



**FORTINET**<sup>®</sup>

# From Threat Intelligence to Active Defense Based on Industroyer.V2



**THREAT INTELLIGENCE PRACTITIONERS' SUMMIT**

# Gergely (Geri) Revay

Security Researcher at FortiGuard Labs

- Comes from Hungary
- Lives in Germany
- M.Sc. in Computer Engineering specialized on Information and Network Security
- 4 years as QA tester at a Firewall vendor (Balabit)
- 7 years as penetration tester at OptimaBit and Siemens both in Germany and USA
- 3 years offensive security research at Siemens with focus on binary analysis and reverse engineering
- Author of various online courses: <https://hackademy.aetherlab.net>
- FortiGuard Labs researcher doing malware reverse engineering and threat intel
- Youtube channel: <https://youtube.com/aetherlabnet>
- Twitter: @geri\_revay



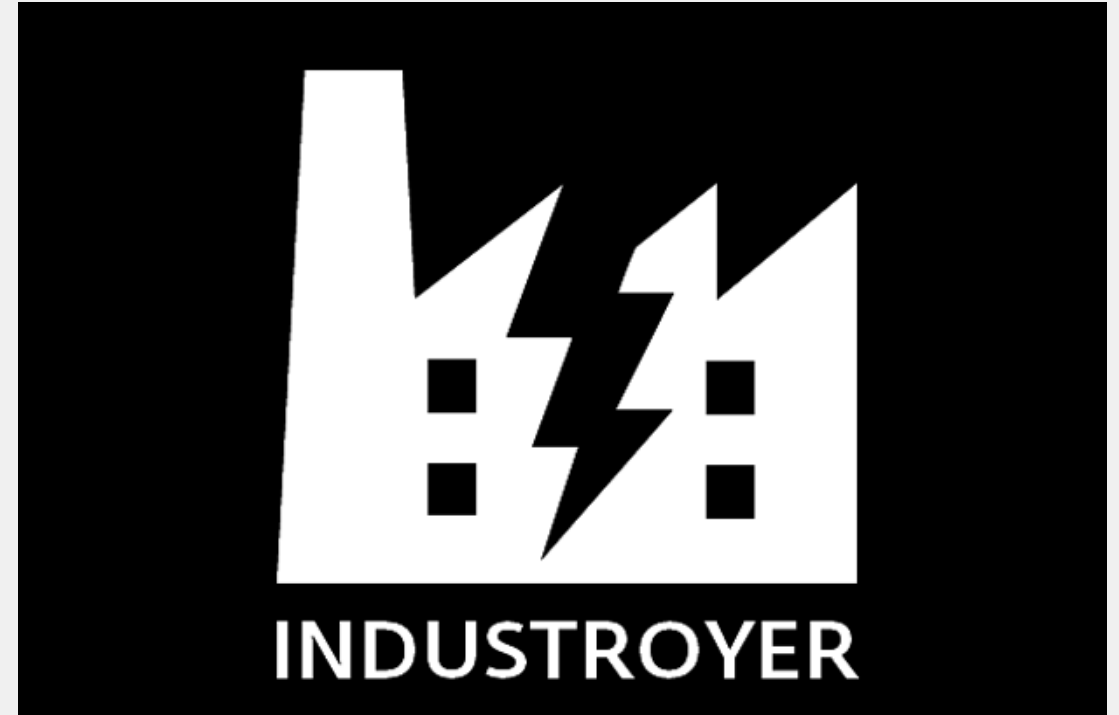
# Goal: Turn intelligence actionable

- Actionable intelligence is kind of a buzz word
- How can we use publicly available intel?
- How to turn that intel actionable?



# Industroyer / CrashOverride

- Targeted Ukraine's power grid in 2016
- Caused an hour power outage in a part of Kyiv
- Industroyer is a complex OT specific malware used in the attack
- It can manipulate Intelligent Electronic Devices (IED) using the following protocols:
  - IEC 60870-5-101
  - IEC 60870-5-104
  - IEC 61850
  - OLE for Process Control Data Access (OPC DA)

