FORTINET

From Threat Intelligence to Active Defense Based on Industroyer.V2

CYBER THREAT ALLIANCE

THREAT INTELLIGENCE PRACTITIONERS' SUMMIT

Gergely (Geri) Revay

Security Researcher at FortiGuard Labs

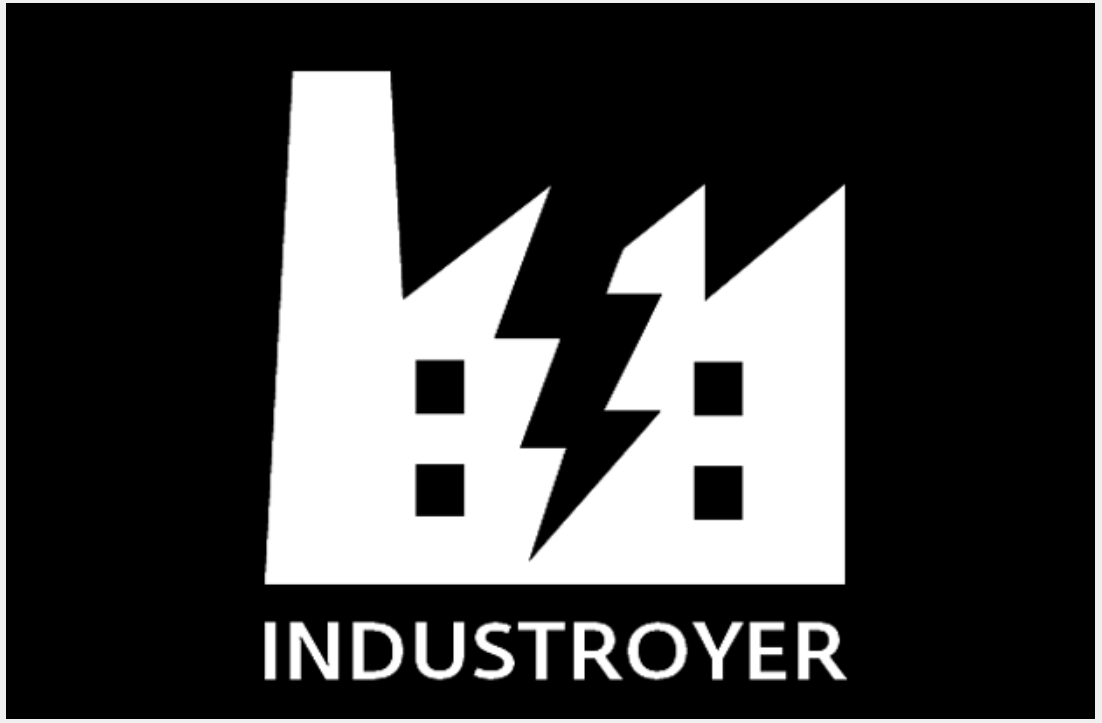
- Comes from Hungary
- Lives in Germany
- M.Sc. in Computer Engineering specialized on Information and Network Security
- 4 years as QA tester at a Firewall vendor (Balabit)
- 7 years as penetration tester at OptimaBit and Siemens both in Germany and USA
- 3 years offensive security research at Siemens 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

