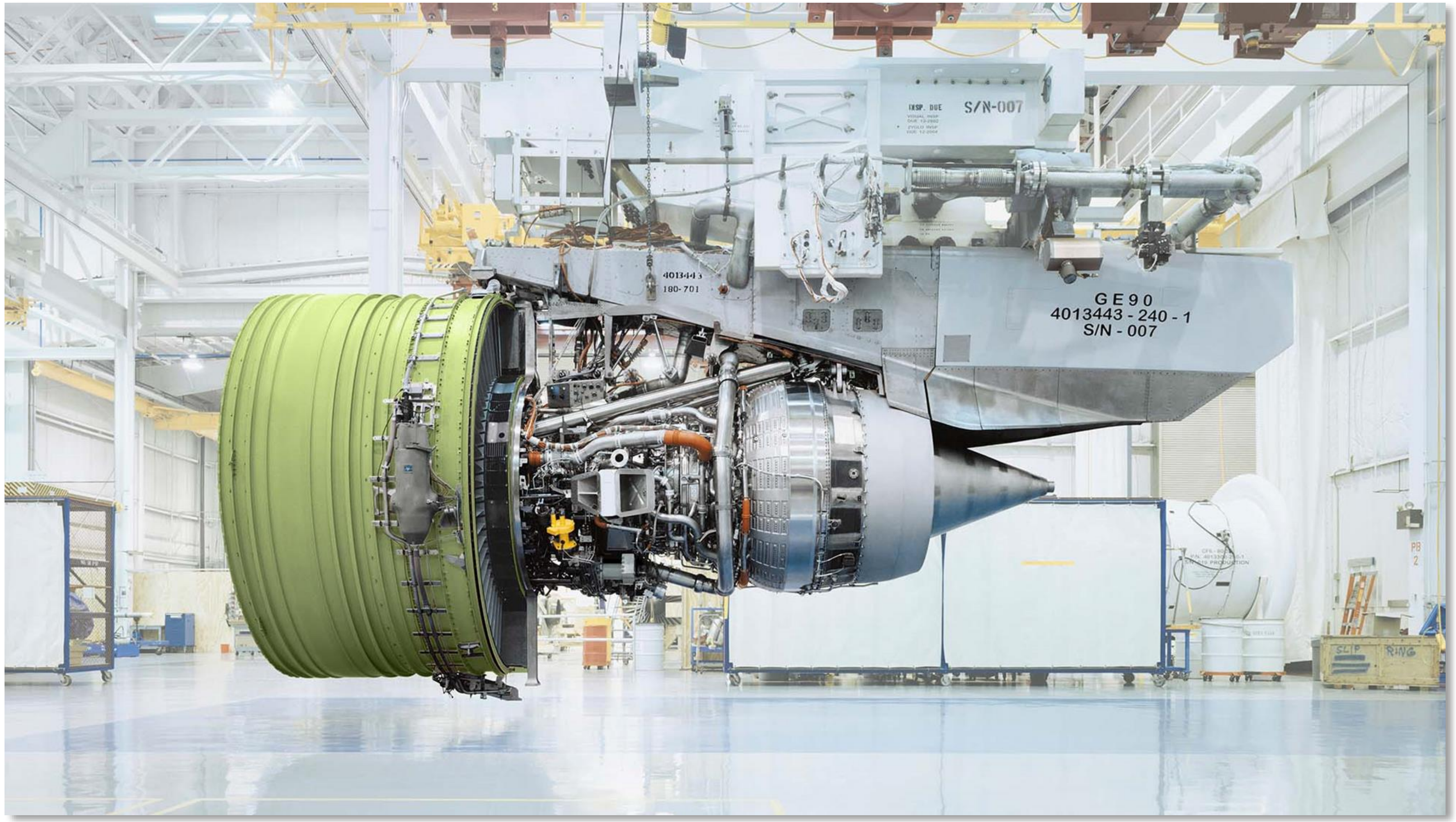
MS Cyber-security Intelligence

BS Digital Forensic Science

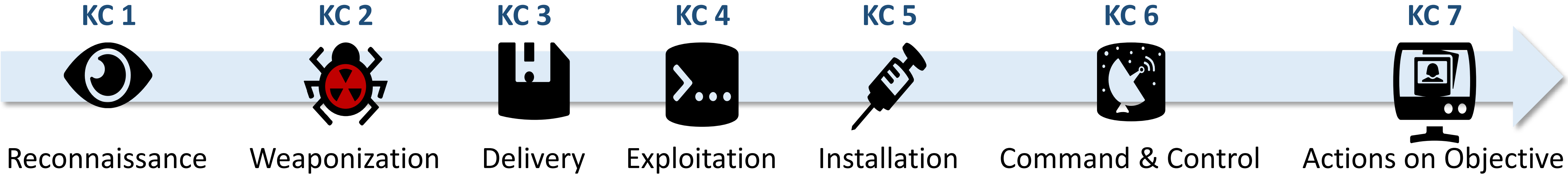
Discussion topics

- Frameworks (Kill Chain, Pyramid of Pain, Mitre ATT&CK™, TIAMAT)
- Extracting ICS indicators for behavioral detection
- Scenarios developed from ATT&CK™ behaviors
- Detection & confidence
- Q&A

Frameworks



Lockheed Martin Kill Chain™



KC 1 Reconnaissance

KC 2 Weaponization

KC 3 Delivery

KC 4 Exploitation

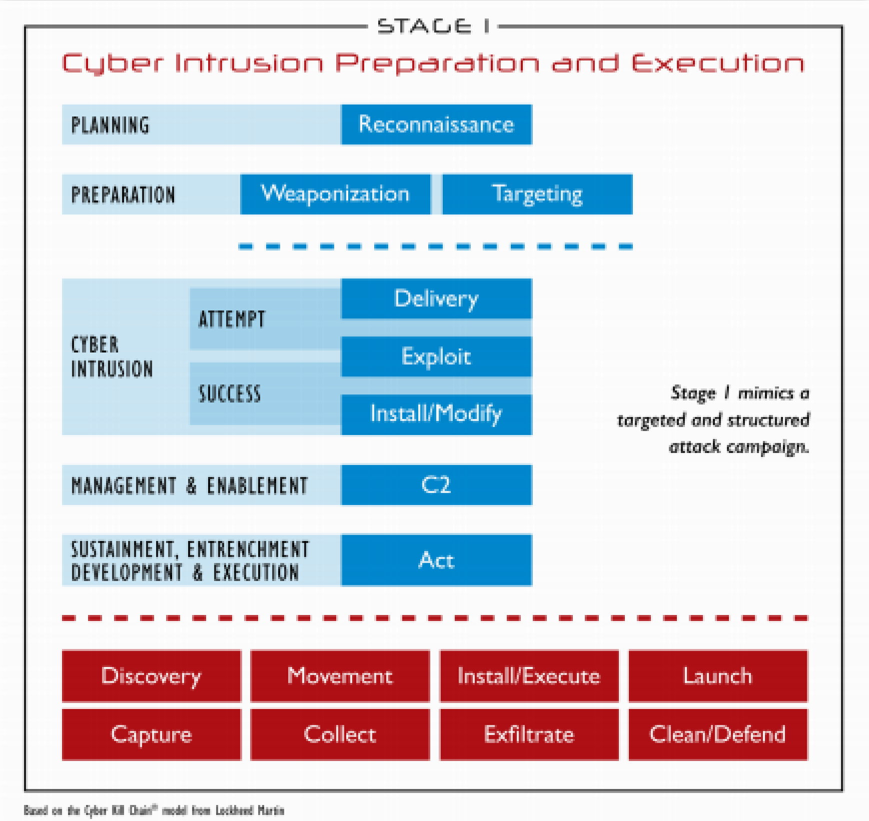
KC 5 Installation

KC 6 Command & Control

KC 7 Actions on Objective

(Reference 1,2)

SANS ICS Kill Chain™



STAGE 1

Cyber Intrusion Preparation and Execution

PLANNING
Reconnaissance

PREPARATION
Weaponization
Targeting

CYBER INTRUSION
ATTEMPT
Delivery
Exploit
SUCCESS
Install/Modify

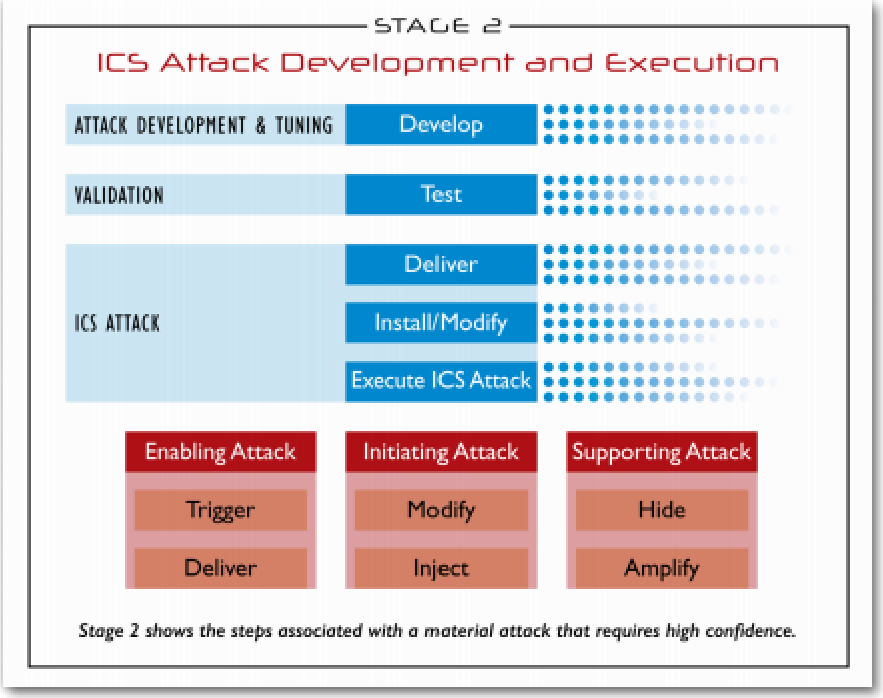
MANAGEMENT & ENABLEMENT
C2

SUSTAINMENT, ENTRENCHMENT DEVELOPMENT & EXECUTION
Act

Discovery
Movement
Install/Execute
Launch
Capture
Collect
Exfiltrate
Clean/Defend

Stage 1 mimics a targeted and structured attack campaign.