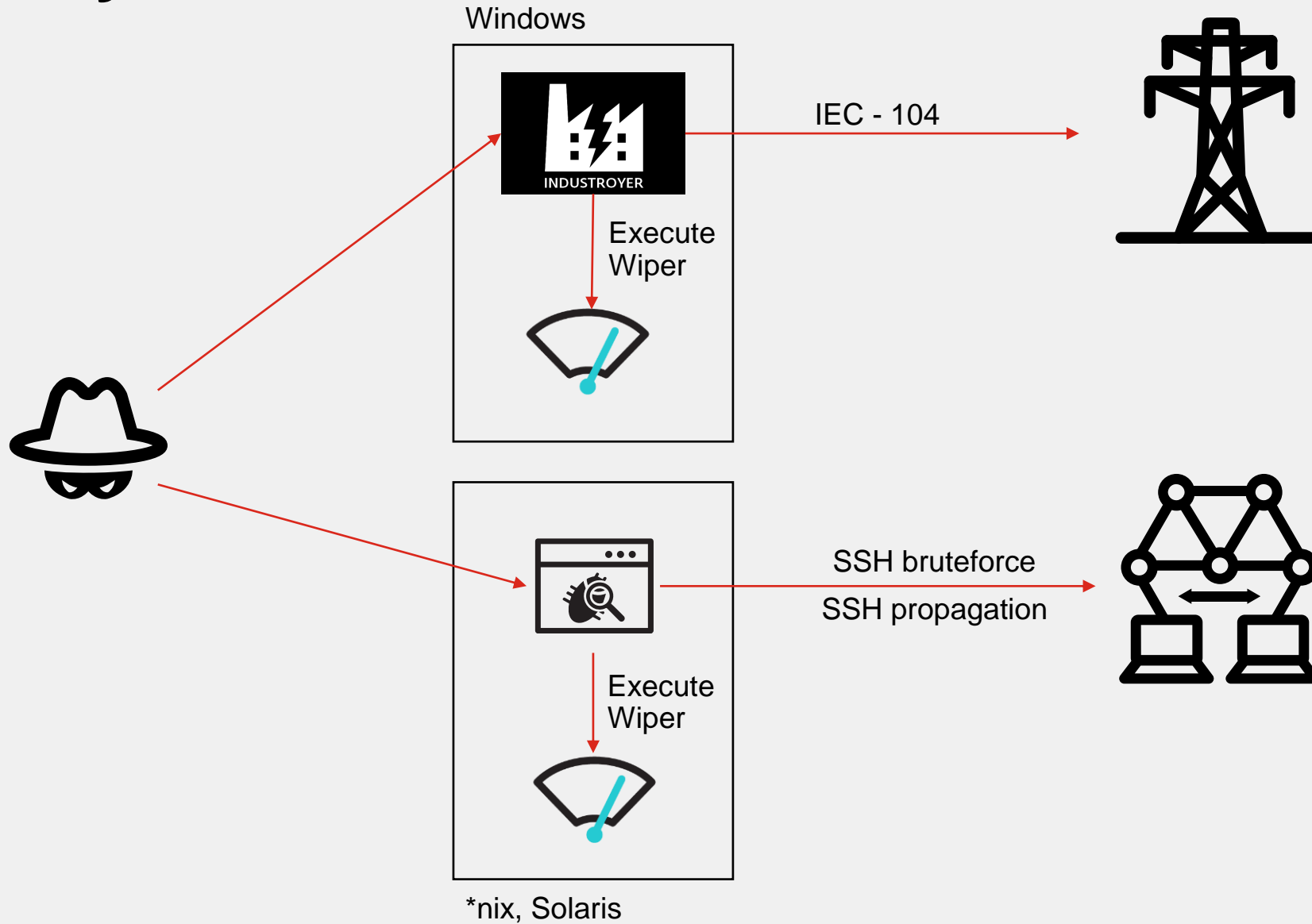


# Industroyer.V2

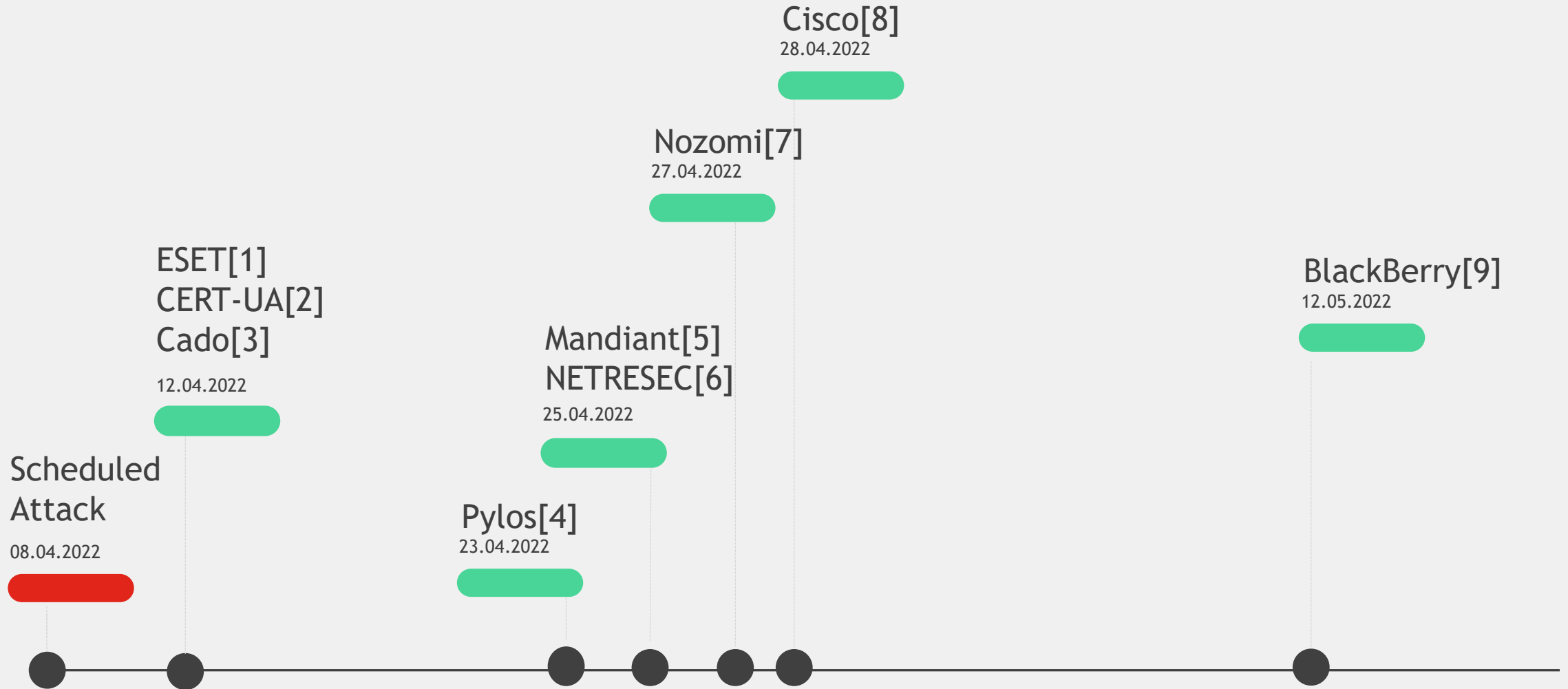
- Target was Ukrainian energy company
- ESET responded with CERT-UA
- High voltage electric substation
- It was scheduled to 'detonate' on 08.04.2022
- It was detected before detonation
- Deployed together with different wipers
  - CADDYWIPER: Windows wiper
  - ORCSHRED: worm → SSH scanning and bruteforce, propagation, wiper deployment
  - SOLOSHRED: Solaris wiper
  - AWFULSHRED: Linux wiper