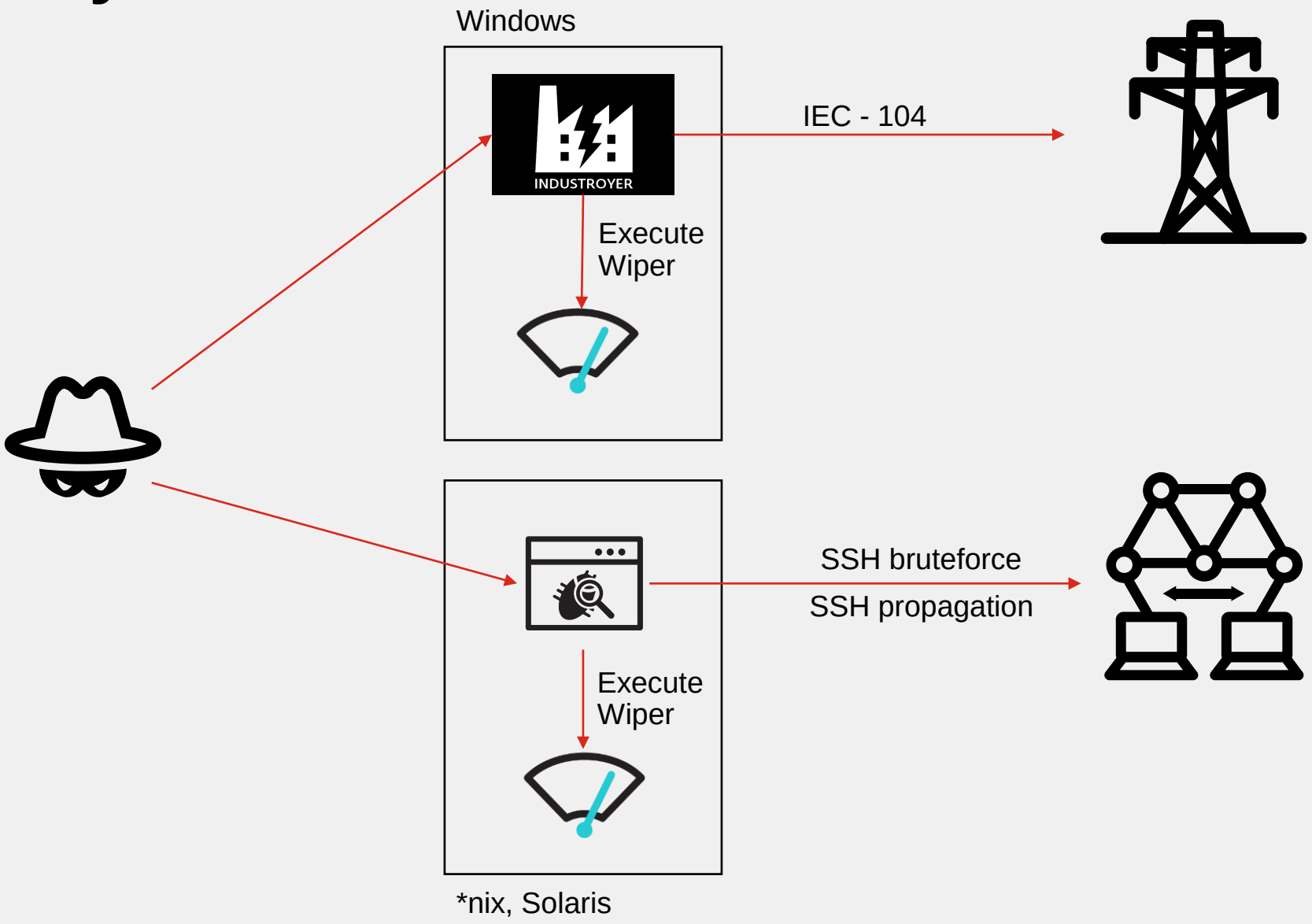
- Targeted Ukraine's power grid in 2016
- Caused an hour power outage in a part of Kyiv
- Industroyer is a complex OT specific malware used in the attack
- It can manipulate Intelligent Electronic Devices (IED) using the following protocols:
  - IEC 60870-5-101
  - IEC 60870-5-104
  - IEC 61850
  - OLE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