Based on the Cyber Kill Chain® model from Lockheed Martin



STAGE 2

ICS Attack Development and Execution

ATTACK DEVELOPMENT & TUNING
Develop

VALIDATION
Test

ICS ATTACK
Deliver
Install/Modify
Execute ICS Attack

Enabling Attack
Trigger
Deliver

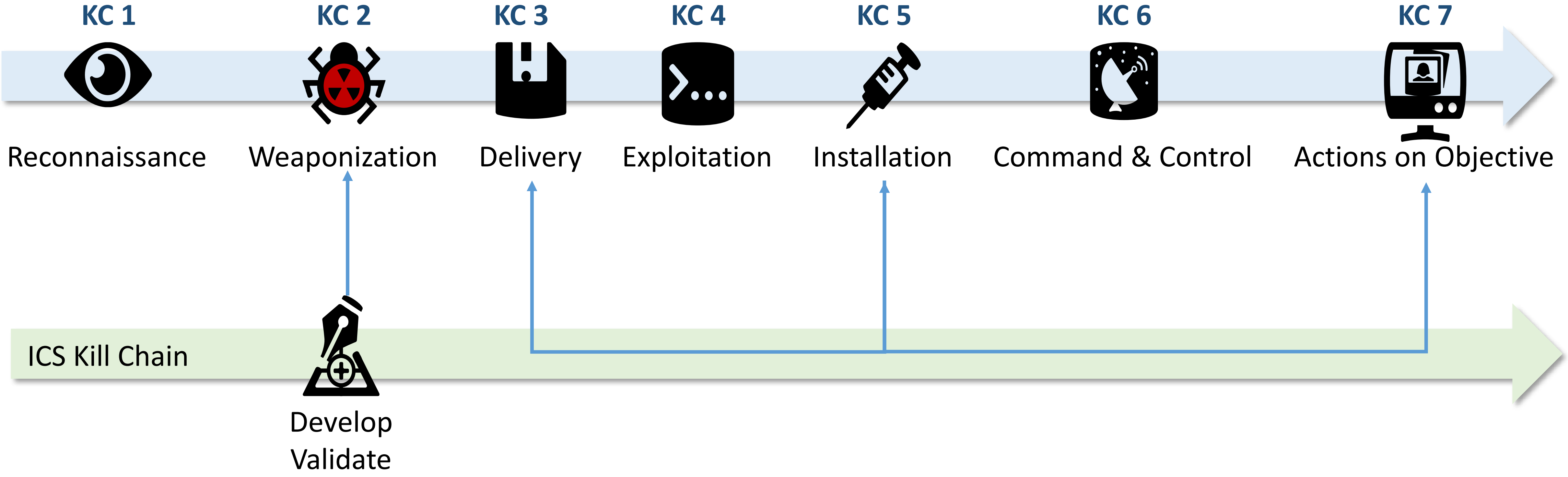
Initiating Attack
Modify
Inject

Supporting Attack
Hide
Amplify

Stage 2 shows the steps associated with a material attack that requires high confidence.

(Reference 1,2)

Kill Chain integration



KC 1 Reconnaissance

KC 2 Weaponization

KC 3 Delivery

KC 4 Exploitation

KC 5 Installation

KC 6 Command & Control

KC 7 Actions on Objective

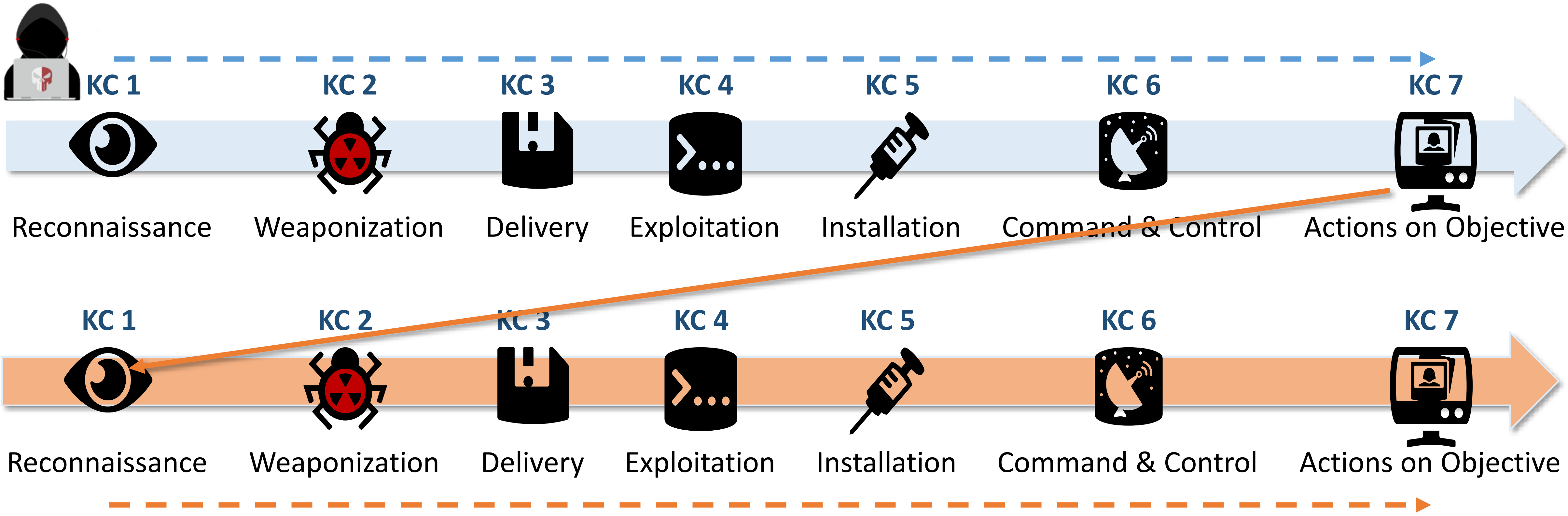
ICS Kill Chain

Develop
Validate

(Reference 1,2)

Lockheed Martin Kill Chain^{TM}

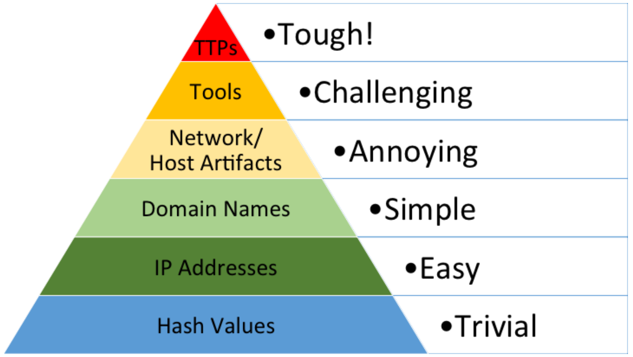
Multi-Environment

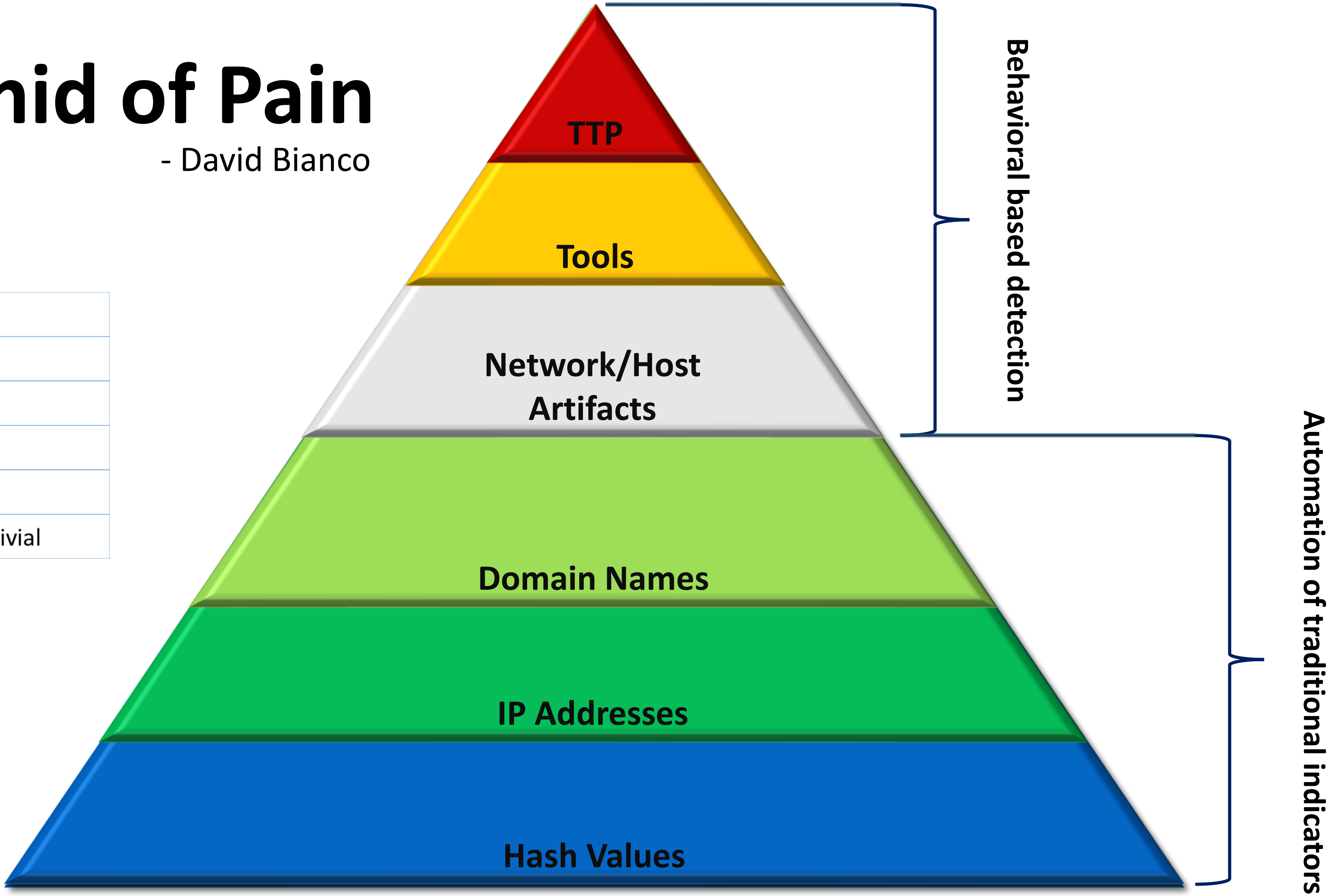


(Reference 1,2)

The Pyramid of Pain

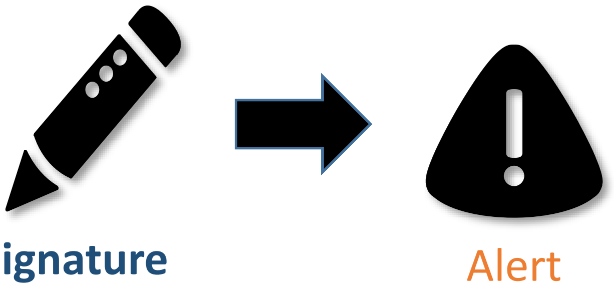
- David Bianco





(Reference 5)