The logo features the words "INDUSTROYER" and "STRIKES BACK" in a bold, yellow, outlined font, stacked vertically on a black rectangular background.

# Industroyer.V2 Process



# Available Intelligence



08.04.2022

# Collecting IOCs

- Explicit IOCs
- Implicit IOCs
- Most information is about the deployed malware
- Not much is publicly known about the rest of the Kill Chain
- Time consuming
- Result: 59 IOC (w/o hashes)

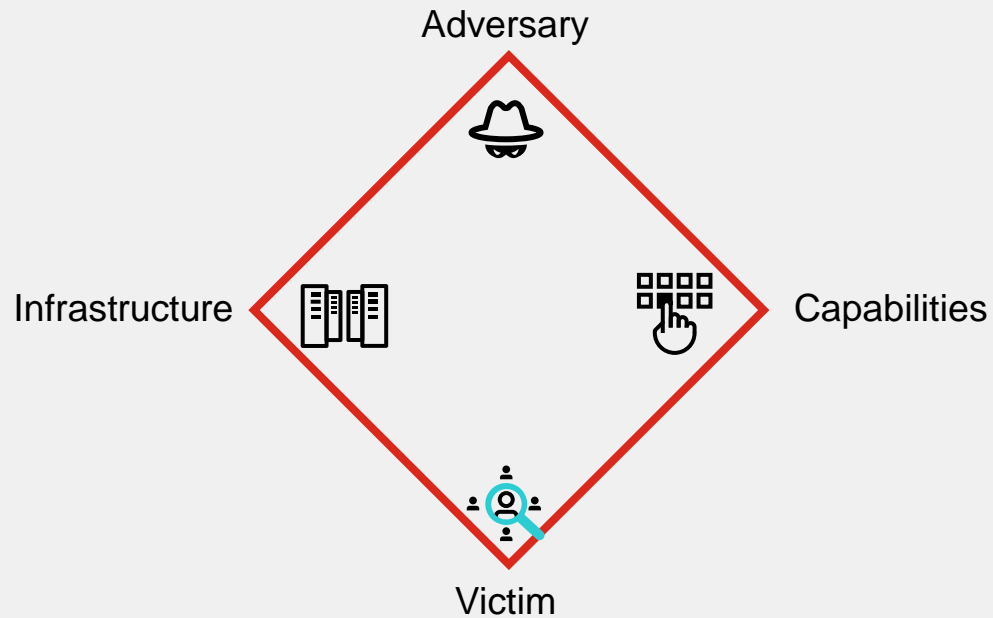
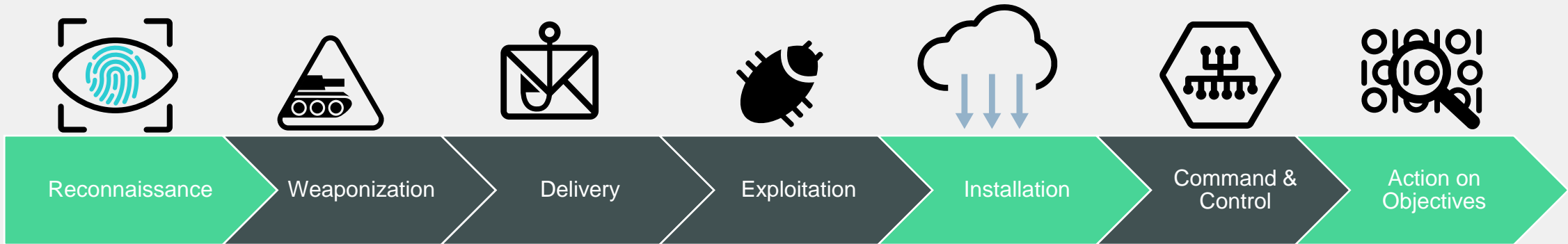
<b>Industroyer2 malware</b>
PService_PPD.exe
PServiceControl.exe
D:\OIK\DevCounter
Rename service files
108_100.exe
IEC-104
executed by scheduled task
IEC-104 manipulation
port 2404
<b>CADDYWIPER</b>
pa.pay
dropped by arguepatch
deployed through GPO
enumerating drives
\\.\\PHYSICALDRIVE0-9
\\.\\PHYSICALDRIVE0-9
delete MBR
deletes drives
deletes physical drives
<b>ORCSHRED</b>
"Start most security mode!"
"check_solaris"
"wsol.sh"
"wobf.sh"
"/var/log/res"
sc.sh
cron job
scans SSH
SSH bruteforce
self-replication