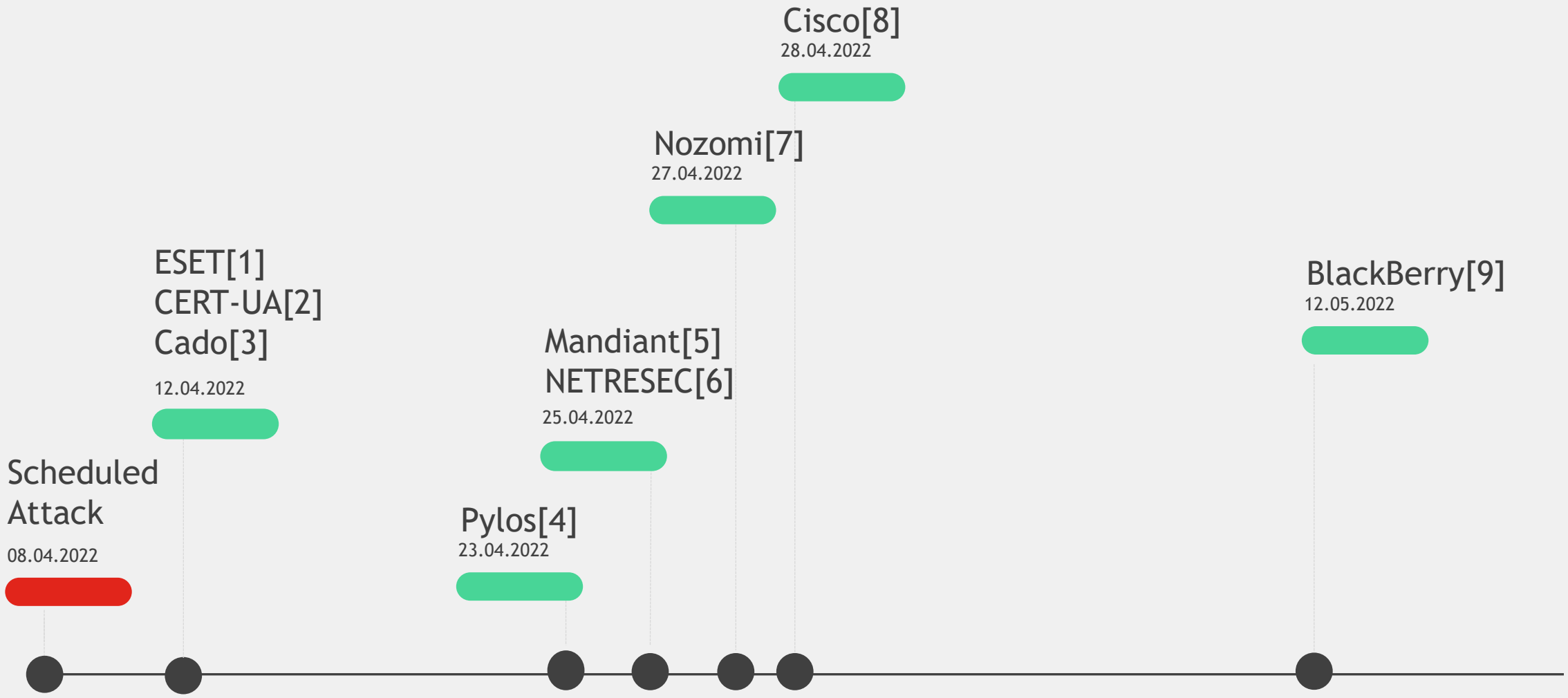
Industroyer.V2

- 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

Industroyer.V2 Process



Available Intelligence



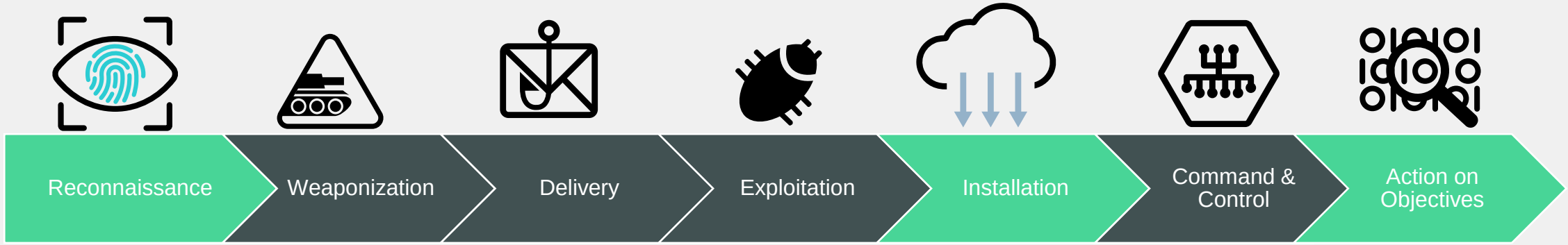
Collecting IOCs

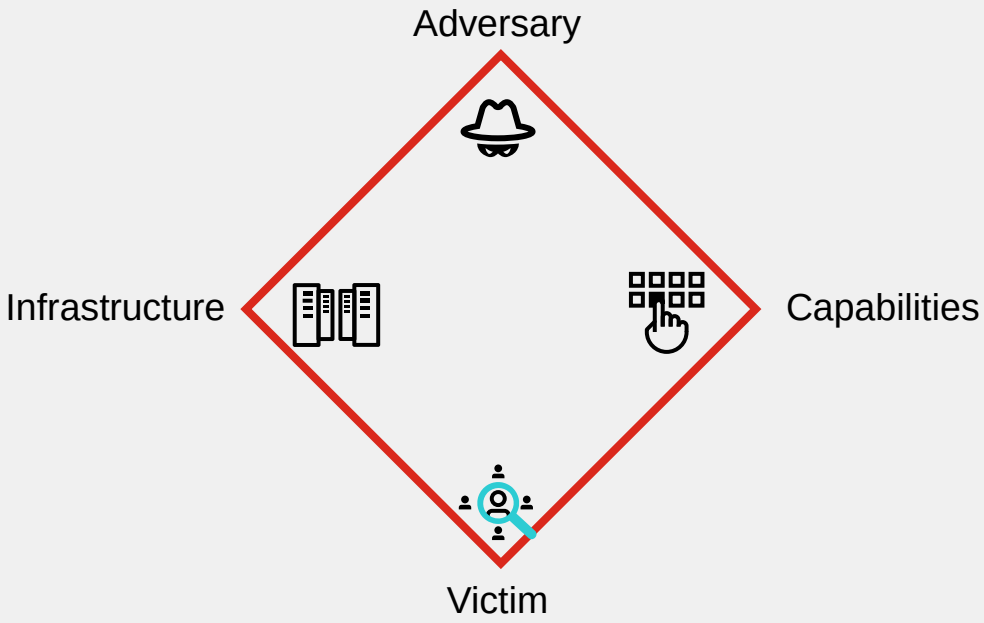
- Explicit IOCs
- Implicit IOCs
- Most information is about the deployed malware
- Not much is publicly known about the rest of the Kill Chain
- Time consuming
- Result: 59 IOC (w/o hashes)

Industroyer2 malware
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
CADDYWIPER
pa.pay
dropped by arguepatch
deployed through GPO
enumerating drives
\.\\PHYSICALDRIVE0-9
\.\\PHYSICALDRIVE0-9
delete MBR
deletes drives
deletes physical drives
ORCSHRED
"Start most security mode!"
"check_solaris"
"wsol.sh"
"wobf.sh"
"/var/log/res"
sc.sh
cron job
scans SSH
SSH bruteforce
self-replication

SOLOSHRED
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
AWFULSHRED
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
arguepatch
zrada.exe
modified IDA debug server
peremoga.exe
AD_enum_script
uses the ADSI interface
powershell
enumerates GPOs
link.ps1

Mapping IOCs to Kill Chain and Diamond Model





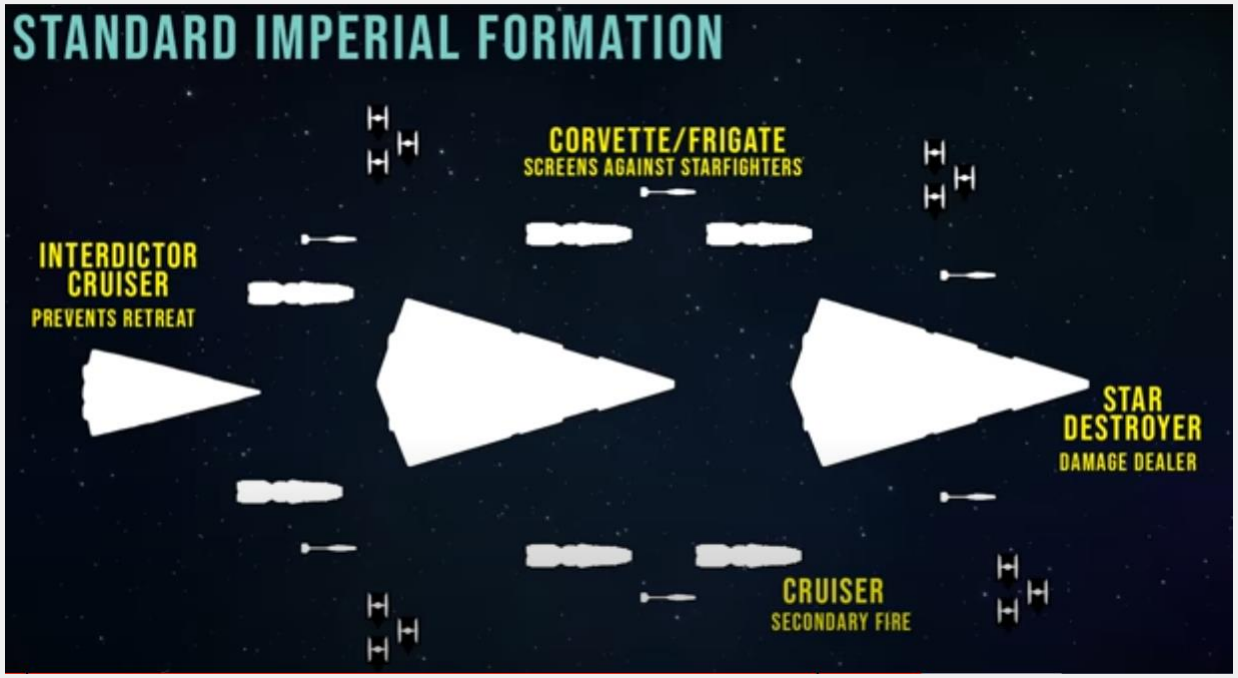
Mapping IOCs to Kill Chain and Diamond Model

- 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				
Industroyer2 malware			Industroyer2		
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
CADDYWIPER			CADDYWIPER		
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				

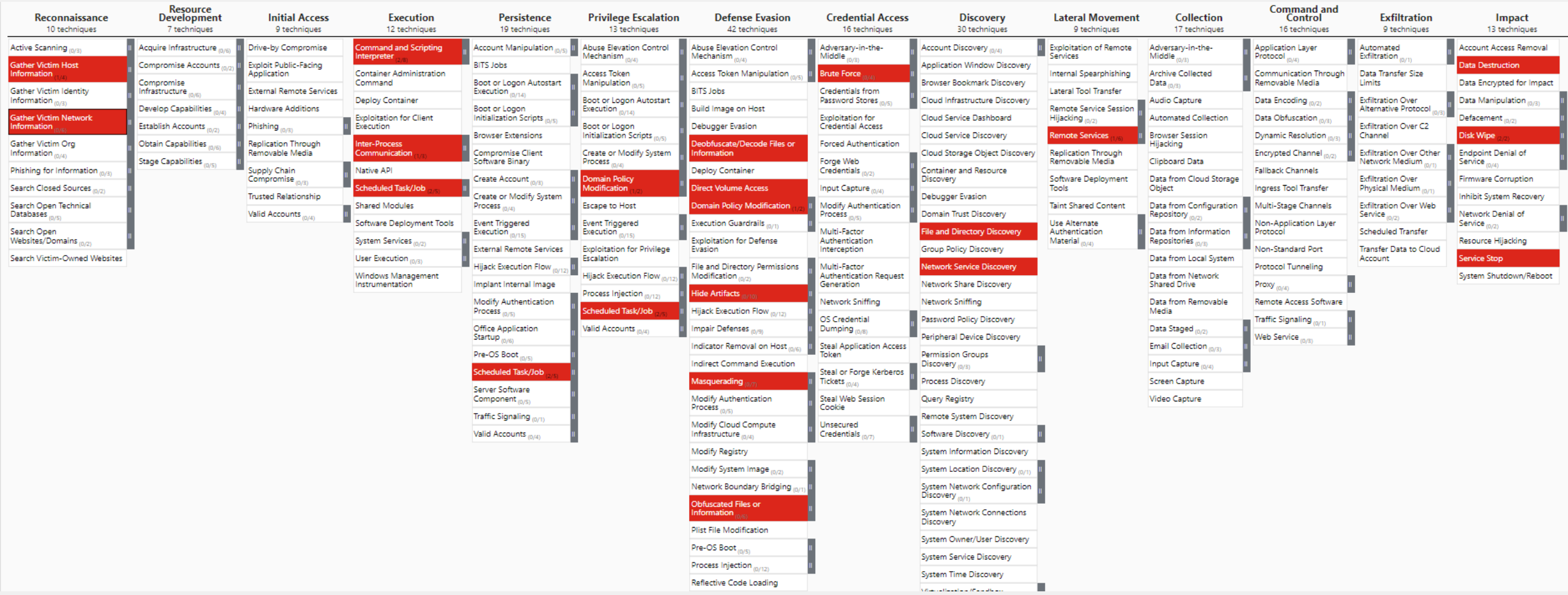
Mapping to ATT&CK TTPs

Indicator	ATT&CK Matrix	ATT&CK Tactic	ATT&CK Technique
Industroyer2 malware	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
CADDYWIPER			
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

Mapping to ATT&CK

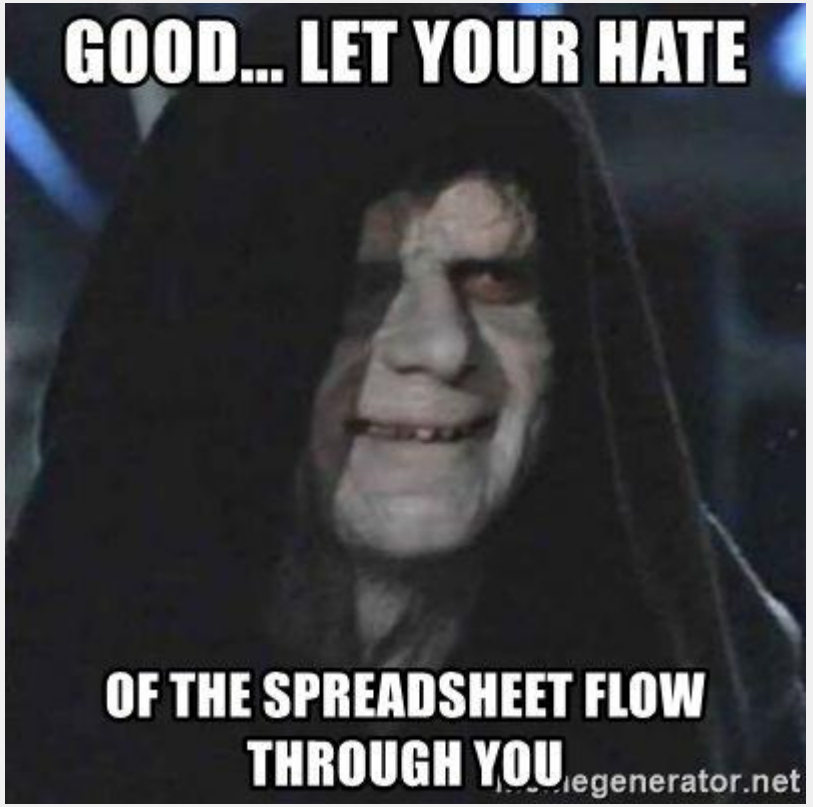


Creating Courses of Actions

Indicator	Discover	Detect	Deny	Disrupt	Degrade	Deceive
Industroyer2 malware						
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?”

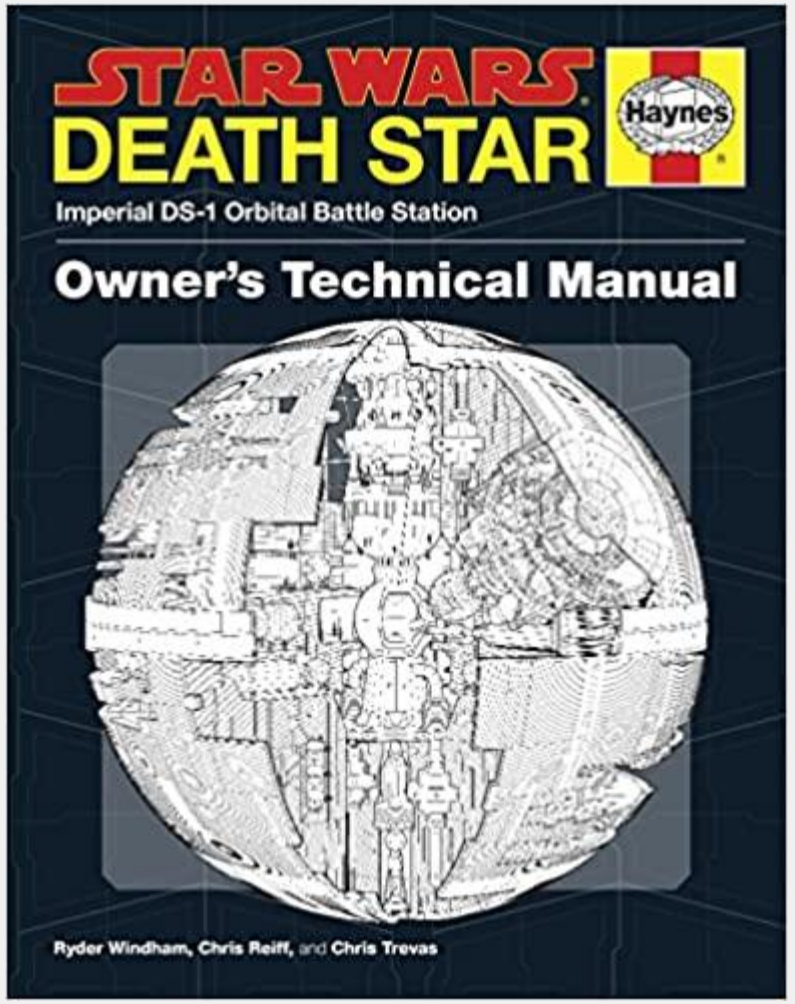


Know your enemy - Know yourself

- 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 modificccation	Active Directory / SIEM

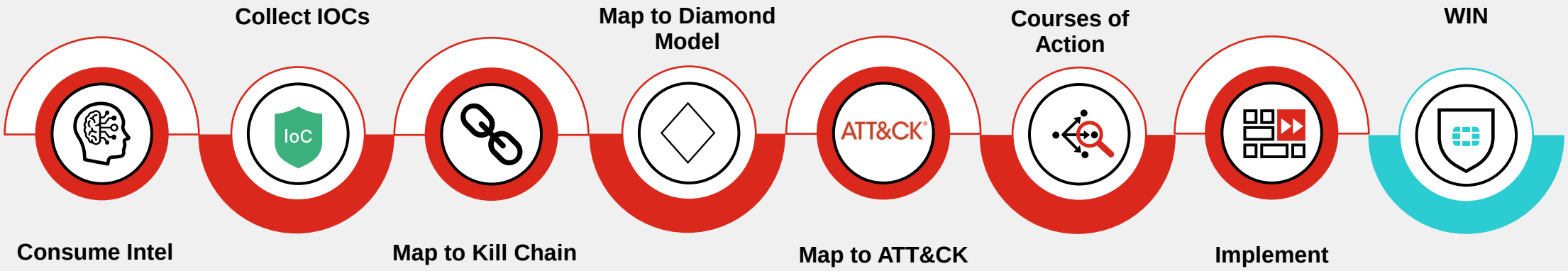
Implementing defenses in security tools – Detect 1

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

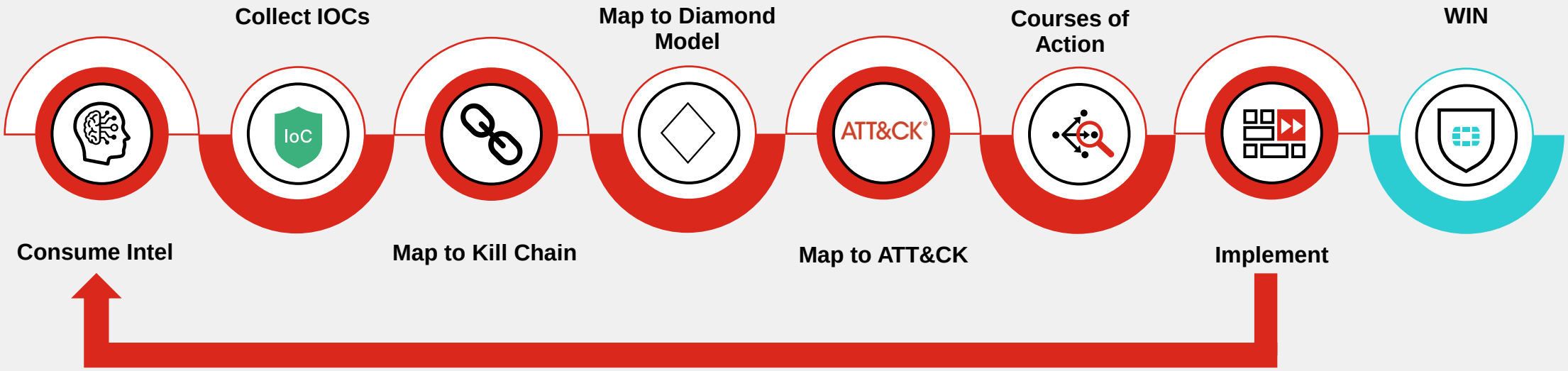
Implementing defenses in security tools – Detect 2, Deny, Disrupt

What?	Where?
Detect	
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
Deny	
Block powershell script execution	EDR / AV
Disrupt	
Block SSH brute force	Firewall / IPS

Conclusion



Conclusion



Thanks and Q ‘n’ A

Geri Revay
Security Researcher at FortiGuard Labs

- Twitter: @geri_revay


FORTINET