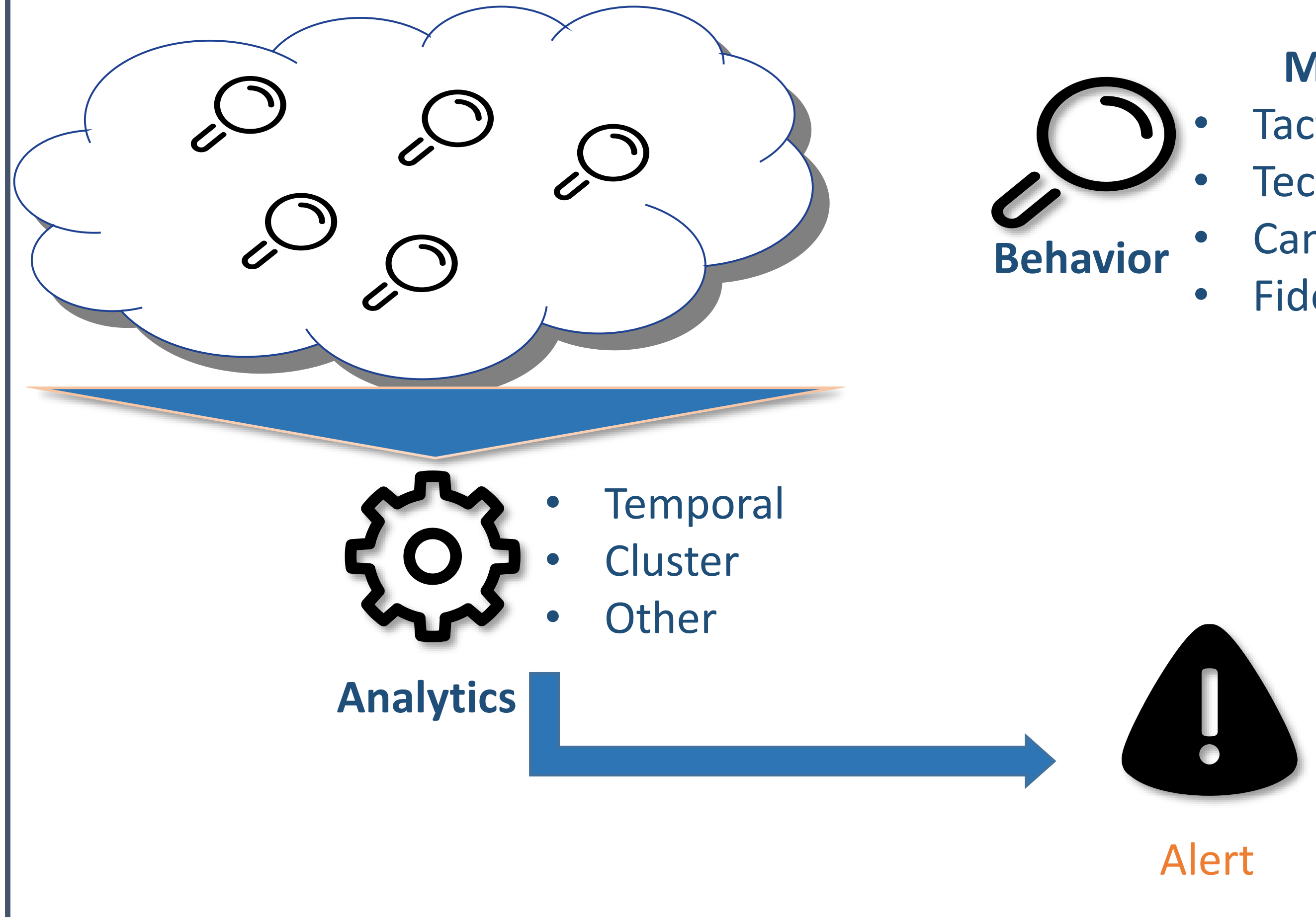
Leveraging behaviors



Signature

Alert

- Critical
- High
- Medium
- Low



Behavior

Meta

- Tactic
- Technique
- Campaign
- Fidelity

Analytics

- Temporal
- Cluster
- Other

Alert

- Critical
- High
- Medium
- Low

Detection Strategies

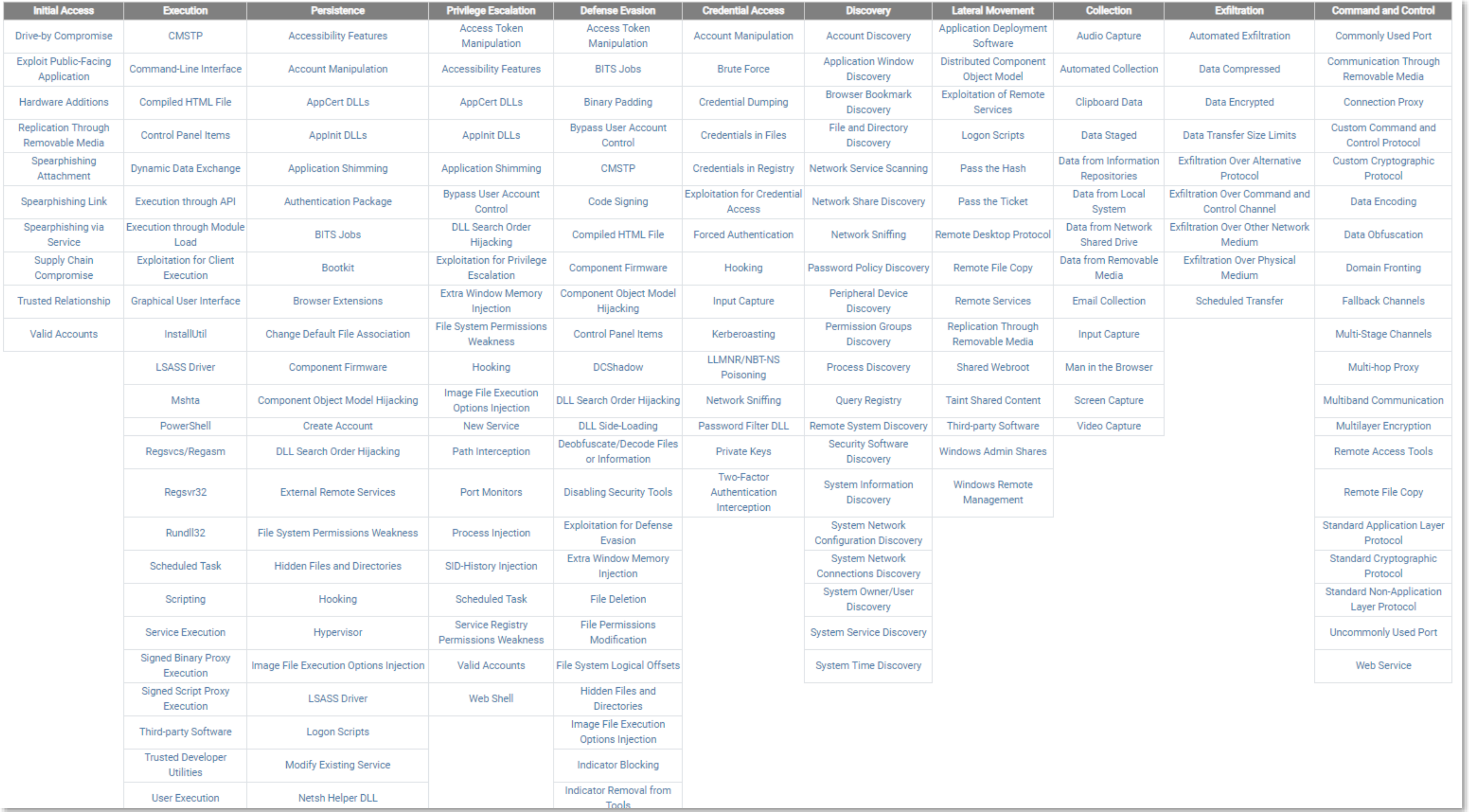
- Atomic Indicators of Compromise-based

- Static
  - Signatures are specific for one indicator
  - Does not apply for other samples across the same malware family or actor
  - Quick deployment
  - Analyst fatigue
  - Loses fidelity over time

- Behavior-based

- Dynamic
  - Signatures are indicator independent
  - Focuses on observable malicious actions
  - Detects across multiple malware families, and across Cybercrime and APT actors
  - Fidelity over longer time

ATT&CK™ Framework



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

(Reference 3)

Mitre ICS ATT&CK™

Persistence	Privilege Escalation	Defense Evasion	Operator Evasion	Credential Access	Discovery	Lateral Movement	Execution	Command and Control	Compromise Integrity	Physical Impact
External Remote Services	Exploitation for Privilege Escalation	Alternate Modes of Operation	Block Reporting Message	Brute Force	Control Device Discovery	Default Credentials	Alternate Modes of Operation	Commonly Used Port	Alternate Modes of Operation	Block Command Message
Modify Control Logic	Valid Accounts	Exploitation for Defense Evasion	Block Serial Comm Port	Credential Dumping	Control Process	External Remote Services	Command-Line Interface	Connection Proxy	Block Serial Comm Port	Block Reporting Message
Module Firmware		File Deletion	Modify Control Logic	Default Credentials	I/O Module Enumeration	Modify Control Logic	Execution through API		Device Shutdown	DoS Service
System Firmware		Masquerading	Modify HMI/Historian Reporting	Network Sniffing	Location Identification	Valid Accounts	Graphical User Interface		DoS Service	Exploitation for Denial of Service
Valid Accounts		Modify Event Log	Modify I/O Image		Network Connection Enumeration		Man in the Middle		Modify Control Logic	Masquerading
		Modify System Settings	Modify Parameter		Network Service Scanning		Modify Control Logic		System Firmware	Modify Command Message
		Rootkit	Modify Physical Device Display		Network Sniffing		Modify System Settings			Modify Control Logic
			Modify Reporting Message		Remote System Discovery		Scripting			Modify Parameter
			Modify Reporting Settings		Role Identification					Modify Reporting Settings
			Modify Tag		Serial Connection Enumeration					Modify Tag
			Rootkit							Module Firmware
			Spoof Reporting Message							Spoof Command Message
										Spoof Reporting Message