<b>SOLOSHRED</b>
disables services including 'ssh', 'http', 'apache', 'ora_', or 'oracle'
uses svcadm or systemctl
deletes file in /boot, /home and /var/log
uses shred or rm
deletes directories in env variables starting with ORA
enumerates and deletes all disks under /dev/dsk/
wsol.sh
<b>AWFULSHRED</b>
wobf.sh
function names are random 8 letter strings
using shred or dd
stop SSH and HTTP services
deletes file in /boot, /home and /var/log
<b>arguepatch</b>
zrada.exe
modified IDA debug server
peremoga.exe
<b>AD_enum_script</b>
uses the ADSI interface
powershell
enumerates GPOs
link.ps1





# Mapping IOCs to Kill Chain and Diamond Model



# Mapping IOCs to Kill Chain and Diamond Model

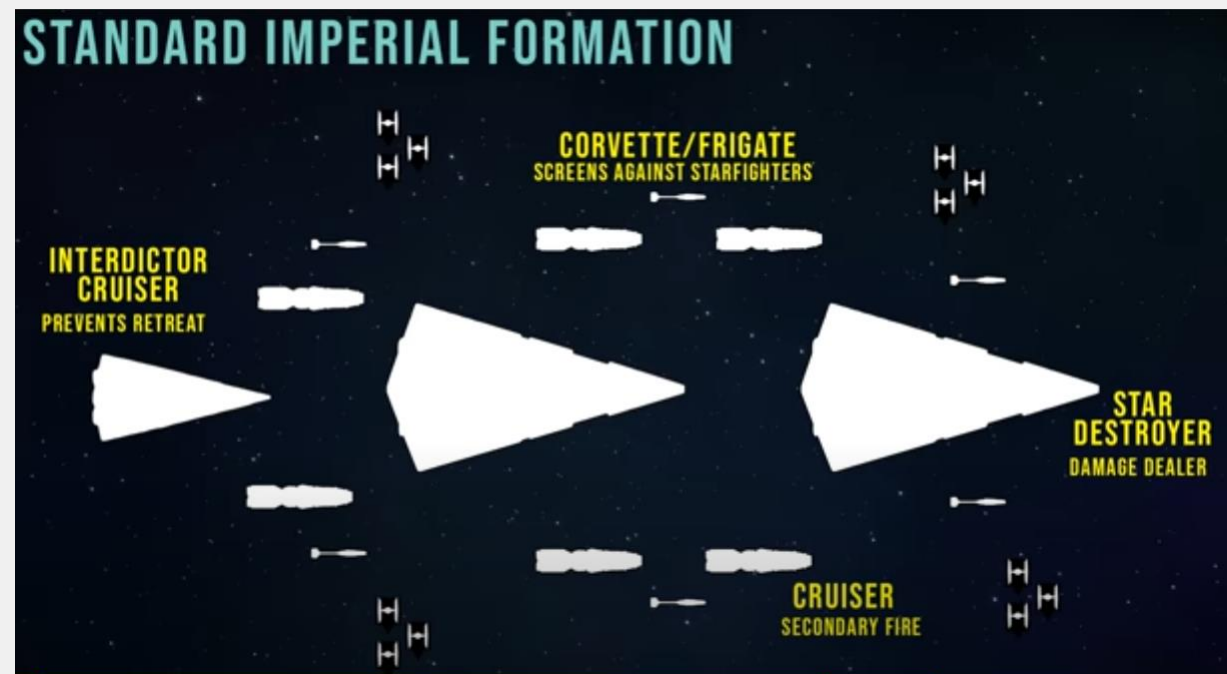
- Go through each IOC and map it to
  - Kill Chain
  - Diamond Model
- Helps us better understand the attack
- We see what we are missing
- Will be useful in categorization