Operator Evasion

How can we fool the operator into thinking everything is OK

How can we fool the operator to take the wrong action

Compromise Integrity

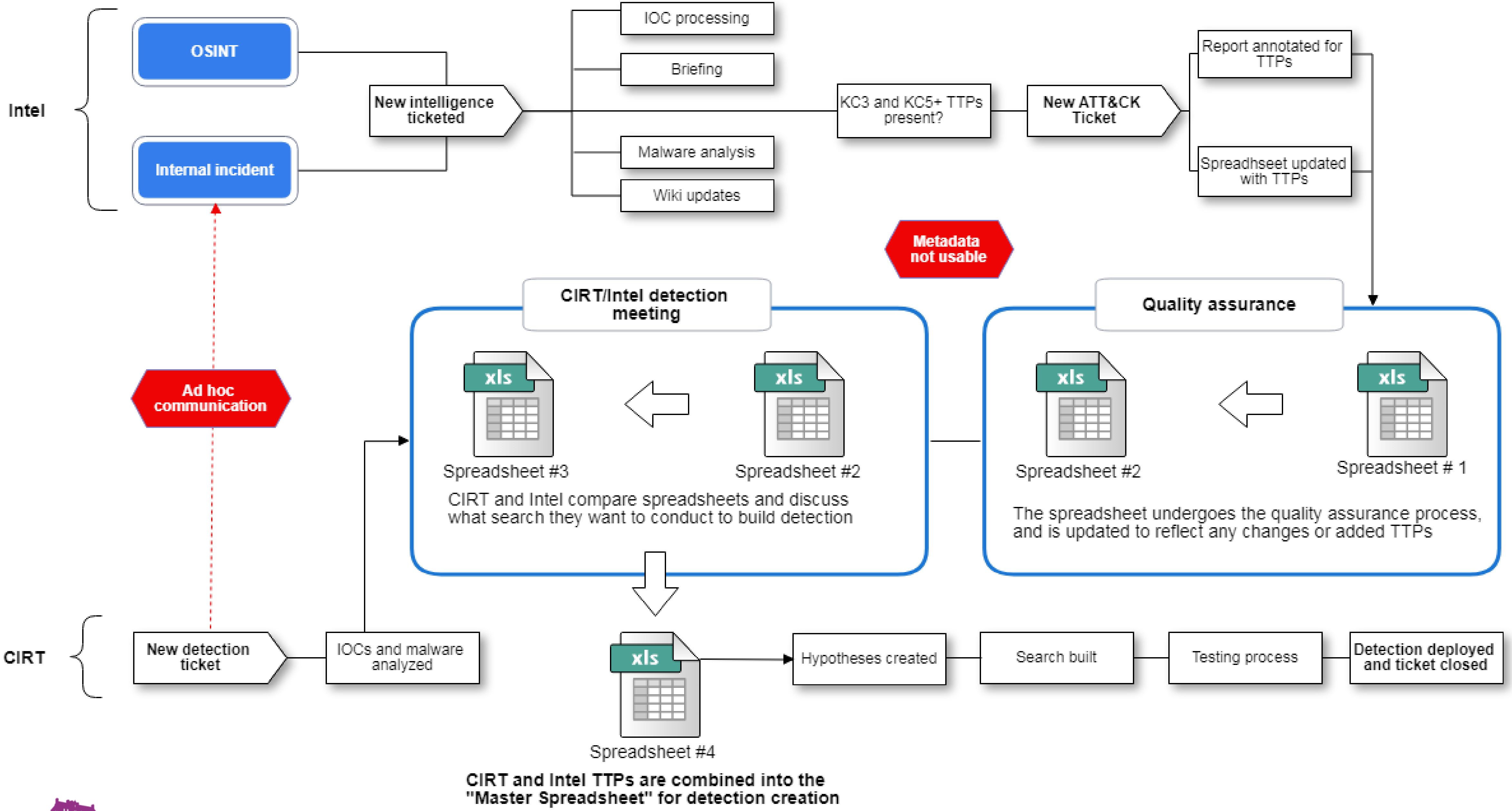
How can we make changes to cause future physical impacts

Physical Impact

How can we stop/degrade the process

How can we cause catastrophic failure

(Reference 4)



Intel

OSINT

Internal incident

New intelligence ticketed

IOC processing

Briefing

Malware analysis

Wiki updates

KC3 and KC5+ TTPs present?

New ATT&CK Ticket

Report annotated for TTPs

Spreadhseet updated with TTPs

Metadata not usable

Ad hoc communication

CIRT/Intel detection meeting

Spreadsheet #3

Spreadsheet #2

CIRT and Intel compare spreadsheets and discuss what search they want to conduct to build detection

Quality assurance

Spreadsheet #2

Spreadsheet # 1

The spreadsheet undergoes the quality assurance process, and is updated to reflect any changes or added TTPs

CIRT

New detection ticket

IOCs and malware analyzed

Spreadsheet #4

Hypotheses created

Search built

Testing process

Detection deployed and ticket closed

CIRT and Intel TTPs are combined into the "Master Spreadsheet" for detection creation

TIAMAT

Supremely strong and powerful 5-headed draconic goddess

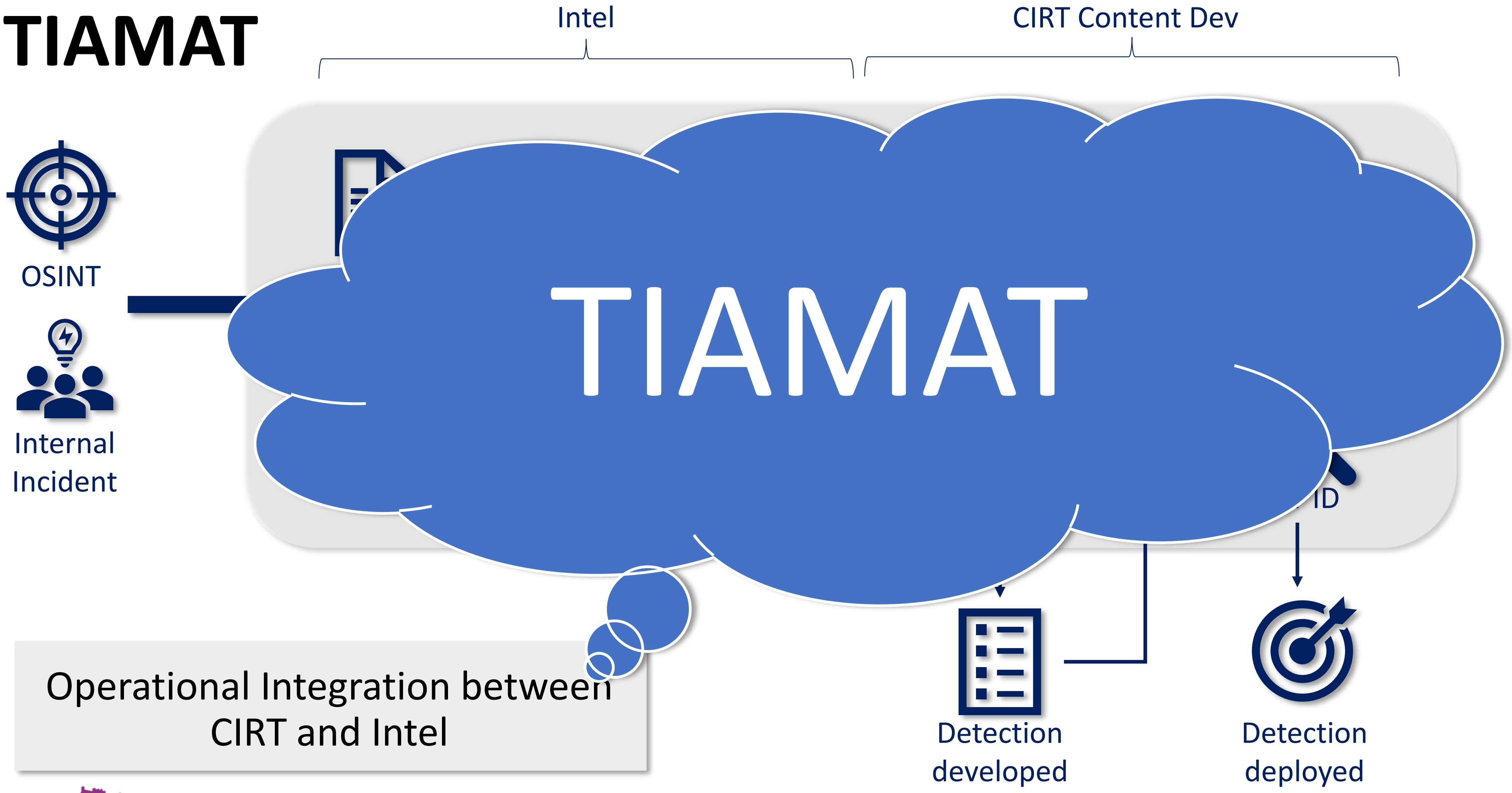
A goddess in ancient Mesopotamian mythology.

Queen and mother of evil dragons

Named as one of the greatest villains in D&D history in Dragon #359, the magazine's final print issue.

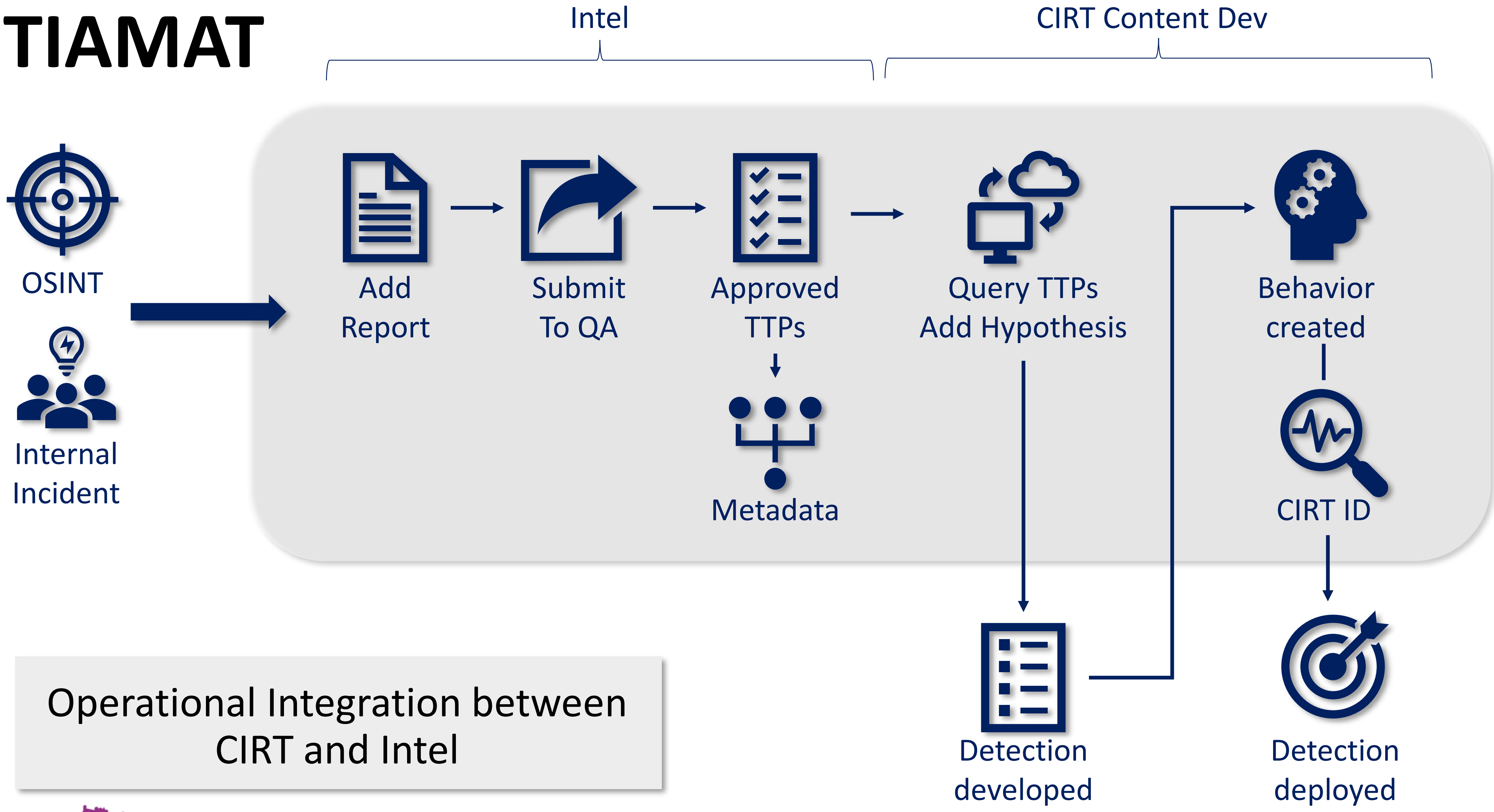
(Reference 6)

TIAMAT



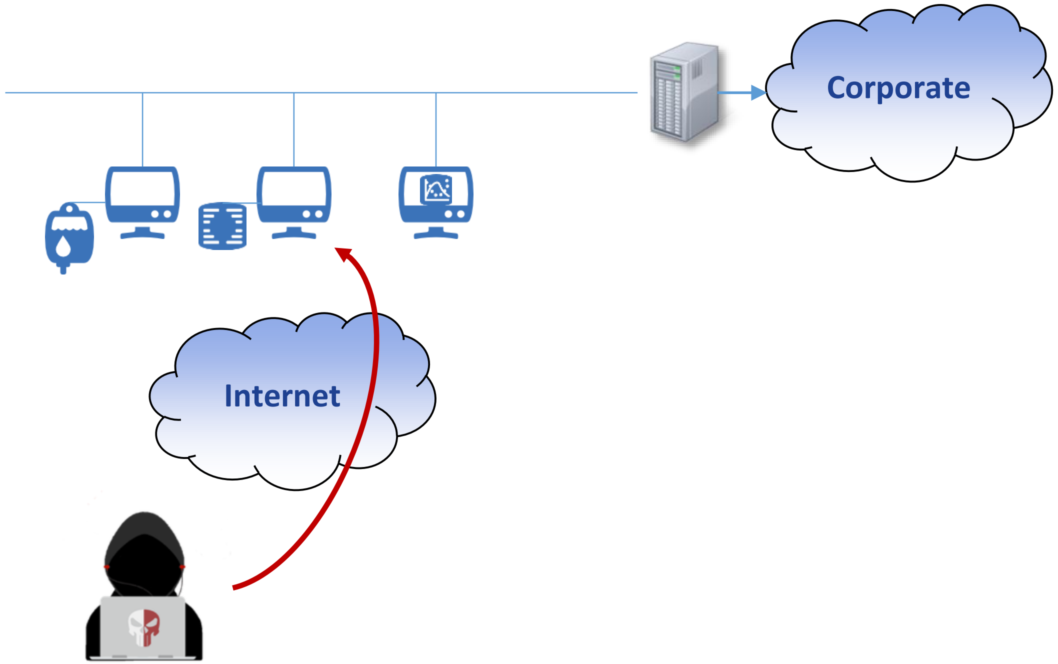
Operational Integration between CIRT and Intel

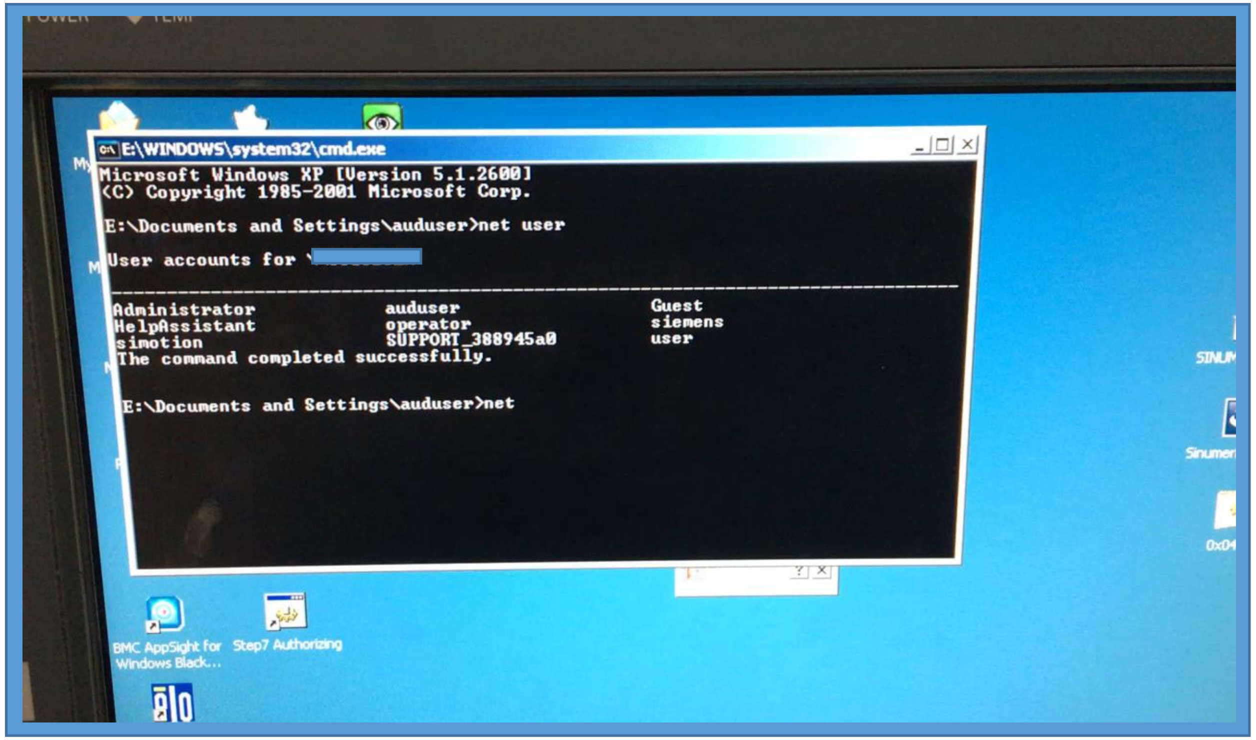
TIAMAT



Operational Integration between CIRT and Intel

Multi-Stage Kill Chain




E:\WINDOWS\system32\cmd.exe
BMC AppSight for Windows Black...
Step7 Authorizing

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\auduser>net user

User accounts for \[redacted]

-------------------------------------------------------------------------------
Administrator            auduser                  Guest
HelpAssistant            operator                 siemens
simotion                 SUPPORT_388945a0         user
The command completed successfully.


E:\Documents and Settings\auduser>net
```

We must focus on the behaviors in the environment

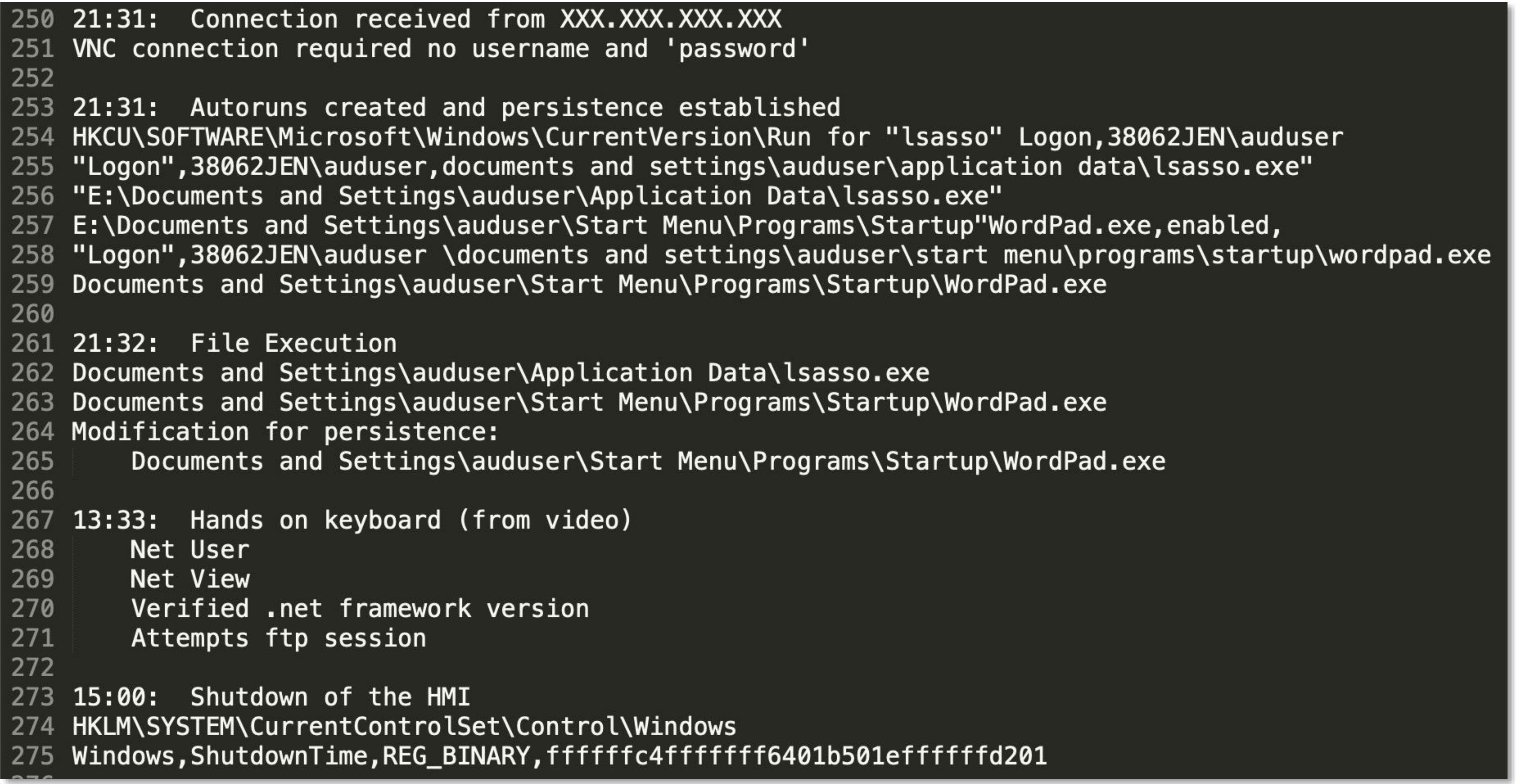
Indicators & Scenarios

Extracting ICS indicators

Behavioral detection from internal incidents

- Establish a timeline of events with brief narrative
- Perform root cause analysis
- Align significant events to the Lockheed martin cyber kill chain
- Map the events to the appropriate tactic and technique
- Document the kill chain levels, tactics and techniques
- Evaluate detection opportunities

Extracting ICS indicators *key events*



```
21:31:  Connection received from XXX.XXX.XXX.XXX
VNC connection required no username and 'password'

21:31:  Autoruns created and persistence established
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run for "lsasso" Logon,38062JEN\auduser
"Logon",38062JEN\auduser,documents and settings\auduser\application data\lsasso.exe"
"E:\Documents and Settings\auduser\Application Data\lsasso.exe"
E:\Documents and Settings\auduser\Start Menu\Programs\Startup"WordPad.exe,enabled,
"Logon",38062JEN\auduser \documents and settings\auduser\start menu\programs\startup\wordpad.exe
Documents and Settings\auduser\Start Menu\Programs\Startup\WordPad.exe

21:32:  File Execution
Documents and Settings\auduser\Application Data\lsasso.exe
Documents and Settings\auduser\Start Menu\Programs\Startup\WordPad.exe
Modification for persistence:
    Documents and Settings\auduser\Start Menu\Programs\Startup\WordPad.exe

13:33:  Hands on keyboard (from video)
    Net User
    Net View
    Verified .net framework version
    Attempts ftp session