Indicator	KC Phase	DM: Adversary	DM: Capability	DM: Infrastructure	DM: Victim
PService_PPD.exe	Recon				
PServiceControl.exe	Recon				
D:\OIK\DevCounter	Recon				
IEC-104 is used	Recon				
<b>Industroyer2 malware</b>		<b>Industroyer2</b>			
PService_PPD.exe	Installation				PService_PPD.exe
PServiceControl.exe	Installation				PServiceControl.exe
D:\OIK\DevCounter	Installation				D:\OIK\DevCounter
Rename service files	Installation				
108_100.exe	Installation		108_100.exe		
IEC-104	Action		IEC-104		IEC-104
executed by scheduled task	Installation		Scheduled task		
IEC-104 manipulation	Action		IEC-104 communication		
port 2404	Action				port 2404
<b>CADDYWIPER</b>		<b>CADDYWIPER</b>			
pa.pay	Weaponization		pa.pay		arguepatch
dropped by arguepatch	Installation				GPO
deployed through GPO	Installation		edit GPO		
enumerating drives	Action		enumerating drives D: -Z:		from D:\ to Z:\
\\.\\PHYSICALDRIVE0-9	Action		enumerated physical drives		\\.\\PHYSICALDRIVE0-9
\\.\\PHYSICALDRIVE0-9	Action		enumerated physical drives		\\.\\PHYSICALDRIVE0-9
delete MBR	Action		delete MBR		
deletes drives	Action				
deletes physical drives	Action				



# Mapping to ATT&CK TTPs

Indicator	ATT&CK Matrix	ATT&CK Tactic	ATT&CK Technique
<b>Industroyer2 malware</b>	Enterprise		
PService_PPD.exe	Enterprise	Impact	Service Stop (T1489)
PServiceControl.exe	Enterprise	Impact	Service Stop (T1489)
D:\OIK\DevCounter			
Rename service files	Enterprise	Defense Evasion	Hide Artifacts (T1564)
108_100.exe			
IEC-104			
executed by scheduled task	Enterprise	Execution	Scheduled Task/Job (T1053)
IEC-104 manipulation	ICS	Impact	Manipulation of Control (T0831)
port 2404			N/A
<b>CADDYWIPER</b>			
pa.pay			N/A
dropped by arguepatch	Enterprise	Defense Evasion	Deobfuscate/Decode Files or Information (T1140)
deployed through GPO	Enterprise	Defense Evasion	Domain Policy Modification: Group Policy Modification (T1484.001)
enumerating drives	Enterprise	Discovery	File and Directory Discovery (T1083)
\\.\PHYSICALDRIVE0-9	Enterprise	Defense Evasion	Direct Volume Access (T1006)
\\.\PHYSICALDRIVE0-9	Enterprise	Defense Evasion	Direct Volume Access (T1006)
delete MBR	Enterprise	Impact	Data Destruction (T1485)
deletes drives	Enterprise	Impact	Data Destruction (T1485)
deletes physical drives	Enterprise	Impact	Data Destruction (T1485)



[https://www.youtube.com/watch?v=p\\_dqgAQw9xA](https://www.youtube.com/watch?v=p_dqgAQw9xA)



# Mapping to ATT&CK

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/6)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Remote Service Session Hijacking (0/2)	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/1)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/5)	Inter-Process Communication (1/3)	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (1/4)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Channel	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Other Network Medium (0/1)	Disk Wipe (2/2)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create Account (0/3)	Domain Policy Modification (1/2)	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Physical Medium (0/1)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Trusted Relationship	Valid Accounts (0/4)	Shared Modules	Create or Modify System Process (0/4)	Escape to Host	Direct Volume Access	Modify Authentication Process (0/5)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Exfiltration Over Web Service (0/2)	Firmware Corruption
Search Open Websites/Domains (0/2)	System Services (0/2)	User Execution (0/3)	Software Deployment Tools	Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Domain Policy Modification (1/2)	Multi-Factor Authentication Interception (0/5)	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Scheduled Transfer	Inhibit System Recovery
Search Victim-Owned Websites	Windows Management Instrumentation	Windows Management Instrumentation	System Services (0/2)	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery	File and Directory Permissions Modification (0/2)	Data from Local System	Non-Application Layer Protocol	Transfer Data to Cloud Account	Network Denial of Service (0/2)
			System Services (0/2)	Hijack Execution Flow (0/12)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery	Hide Artifacts (0/15)	Data from Network Shared Drive	Non-Standard Port	Proxy (0/4)	Resource Hijacking
			System Services (0/2)	Implant Internal Image	Hijack Execution Flow (0/12)	Hide Artifacts (0/15)	OS Credential Dumping (0/8)	Group Policy Discovery	Hijack Execution Flow (0/12)	Data from Removable Media	Protocol Tunneling	Remote Access Software	Service Stop
			System Services (0/2)	Modify Authentication Process (0/5)	Process Injection (0/12)	Impair Defenses (0/9)	Steal Application Access Token	Network Service Discovery	Impair Defenses (0/9)	Data Staged (0/2)	Traffic Signaling (0/1)	Web Service (0/3)	System Shutdown/Reboot
			System Services (0/2)	Office Application Startup (0/6)	Scheduled Task/Job (2/5)	Indicator Removal on Host (0/6)	Steal or Forge Kerberos Tickets (0/4)	Network Share Discovery	Indirect Command Execution	Email Collection (0/3)			
			System Services (0/2)	Pre-OS Boot (0/5)	Server Software Component (0/5)	Indirect Command Execution	Steal Web Session Cookie	Network Sniffing	Masquerading (0/7)	Input Capture (0/4)			
			System Services (0/2)	Scheduled Task/Job (0/5)	Traffic Signaling (0/1)	Modify Authentication Process (0/5)	Unsecured Credentials (0/7)	Network Sniffing	Modify Authentication Process (0/5)	Screen Capture			
			System Services (0/2)	Server Software Component (0/5)	Valid Accounts (0/4)	Modify Cloud Compute Infrastructure (0/4)	Unsecured Credentials (0/7)	Network Sniffing	Modify Cloud Compute Infrastructure (0/4)	Video Capture			
			System Services (0/2)	Traffic Signaling (0/1)		Modify Registry		Network Sniffing	Modify Registry				
			System Services (0/2)			Modify System Image (0/2)		Network Sniffing	Modify System Image (0/2)				
			System Services (0/2)			Network Boundary Bridging (0/1)		Network Sniffing	Network Boundary Bridging (0/1)				
			System Services (0/2)			Obfuscated Files or Information (0/6)		Network Sniffing	Obfuscated Files or Information (0/6)				
			System Services (0/2)			Plist File Modification		Network Sniffing	Plist File Modification				
			System Services (0/2)			Pre-OS Boot (0/5)		Network Sniffing	Pre-OS Boot (0/5)				
			System Services (0/2)			Process Injection (0/12)		Network Sniffing	Process Injection (0/12)				
			System Services (0/2)			Reflective Code Loading		Network Sniffing	Reflective Code Loading				



# Creating Courses of Actions

Indicator	Discover	Detect	Deny	Disrupt	Degrade	Deceive
<b>Industroyer2 malware</b>						
PService_PPD.exe	Find hosts with this file/service	Detect service stop				Investigate and disrupt process/user
PServiceControl.exe	Find hosts with this file/service	Detect service stop				Investigate and disrupt process/user
D:\OIK\DevCounter	Find hosts with this folder	Detect file changes in this folder				Investigate and disrupt process/user
Rename service files		Detect changes in filenames				Investigate and disrupt process/user
108_100.exe	Find hosts with this file/service	Detect if file is downloaded and send to AV	Based on AV output deny			
IEC-104	Find hosts talking IEC-104					
executed by scheduled task	Review current scheduled tasks in the network	Alert when new scheduled tasks are created				Investigate and disrupt process/user
IEC-104 manipulation		- Create baseline of IEC-104 comm, and alert anomalies - Alert if an unexpected host talks IEC-104				Investigate and disrupt process/user
port 2404	Find hosts with open port	- Create baseline of comm to this port, and alert anomalies - Alert if an unexpected host talk	Depending on the host which makes the changes deny if possible			Investigate and disrupt process/user



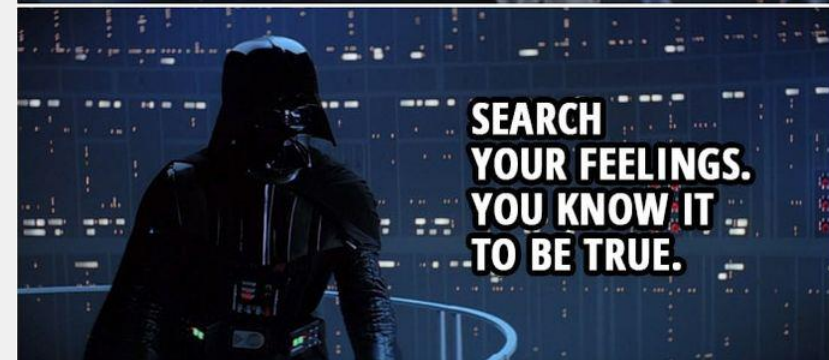
# Now what?

- Great that we have an excel table nobody will ever read
- Now comes the crucial part to figure out what to do with the information we learnt
- Goal: improve our defences
- Goal: answer questions like “Are we protected against Industroyer.V2?”



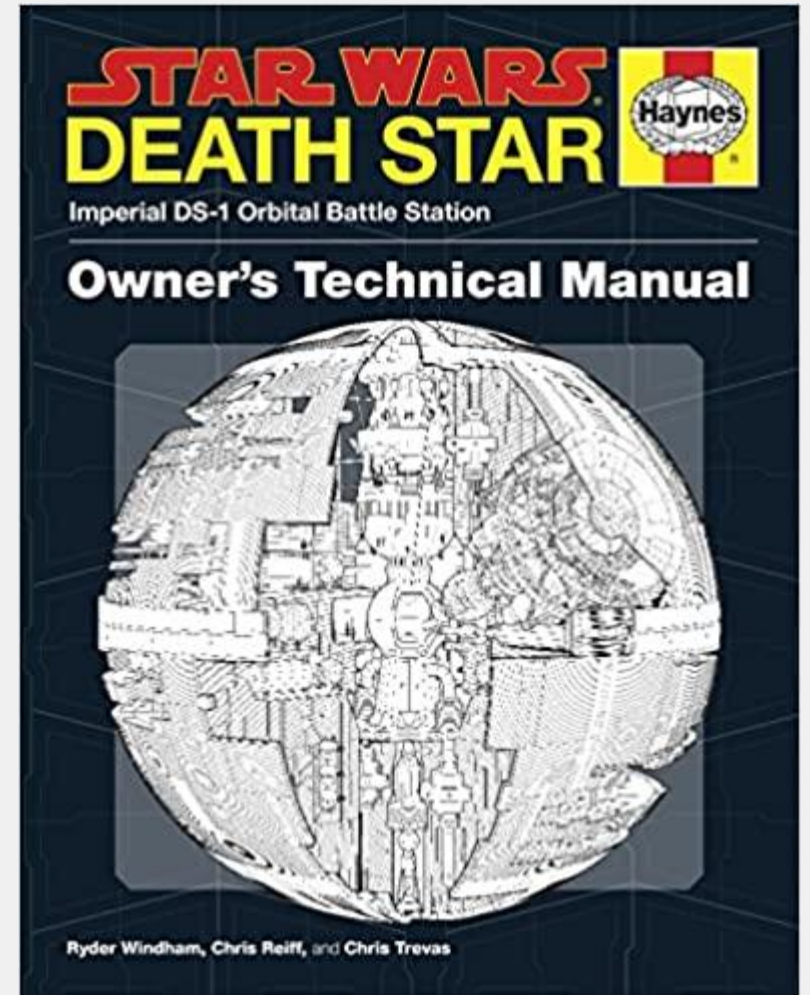
# Know your enemy - Know yourself

- Identify potential targets, i.e. ;
  - Find hosts that have PService\_PPD.exe
  - Identify IEDs and hosts using IEC-104
  - Search for open TCP port 2404
- Update risk assessment and threat model
  - The risk increases for the identified targets
- Exercise
  - Simulate incident to see how you would react
  - Create playbook
- Test our current defensive capabilities (Search your feelings)
- Improve our capabilities



# Test defenses against threat actor model

- Breach and Attack Simulation for the win
- Use the identified TTPs to see what will be detected
- Testing gives you an idea
  - where our blind spots are
  - where we should invest money and time
- There are plenty of options, i.e.:
  - Open source: Mitre's Caldera
  - Commercial: FortiTester, AttackIQ, etc..
- Decoys
  - Many options to build honeypots





# Threat Hunting

- Yara rules for the four malware samples are publicly available
  - VirusTotal: Live hunt, retro hunt
  - Sandbox tools
  - EDR solutions
  - AV engines
- Event log analysis / monitoring
- Creating baseline for OT network communication
- Review scheduled tasks



# Implementing defenses in security tools - Discover

What?	Where?
Discover	
Use Yara rules	Sandbox
Find hosts with specific or file/service	EDR / osquery
Find hosts with a specific folder	EDR / osquery
Find hosts talking IEC-104	Firewall / IPS
Review current scheduled tasks in the network	Custom script / osquery
Find hosts with open port TCP 2024	Port scanner/Firewall
Hunt for filename	EDR / osquery / custom script
Hunt for specific cron jobs	EDR / osquery / custom script
Hunt for ports scans in the past	Firewall / SIEM / IPS
Hunt for SSH bruteforce in the past	Firewall / SIEM / IPS
Find hosts with specific environment variables	Custom script
Search for scripts with this obfuscation (defined as a yara rule)	EDR / osquery
Hunt for similar binaries (defined as yara rule)	EDR / osquery
Audit past GPO modifcication	Active Directory / SIEM



# Implementing defenses in security tools – Detect 1

What?	Where?
Detect	
Use Yara rules	Sandbox
Detect service stopping	EDR / osquery / custom script
Detect file changes in this folder	Integrity Monitoring
Detect changes in filenames	Integrity Monitoring
Alert when new scheduled tasks are created	SIEM
Create baseline of IEC-104 comm, and alert anomalies	NDR / Firewall
Alert if an unexpected host talks IEC-104	NDR / Firewall
Create baseline of comm to a specific port and alert anomalies	NDR / Firewall
Alert if an unexpected host talk	NDR / Firewall
Detect in memory malware	EDR / AV
Detect AD object creation/modification	EDR / SIEM
Detect command execution that can alter GPOs	EDR / SIEM
Detect Windows API calls that enumerate drives	EDR
Detect enumeration of physical drives	EDR

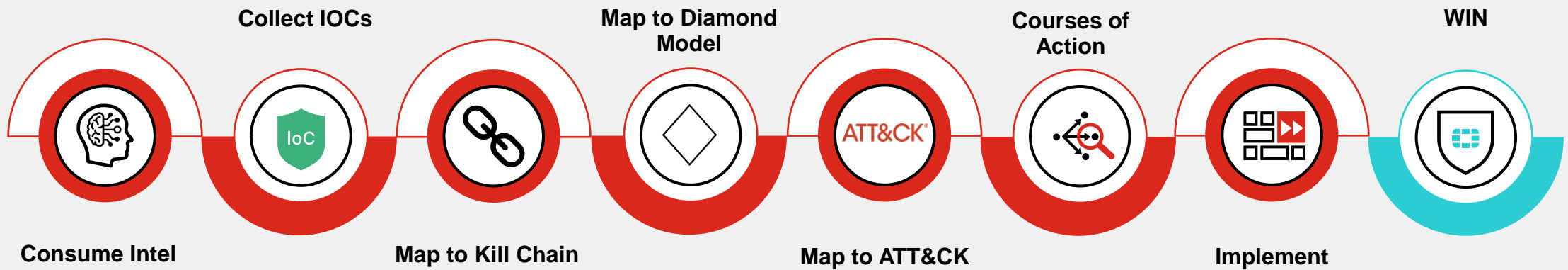


# Implementing defenses in security tools – Detect 2, Deny, Disrupt

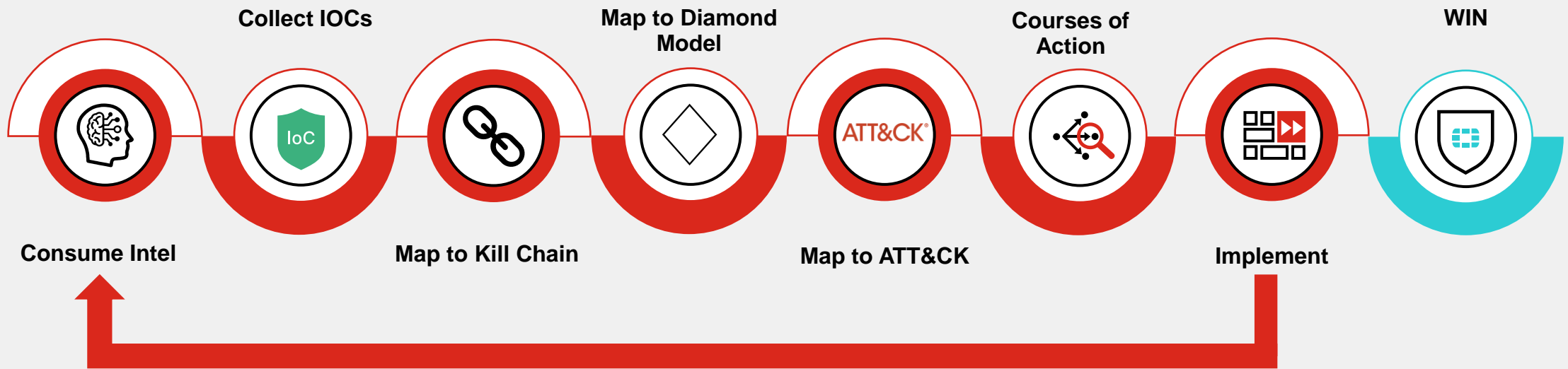
What?	Where?
<b>Detect</b>	
Monitor cron job creation	SIEM / custom script / osquery
Detect port scans (for SSH)	Firewall / IPS
Detect ssh bruteforce	Firewall / IPS
Alert on multiple failed ssh logins	EDR / SIEM
Monitor file changes in /boot	EDR / Integrity Protection
Monitor uses of shred and rm on a scale	EDR / SIEM
Monitor file deletion in folders that is in the ORA* environment variables	EDR
Monitor file enumeration and disk deletion	EDR
Monitor similar binaries on production machines	EDR / Sandbox
Monitor the use of COM objects, establish baseline and look for anomalies	EDR / SIEM
Enable powershell logging	GPO
Monitor powershell command execution	EDR / SIEM
Detect AD object creation/modification	EDR
Detect command execution that can alter GPOs	EDR / SIEM
<b>Deny</b>	
Block powershell script execution	EDR / AV
<b>Disrupt</b>	
Block SSH brute force	Firewall / IPS



# Conclusion



# Conclusion



# Thanks and Q 'n' A

Geri Revay  
Security Researcher at FortiGuard Labs

❖ Twitter: @geri\_revay



**FORTINET**®