15:00:  Shutdown of the HMI
HKLM\SYSTEM\CurrentControlSet\Control\Windows
Windows,ShutdownTime,REG_BINARY,ffffffc4fffffff6401b501effffffd201
```

Mapping key events to the ATT&CK Framework

Initial Connection

Cyber Kill Chain Level	ICS-ATT&CK Tactic	ICS-ATT&CK Technique
KC6	Discovery	Control Device Discovery
KC6	Credential Access	Default Credentials
Cyber Kill Chain Level	**Enterprise-ATT&CK Tactic**	**Enterprise-ATT&CK Technique**
KC3	Initial Access	Trusted Relationship

Actor: Unknown

Tools: N/A

Execution Notes: IPv4: `xxx.xxx.xxx.xxx`

Patterns & Trends: Public facing modem with VNC connection required no username and 'password’

Mapping key events to the ATT&CK Framework

File Execution

Cyber Kill Chain Level	Enterprise-ATT&CK Tactic	Enterprise-ATT&CK Technique
KC5	Execution	Scripting

Actor: Unknown

Tools: lsasso.exe, malicious WordPad.exe

Execution Notes:

```
Documents and Settings\auduser\Application Data\lsasso.exe
Documents and Settings\auduser\Start Menu\Programs\Startup\WordPad.exe
```

Patterns & Trends: lsasso.exe & a malicious version of WordPad.exe launched via script

Mapping key events to the ATT&CK Framework

Establish Persistence

Cyber Kill Chain Level	Enterprise-ATT&CK Tactic	Enterprise-ATT&CK Technique
KC5	Persistence	Registry Run Keys / Startup Folder
KC5	Execution	Scripting

Actor: Unknown

Tools: lsasso.exe, malicious WordPad.exe

Execution Notes: `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run for "lsasso" Logon,38062JEN\auduser  "Logon",38062JEN\auduser,documents and settings\auduser\application data\lsasso.exe” "E:\Documents and Settings\auduser\Application Data\lsasso.exe”`

Patterns & Trends: Autoruns created and persistence established

Mapping key events to the ATT&CK Framework

.NET Framework version checking

Cyber Kill Chain Level	Enterprise-ATT&CK Tactic	Enterprise-ATT&CK Technique
KC6	Discovery	System Information Discovery

Actor: Unknown

Tools: N/A

Execution Notes: N/A

Patterns & Trends: video shows attacker checking the .NET Framework version through the control panel

Mapping key events to the ATT&CK Framework

Hands on Keyboard

Cyber Kill Chain Level	Enterprise-ATT&CK Tactic	Enterprise-ATT&CK Technique
KC6	Discovery	System Owner/User Discovery
KC6	Discovery	Network Share Discovery
Cyber Kill Chain Level	**ICS-ATT&CK Tactic**	**ICS-ATT&CK Technique**
KC5	Execution	Command-line Interface

Actor: Unknown

Tools: N/A

Execution Notes:

```
Net User
Net View
```

Patterns & Trends: video shows attacker running ‘Net’ commands via windows cmd.exe

Mapping key events to the ATT&CK Framework

System Shutdown

Cyber Kill Chain Level	ICS-ATT&CK Tactic	ICS-ATT&CK Technique
KC7	Compromise Integrity	Device Shutdown
KC7	Physical Impact	Denial of Service

Actor: Unknown

Tools: N/A

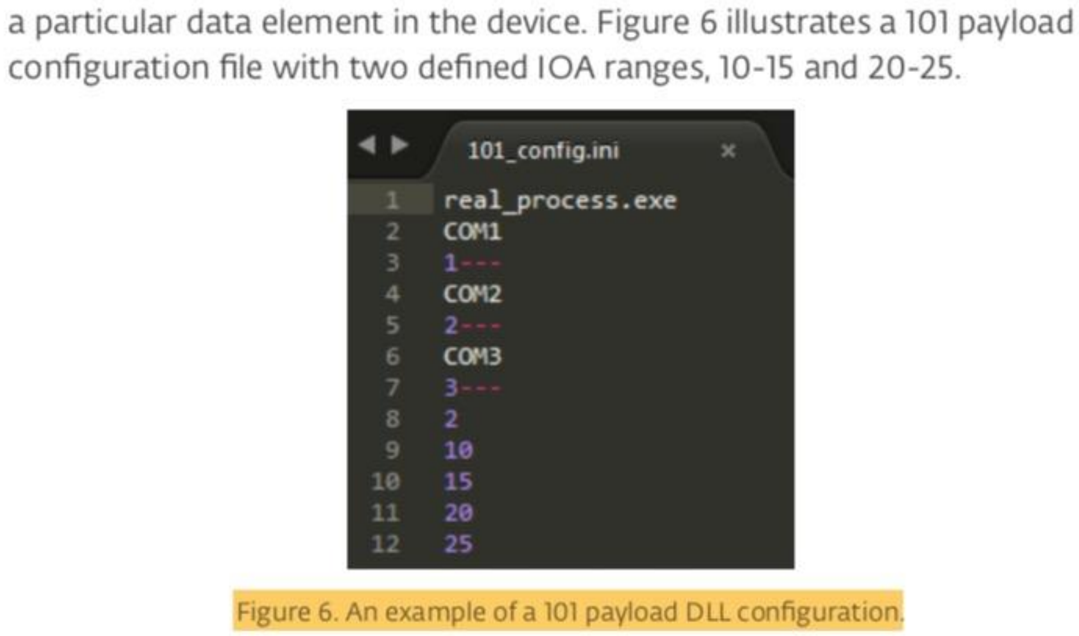
Execution Notes:

```
HKLM\SYSTEM\CurrentControlSet\Control\Windows
Windows,ShutdownTime,REG_BINARY,ffffffc4fffffff6401b501efffffffd201
```

Patterns & Trends: Shutdown of milling machine controller

Extracting ICS indicators

Behavioral detection from external reports – Industroyer



a particular data element in the device. Figure 6 illustrates a 101 payload configuration file with two defined IOA ranges, 10-15 and 20-25.

```
real_process.exe
COM1
1---
COM2
2---
COM3
3---
2
10
15
20
25
```

Figure 6. An example of a 101 payload DLL configuration.

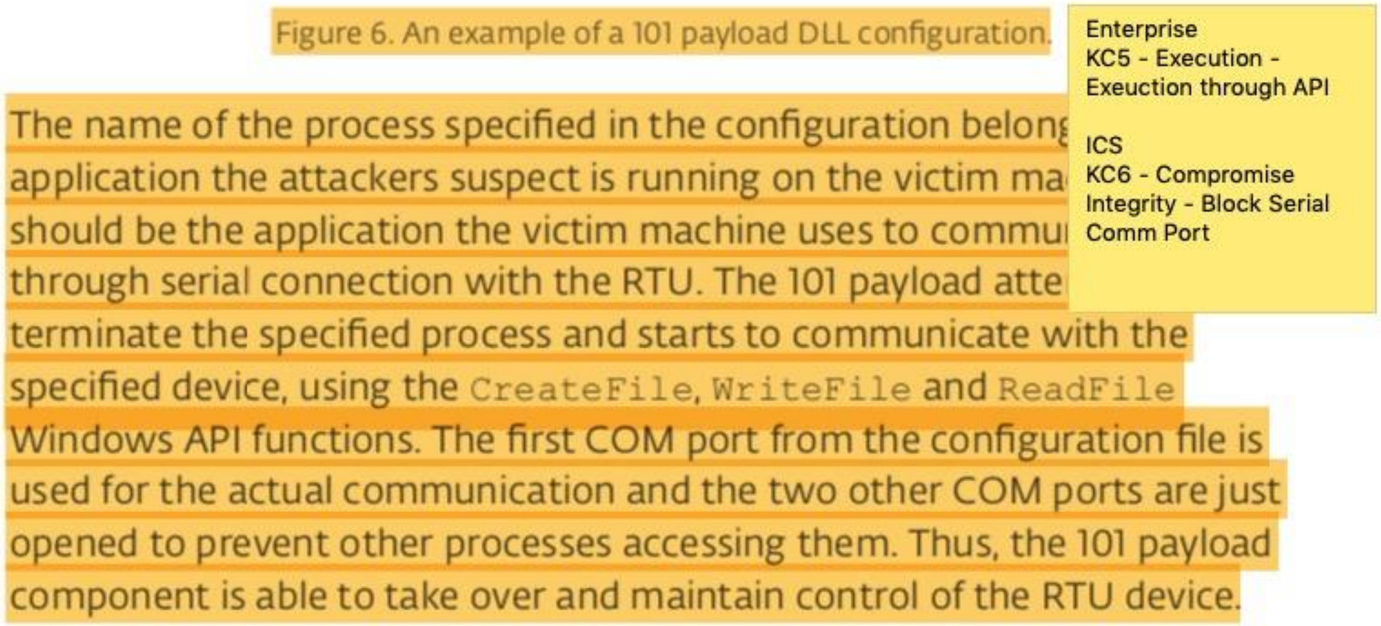


Figure 6. An example of a 101 payload DLL configuration.

The name of the process specified in the configuration belong application the attackers suspect is running on the victim ma should be the application the victim machine uses to commu through serial connection with the RTU. The 101 payload atte terminate the specified process and starts to communicate with the specified device, using the `CreateFile`, `WriteFile` and `ReadFile` Windows API functions. The first COM port from the configuration file is used for the actual communication and the two other COM ports are just opened to prevent other processes accessing them. Thus, the 101 payload component is able to take over and maintain control of the RTU device.

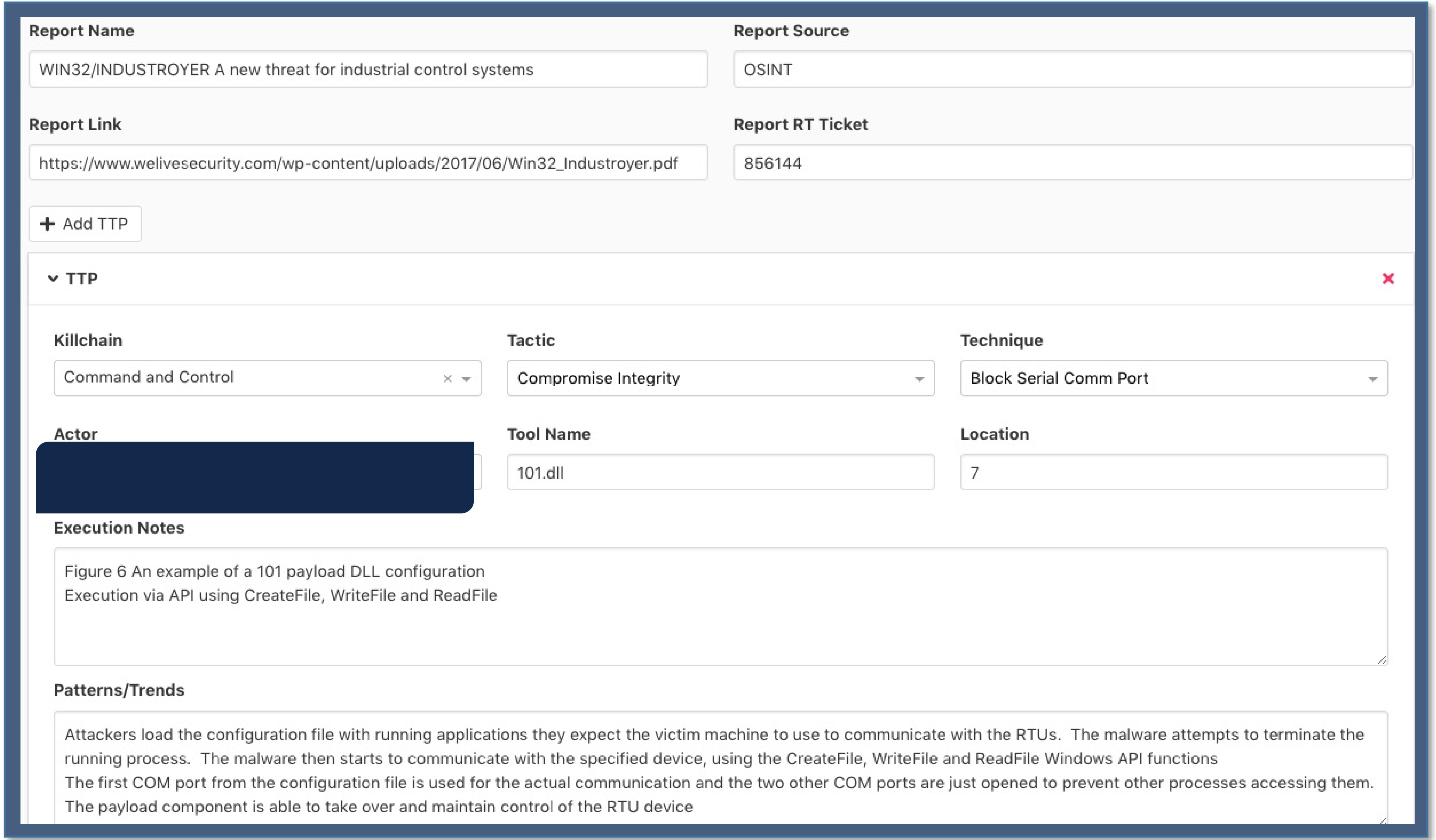
Enterprise
KC5 - Execution - Exeuction through API

ICS
KC6 - Compromise Integrity - Block Serial Comm Port

(Reference 7)

Detection & Confidence

Entering ATT&CK data into TIAMAT



Report Name
WIN32/INDUSTROYER A new threat for industrial control systems

Report Source
OSINT

Report Link
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Report RT Ticket
856144

Killchain
Command and Control

Tactic
Compromise Integrity

Technique
Block Serial Comm Port

Actor
[redacted]

Tool Name
101.dll

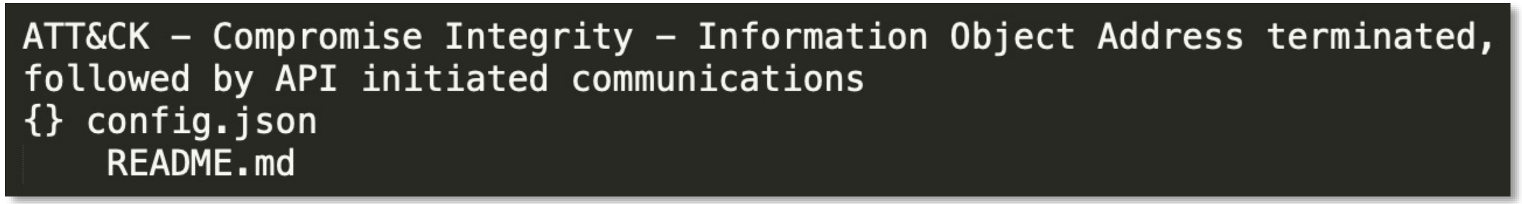
Location
7

Execution Notes
Figure 6 An example of a 101 payload DLL configuration
Execution via API using CreateFile, WriteFile and ReadFile

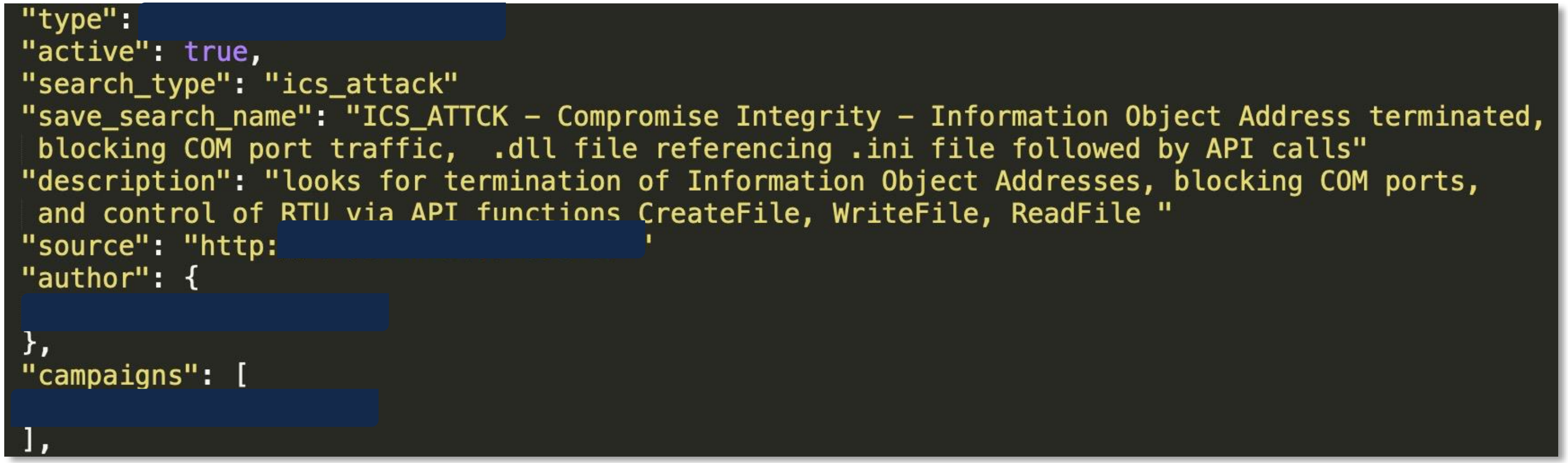
Patterns/Trends
Attackers load the configuration file with running applications they expect the victim machine to use to communicate with the RTUs. The malware attempts to terminate the running process. The malware then starts to communicate with the specified device, using the CreateFile, WriteFile and ReadFile Windows API functions
The first COM port from the configuration file is used for the actual communication and the two other COM ports are just opened to prevent other processes accessing them.
The payload component is able to take over and maintain control of the RTU device

Content Development

Behavior-based signatures

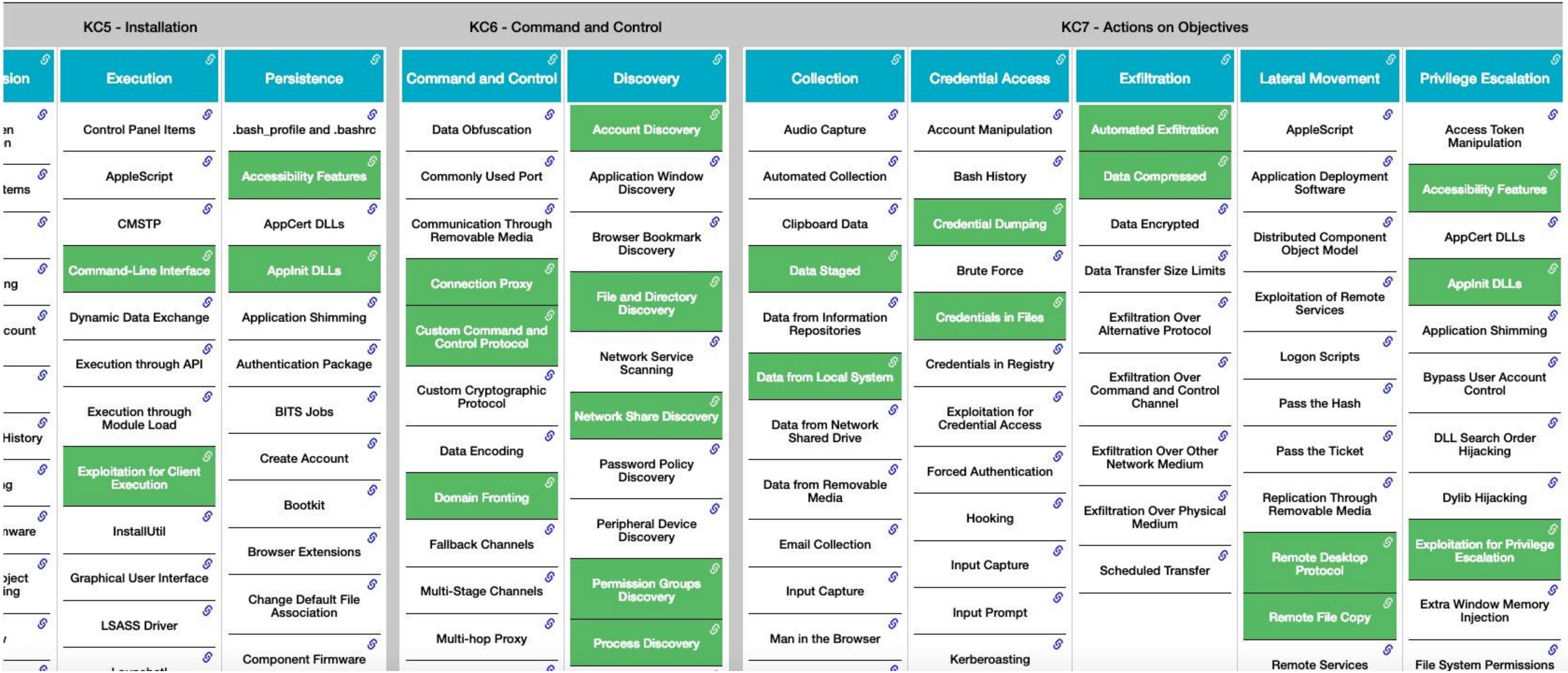


```
ATT&CK – Compromise Integrity – Information Object Address terminated,
followed by API initiated communications
{} config.json
    README.md
```



```
"type": [redacted]
"active": true,
"search_type": "ics_attack"
"save_search_name": "ICS_ATTCK – Compromise Integrity – Information Object Address terminated,
 blocking COM port traffic,  .dll file referencing .ini file followed by API calls"
"description": "looks for termination of Information Object Addresses, blocking COM ports,
 and control of RTU via API functions CreateFile, WriteFile, ReadFile "
"source": "http:[redacted]'
"author": {
[redacted]
},
"campaigns": [
[redacted]
],
```

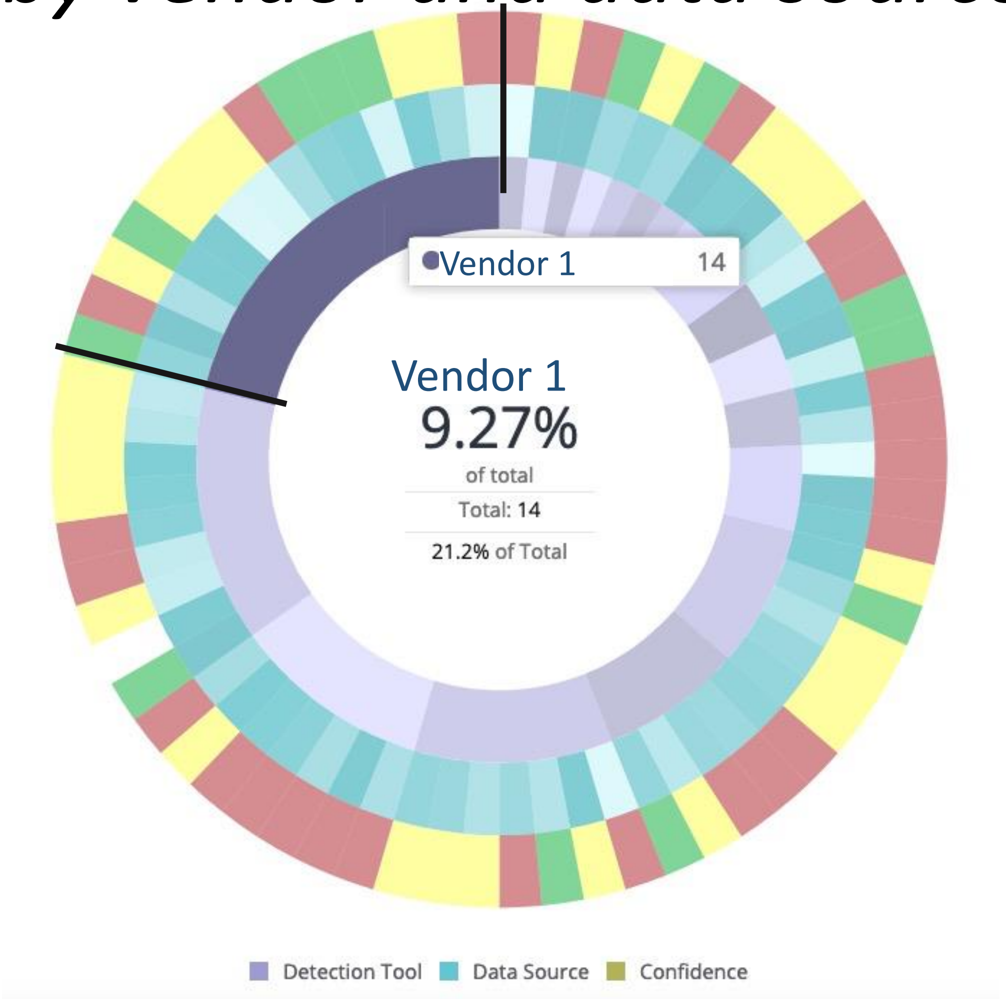
Visual map of behavior-based coverage *(sample)*

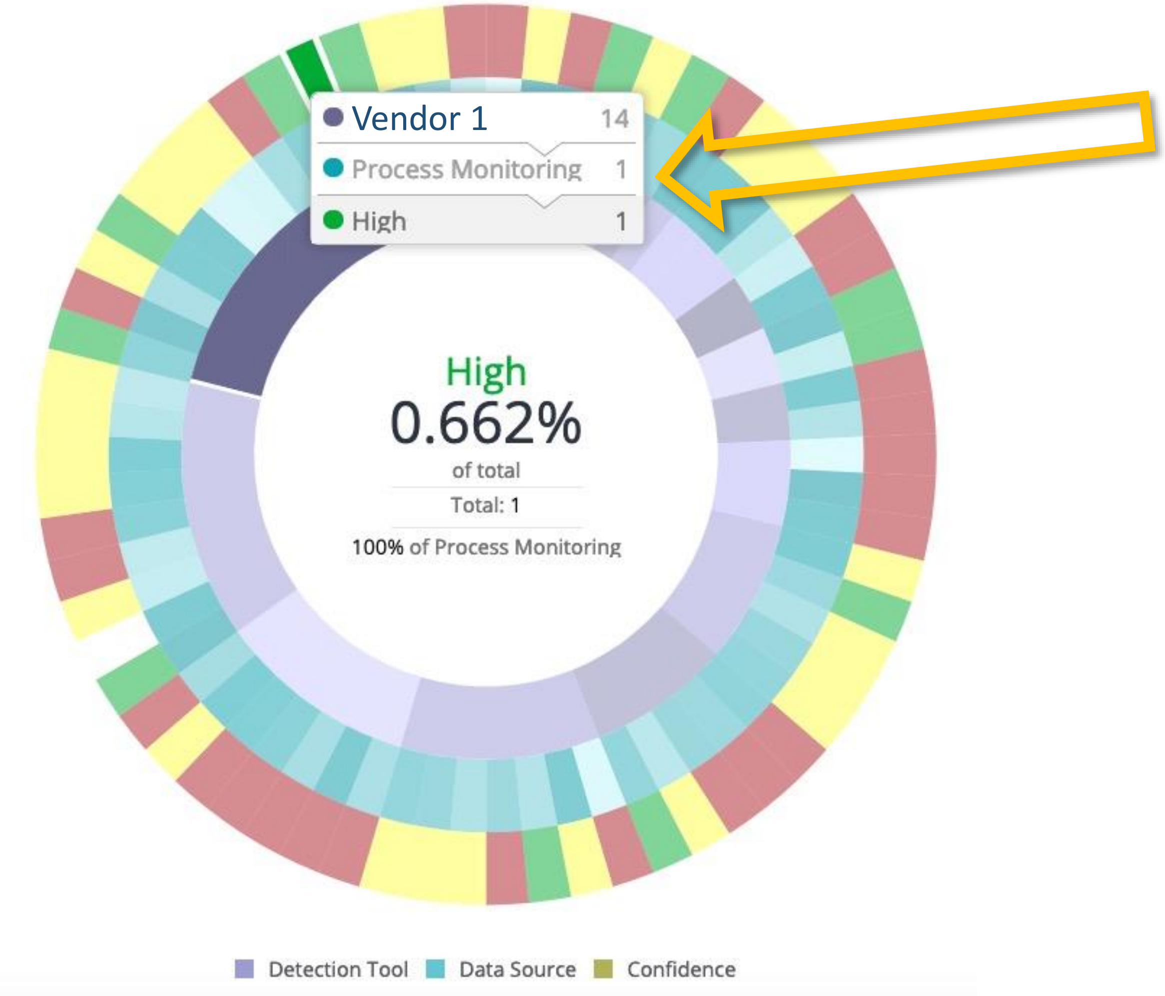


	KC5 - Installation		KC6 - Command and Control		KC7 - Actions on Objectives				
sion	Execution	Persistence	Command and Control	Discovery	Collection	Credential Access	Exfiltration	Lateral Movement	Privilege Escalation
en n	Control Panel Items	.bash_profile and .bashrc	Data Obfuscation	🟩 Account Discovery	Audio Capture	Account Manipulation	🟩 Automated Exfiltration	AppleScript	Access Token Manipulation
tems	AppleScript	🟩 Accessibility Features	Commonly Used Port	Application Window Discovery	Automated Collection	Bash History	🟩 Data Compressed	Application Deployment Software	🟩 Accessibility Features
	CMSTP	AppCert DLLs	Communication Through Removable Media	Browser Bookmark Discovery	Clipboard Data	🟩 Credential Dumping	Data Encrypted	Distributed Component Object Model	AppCert DLLs
ng	🟩 Command-Line Interface	🟩 AppInit DLLs	🟩 Connection Proxy	🟩 File and Directory Discovery	🟩 Data Staged	Brute Force	Data Transfer Size Limits	Exploitation of Remote Services	🟩 AppInit DLLs
count	Dynamic Data Exchange	Application Shimming	🟩 Custom Command and Control Protocol	Network Service Scanning	Data from Information Repositories	🟩 Credentials in Files	Exfiltration Over Alternative Protocol	Logon Scripts	Application Shimming
	Execution through API	Authentication Package	Custom Cryptographic Protocol	🟩 Network Share Discovery	🟩 Data from Local System	Credentials in Registry	Exfiltration Over Command and Control Channel	Pass the Hash	Bypass User Account Control
History	Execution through Module Load	BITS Jobs	Data Encoding	Password Policy Discovery	Data from Network Shared Drive	Exploitation for Credential Access	Exfiltration Over Other Network Medium	Pass the Ticket	DLL Search Order Hijacking
g	🟩 Exploitation for Client Execution	Create Account	🟩 Domain Fronting	Peripheral Device Discovery	Data from Removable Media	Forced Authentication	Exfiltration Over Physical Medium	Replication Through Removable Media	Dylib Hijacking
nware	InstallUtil	Bootkit	Fallback Channels	🟩 Permission Groups Discovery	Email Collection	Hooking	Scheduled Transfer	🟩 Remote Desktop Protocol	🟩 Exploitation for Privilege Escalation
ject ing	Graphical User Interface	Browser Extensions	Multi-Stage Channels	🟩 Process Discovery	Input Capture	Input Capture		🟩 Remote File Copy	Extra Window Memory Injection
/	LSASS Driver	Change Default File Association	Multi-hop Proxy		Man in the Browser	Input Prompt		Remote Services	File System Permissions
		Component Firmware				Kerberoasting			

Detection confidence *(sample)*

by vendor and data source





Technique Prioritization *(sample)*

by detection platform and data source

TTP	
Rundll32	
Meta	
Associated Tools	8
Associated Actors	15
Reports	20
Internal Incidents	2
Detection Priority	Medium

Detection Platform	Data Sources	Number of Signatures	Detection Confidence
Vendor 1	File Monitoring	10	3
	Binary File Metadata	0	1
	Process command-line parameters	8	3
	Process monitoring	12	2
Vendor 2	File Monitoring	0	1
	Binary File Metadata	2	2
	Process command-line parameters	8	1
	Process monitoring	0	1
Vendor 3	Expandable	25	3
Vendor 4	Expandable	0	1
Vendor 5	Expandable	10	2
Vendor 6	Expandable	19	2

Lessons learned and take-aways

- **Common Frameworks** ensure consistency in response
- Leadership buy-in and **patience**
- Operational Ready
- **Enforce rigor**
- Automate first
- Operationalizing the ATT&CK™ framework allows for **threat prioritization**
- Intelligence Driven Defense **increased** GE’s signature fidelity by **124%**

Q&A

Conrad Layne

LinkedIn:
conrad-layne

Email:
conrad.layne1@ge.com

Chip Greene

Twitter:
@urspider
@itotsecops (BigPhish)

LinkedIn:
cpgreene

Email:
chip.greene@ge.com

BOF for **Wednesday, 19 June** at **8:00-9:00** in the **Lowther Suite**
We are hiring…… https://www.ge.com/careers/

References

1. Lockheed Martin Cyber Kill Chain
https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

2. SANS Industrial Control System Cyber Kill Chain
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

3. MITRE ATT&CK Framework
https://attack.mitre.org/matrices/enterprise/windows/

4. MITRE ICS ATT&CK Framework
https://www.rsaconference.com/writable/presentations/file_upload/sbx4-w1-ics_scada_attack_detection_101.pdf

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

6. TIAMAT
https://en.wikipedia.org/wiki/Tiamat_(Dungeons_%26_Dragons)
http://thecampaign20xx.blogspot.com/2015/01/dungeons-dragons-guide-to-tiamat.html?_sm_au_=iDH12DQPwjt7wRJ6

7. Industroyer
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf