



OWASP

Open Web Application  
Security Project

# Testing for cyber resilience

**tools & techniques for adversary  
simulation and improved defense**

Adrian Ifrim & Teodor Cimpoesu, Deloitte

# Cyber Resilience in Focus

## Pillars of the Eurosystem's strategy in relation to FMIs

### 1. FMI readiness

- Overseers should work with FMIs to enhance their cyber posture, with a view to ensuring their safety and soundness against an increasingly sophisticated threat landscape.

### 2. Sector resilience

- Enhance and mature the collective cyber resilience capabilities of the Eurosystem's financial sector, through cross-border/cross-authority collaboration, information sharing and business continuity exercises.

### 3. Strategic regulator-industry engagement

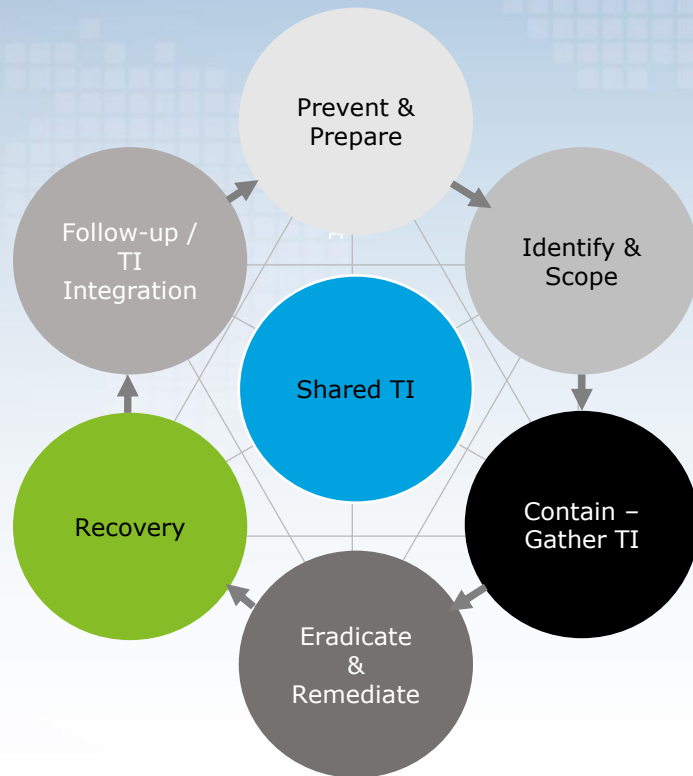
- Develop a joint strategic and Board level pan-European FMI regulator-industry forum, with a view to establishing trust and collaboration among participants, catalysing joint initiatives for enhancing sector capabilities and capacities, and increasing cyber awareness.

- **NIS Directive** – to bring cybersecurity capabilities the same level of development in EU
- **NIS Authority**, CSIRT teams
- **ECB initiative** - “European Red Team Testing Framework”
- **Sector resilience** – efficient sharing of CTI
- **Response and recovery** in a safe and efficient manner are key

Source: ECB.

Source: ECB, Cybercrime: from fiction to reality, IN FOCUS issue #2, 2017

# Intelligence Driven Defense



- Actual state of play: reactive response, whack-a-mole
- SIEM centric, wait for alert
- Own SOC or MSSP – deaf or overwhelmed
- C/TI – only external, LEAs, Vendors, no/little IOC level
- DFIR – Forensic Analysis vs. Threat Hunting (see Live IR)
- Recall: cyberspace favors offense

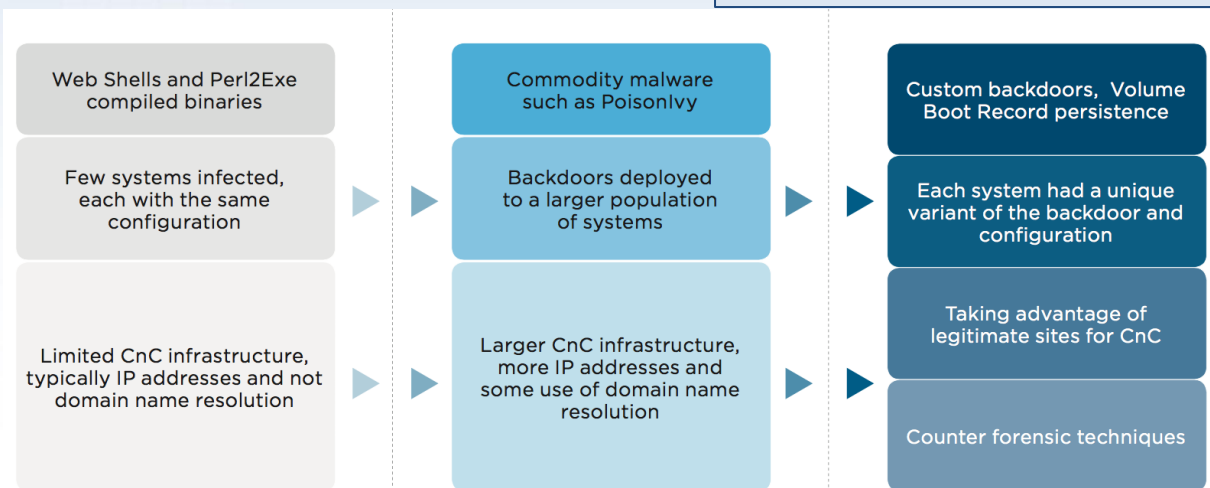
# What is now, before next

Instances of severe non-malware attacks grew throughout 2016. Over a **90-day period**, about **one-third** of organizations are likely to encounter **at least one severe, non-malware** attack (CB2016)

Crimeware-as-a-Service (**CaaS**) providers offer **hacking services** that allow individuals to gain access to computer systems or networks at a **reasonable price**. CaaS has allowed **less technically sophisticated** individuals to utilize crimeware for their **own illicit activities**. (Verizon)

While many organizations have been **establishing better testing methodologies** such as Red Teaming and Response Readiness Assessments to proactively understand their security posture, we suspect the **changing nature of attacks** has had a **significant effect**. (FEYE2017)

Instances of **non-malware attacks** leveraging **PowerShell** and Windows Management Instrumentation (**WMI**) grew throughout 2016. Such attacks **spiked** by more than 90% in the second quarter of this year (+93.2%) and have **stayed at escalated levels** since (CB2016)

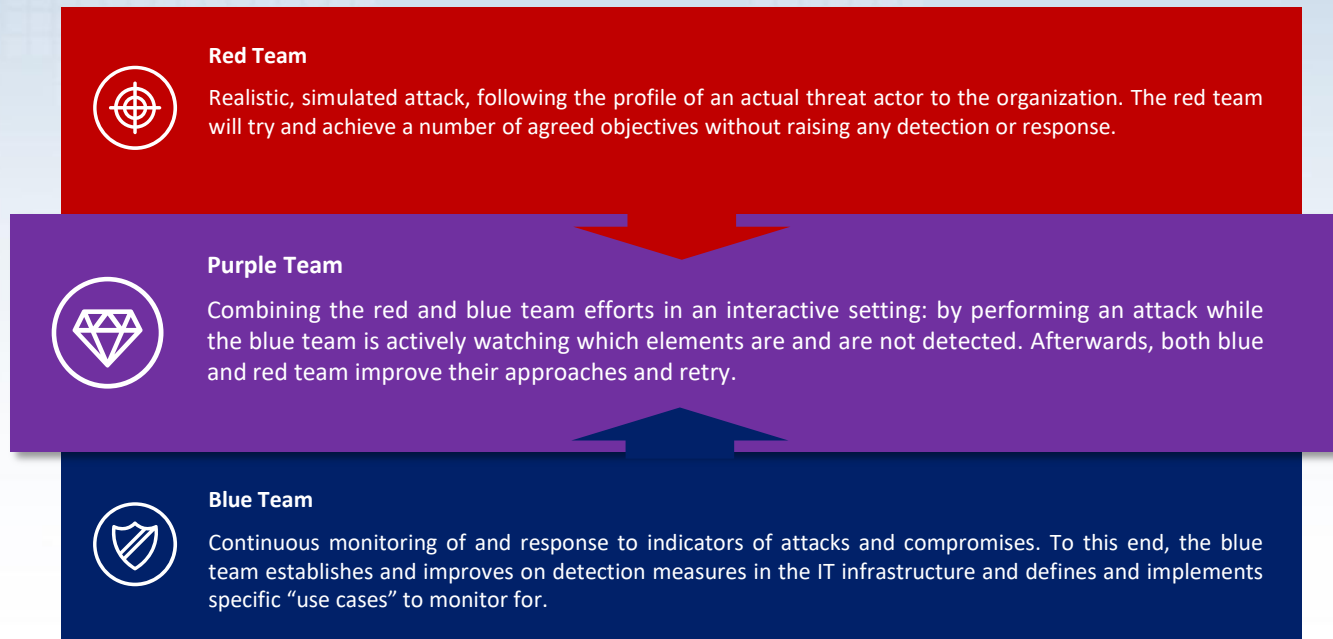


(fig.1) Increase in sophistication of financial attackers (FEYE M-Trends 2017)

# Approach: Red + Blue

## Leveraging the strengths of two essential IT security core teams

Most organizations nowadays leverage teams of simulated attackers (red team) and defenders (blue team) to test assumptions about the state of their IT security. Purple teaming effectively combines these two separate efforts into an integrated approach that allows for rapid, iterative improvement of the security posture. Focusing mainly on *cybersecurity*, continual feedback between both groups should broaden the blue team's knowledge base and rapidly improve their defense capabilities. This function is commonly referred to as the purple team (red and blue mixed together).



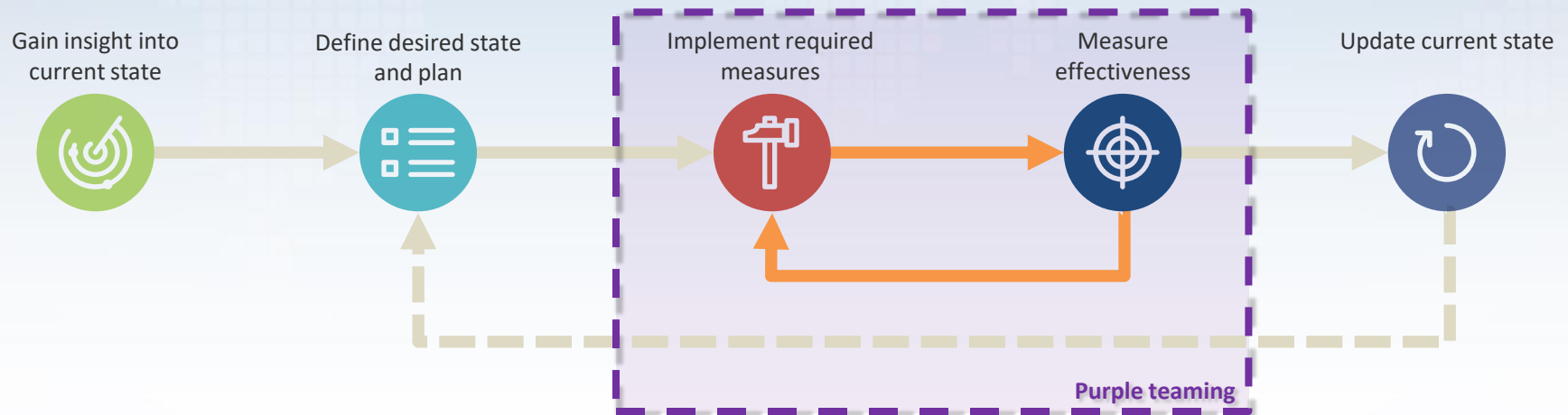


# Purple teaming as a build-up for cyber resilience

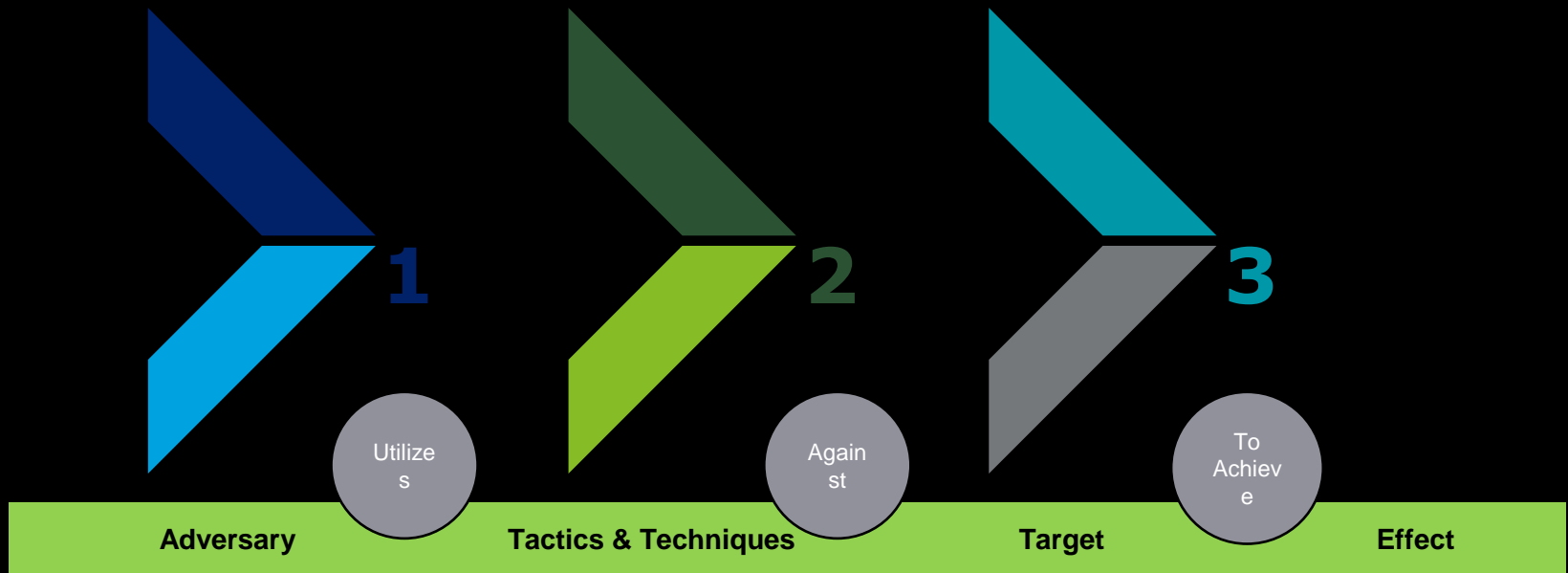
Measuring your progress during (large) security transformations

- Purple teaming is a perfect tool to measure progress during multi-year security transformation projects. By leveraging regular purple teaming engagements, recently implemented measures can be tested for effectiveness in a very targeted way. A change in threat landscape will automatically be covered as well, since any purple team engagement will use up-to-date threat intelligence and knowledge about the current threats to the organization.

## Overall process for security transformations



# Threat Modeling Methodology



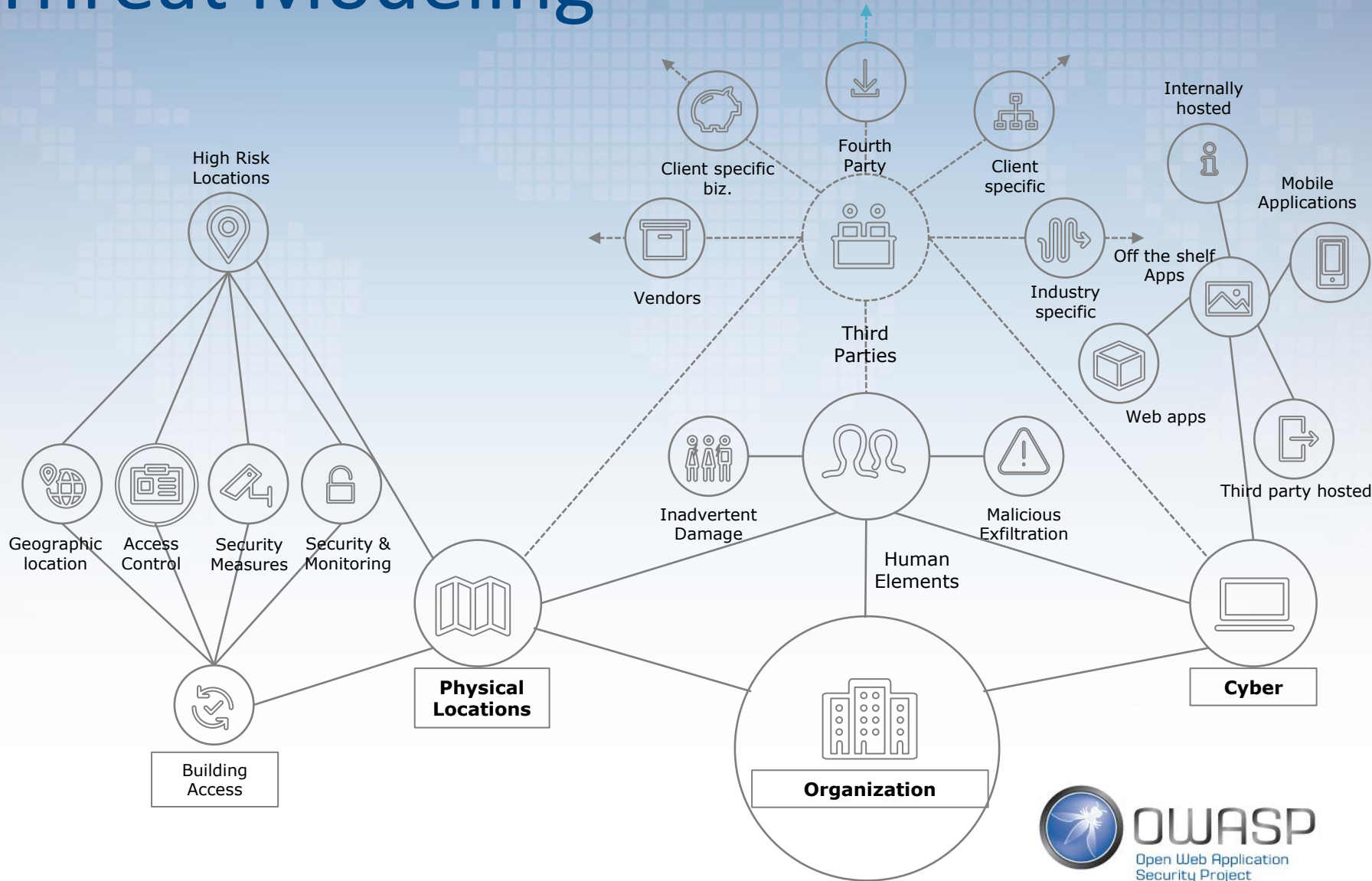
Who conducted the attack/may conduct the attack?

What method was used to conduct the attack?  
How was it implemented?

What specifically was targeted in the attack?

What happened as a result of the attack?

# Threat Modeling





# Mitre ATT&CK

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials			Credential Dumping	Account enumeration	Application deployment software Exploitation of Vulnerability Logon scripts Pass the hash Pass the ticket Peer connections	Command Line	Commonly used port Comm through removable media Custom application layer protocol Custom encryption cipher Data obfuscation Fallback channels Multiband comm Multilayer encryption Peer connections Standard app layer protocol Standard encryption cipher	Automated or scripted exfiltration Data compressed Data encrypted Data size limits Data staged Exfil over C2 channel Exfil over alternate channel to C2 network Exfil over other network medium Exfil over physical medium From local system From network resource From removable media Scheduled transfer
Accessibility Features	AddMonitor	Binary Padding DLL Side-Loading Disabling Security Tools File System Logical Offsets Process Hollowing Rootkit		File system enumeration		Local network connection enumeration		
DLL Search Order Hijack	Edit Default File Handlers	New Service	Network Sniffing	Local networking enumeration	Remote Desktop Protocol	Windows management instrumentation	Windows remote management	
Path Interception	Scheduled Task	Service File Permission Weakness	User Interaction	Operating system enumeration	Owner/User enumeration	Remote Services Replication through removable media Shared webroot Taint shared content Windows admin shares		
Shortcut Modification	Web shell	Indicator blocking on host Indicator removal from tools Indicator removal from host Masquerading NTFS Extended Attributes Obfuscated Payload Rundll32 Scripting Software Packing Timestomp	Credential manipulation	Process enumeration	Security software enumeration			
BIOS	Bypass UAC DLL Injection			Service enumeration	Service enumeration			
Hypervisor Rootkit	Exploitation of Vulnerability			Window enumeration	Window enumeration			
Logon Scripts								
Master Boot Record								
Mod. Exist'g Service								
Registry Run Keys								
Serv. Reg. Perm. Weakness								
Windows Mgmt Instr. Event Subsc.								
Winlogon Helper DLL								

© 2015 The MITRE Corporation. All rights reserved.

Approved for Public Release; Distribution Unlimited. Case Number 15-1288

MITRE



# Exploitation - Attack

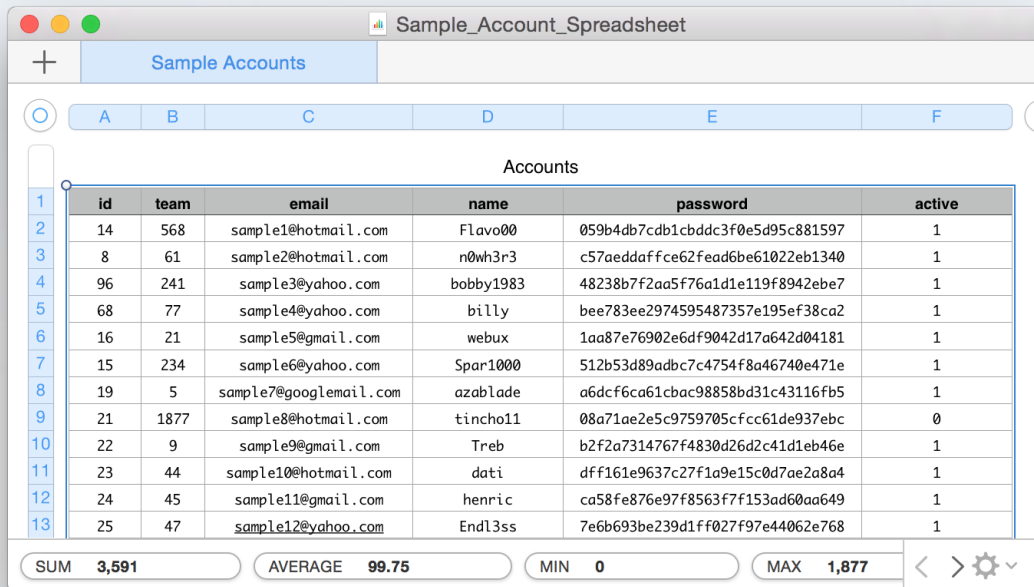
- Attacks
  - Macro-less files
    - PowerPoint
    - Excel
    - Word
  - obfuscated macros (old)
  - What works – secret sauce + some tips

# Moving Around - Attack

- Lateral movement w/powershell, WMIC
- Reflective PE/DLL injection
- PS + mimikatz.dll
- CobaltStrike beacon over SMB pipes
- Anti-forensics (e.g. invoke-phantom)

# Exfil / C&C

- C&C over WebDAV, DropBox, Twitter
- DNS/ICMP channels
- Domain fronting
- CobaltStrike beaconing



Sample Account Spreadsheet

	A	B	C	D	E	F
	Accounts					
	id	team	email	name	password	active
1						
2	14	568	sample1@hotmail.com	Flavo00	059b4db7cdb1cbddc3f0e5d95c881597	1
3	8	61	sample2@hotmail.com	n0wh3r3	c57aeddaffce62fead6be61022eb1340	1
4	96	241	sample3@yahoo.com	bobby1983	48238b7f2aa5f76a1d1e119f8942ebe7	1
5	68	77	sample4@yahoo.com	billy	bee783ee2974595487357e195ef38ca2	1
6	16	21	sample5@gmail.com	webux	1aa87e76902e6df9042d17a642d04181	1
7	15	234	sample6@yahoo.com	Spar1000	512b53d89adc7c4754f8a46740e471e	1
8	19	5	sample7@googlemail.com	azablade	a6dcf6ca61cbac98858bd31c43116fb5	1
9	21	1877	sample8@hotmail.com	tincho11	08a71ae2e5c9759705cfc61de937ebc	0
10	22	9	sample9@gmail.com	Treb	b2f2a7314767f4830d26d2c41d1eb46e	1
11	23	44	sample10@hotmail.com	dati	dff161e9637c27f1a9e15c0d7ae2a8a4	1
12	24	45	sample11@gmail.com	henric	ca58fe876e97f8563f7f153ad60aa649	1
13	25	47	sample12@yahoo.com	Endl3ss	7e6b693be239d1ff027f97e44062e768	1

SUM 3,591    AVERAGE 99.75    MIN 0    MAX 1,877

```
39.871636 -104.609451 Horsea
40.047236 -104.883651 Growlithe
40.025636 -104.630651 Onix
39.964036 -104.931851 Drowzee
40.106836 -104.927851 Vulpix
39.845036 -104.685851 Seel
39.951836 -104.835051 Hitmonlee
40.095436 -104.629851 Sheldler
40.023636 -104.966651 Psyduck
39.805236 -104.854651 Psyduck
39.808236 -104.857051 Poliwhg
39.903236 -104.921651 Lickitung
39.965836 -104.862451 Rhyhorn
40.133036 -104.746451 Mewtwo
39.883036 -104.810651 Kabuto
39.817036 -104.917051 Goldeen
39.879636 -104.877651 Vulpix
39.791236 -104.886851 Growlithe
40.045036 -104.635451 Hitmonlee
39.800436 -104.898651 Ekans
```

# Defenses

- Monitoring & logging 101
- Granular monitoring for PS/WMIC
- At endpoint level – Sysmon & EDR
- At network level – flows
- At SIEM level – quality uses cases
- At DFIR level – dynamic playbooks



# Framework for Gap Analysis

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features	Binary Padding	File and Directory Discovery		Application Deployment Software	Command-Line	Data Staged	Data Encrypted	Custom Command and Control Protocol	
Apprent DLLs	Code Signing		Local Network Configuration Discovery		Execution through API	Data from Local System	Data Transfer Size Limits		Custom Cryptographic Protocol
Local Port Monitor	Component Firmware	Local Network Connections Discovery		Exploitation of Vulnerability	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Obfuscation		
New Service	DLL Side-Loading		Credentials in Files	Logon Scripts	PowerShell	Exfiltration Over Command and Control Channel		Fallback Channels	
		Path Interception		Pass the Hash	Process Hollowing	Data from Removable Media			
Scheduled Task	File Deletion	Network Sniffing	Pass the Ticket	Regsvcs/Regasm	Email Collection	Multi-Stage Channels			
File System Permissions Weakness	File System Logical Drifts	Two-Factor Authentication Interception	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multiband Communication		
Service Registry Permission Weakness	Indicator Blocking		Remote File Copy	Remote Services	Screen Capture	Exfiltration Over Other Physical Medium			
Web Shell	Exploitation of Vulnerability			Network Service Scanning	Scheduled Task	Audio Capture	Multilayer Encryption		
Basic Input/Output System	Bypass User Account Control			Peripheral Device Discovery	Scripting	Video Capture		Peer Connections	
	Bookmark	DLL Injection			Permissions Group Discovery	Service Execution	Scheduled Transfer	Remote File Copy	
Change Default File Association	Component Object Model Hijacking			Process Discovery	Windows Management Instrumentation		Standard Application Layer Protocol		
Component Firmware	Indicator Removal from Tools			Query Registry	Windows Admin Threats		Standard Cryptographic Protocol		
Hypervisor	Indicator Removal on Host			Security Software Discovery			Standard Non-Application Layer Protocol		
Logon Scripts	Initial LSP			System Information Discovery			Uncommonly Used Port		
Modify Existing Service	Masquerading			System Owner/User Discovery			Web Service		
Redundant Access	Modify Registry			System Service Discovery			Data Encoding		
Registry Run Keys/Start Folder	NTFS Extended Attributes			System Time Discovery					
Security Support Provider	Obfuscated Files or Information								
Shortcut Modification	Process Hollowing								
Window Management	Redundant Access								
Instrumentation Event Subscription	Regsvcs/Regasm								
Winlogon Helper DLL	Regsvr								
Netsh helper DLL	Regsvr								
Authentication Package	Scout								
External Remote Services	Rundll32								
	Scripting								
	Software Packing								
	Timestamp								
	MSBuild								
	Network Share Removal								
	Install Root Certificate								

This notional depiction shows how an organization would use the MITRE ATT&CK framework to show defensive gaps against adversary activity within their network.

- Shows a high confidence in the detection or defense of an adversary
- Shows a medium confidence in the detection or defense of an adversary
- Shows no confidence, visibility, or blocking capability of an adversary



# GDPR Context

## Requirements

- **Enhanced Notification** - The Data Protection Authority (DPA) must be informed within **72 hours** of the discovery of a ‘serious’ incident, affected consumers must also be notified without delay
- **Detailed Reporting** - Companies are required to document all aspects of data breach – what happened, what steps they took to fix it, remediation strategies

**“In light of the tight timescales for reporting a breach - it is important to have robust breach detection, *investigation* and *internal reporting* procedures in place”**

**-- UK INFORMATION COMMISSIONERS OFFICE**

*Preparing for the GDPR, 12 steps to take now, 14/3/2016*

*<https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/>*

# GDPR Context

## Challenges with Breach Notification

- **Lack of preparation:**
  - ✓ Cross-functional planning and preparedness is key to success
  - ✓ What processes can improve an organization's cyber resilience?
- **Lack of proven response – Audit and Accountability**
  - ✓ Tracking of critical data throughout the lifecycle of an incident
  - ✓ Clear ownership & responsibility
- **Slow disclosure times – Time to notification:**
  - ✓ Recognizing a 'critical' incident
  - ✓ Building agile, responsive incident plans

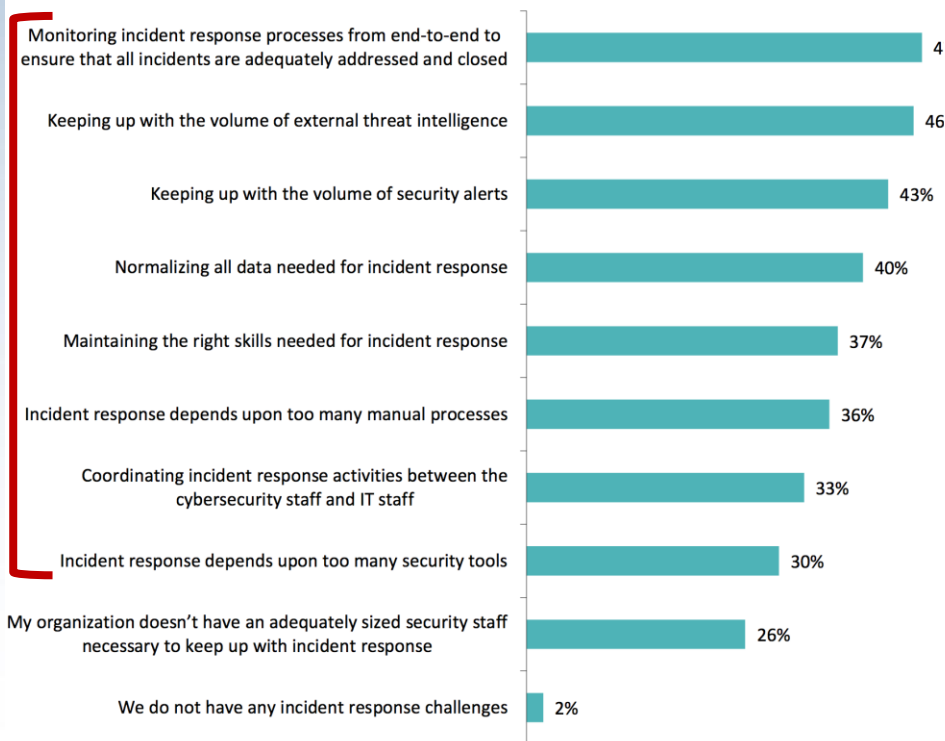
# About (Play | Run)books\*

- **A Playbook** – a plan of action, with roles and task responsibilities
- **A Runbook** – collection of tasks and processes, checklists
- Usually mapped on kill-chain/ATT&CK categories, and authored as SOPs
- ATT&CK related term would be **Analytics**
- SIEMs calls them **Use Cases**
- **Dynamic Playbooks** – scripted on automation and orchestration platforms, provide the agility, intelligence, and expertise needed to deal with complex attacks;
- Dynamic = can automatically **adapt to real-time incident conditions** (e.g. coordinate w/legal & HR, PR) and ensures repetitive, initial triage steps are complete before an analyst even opens the incident.

\* May be seen used interchangeably

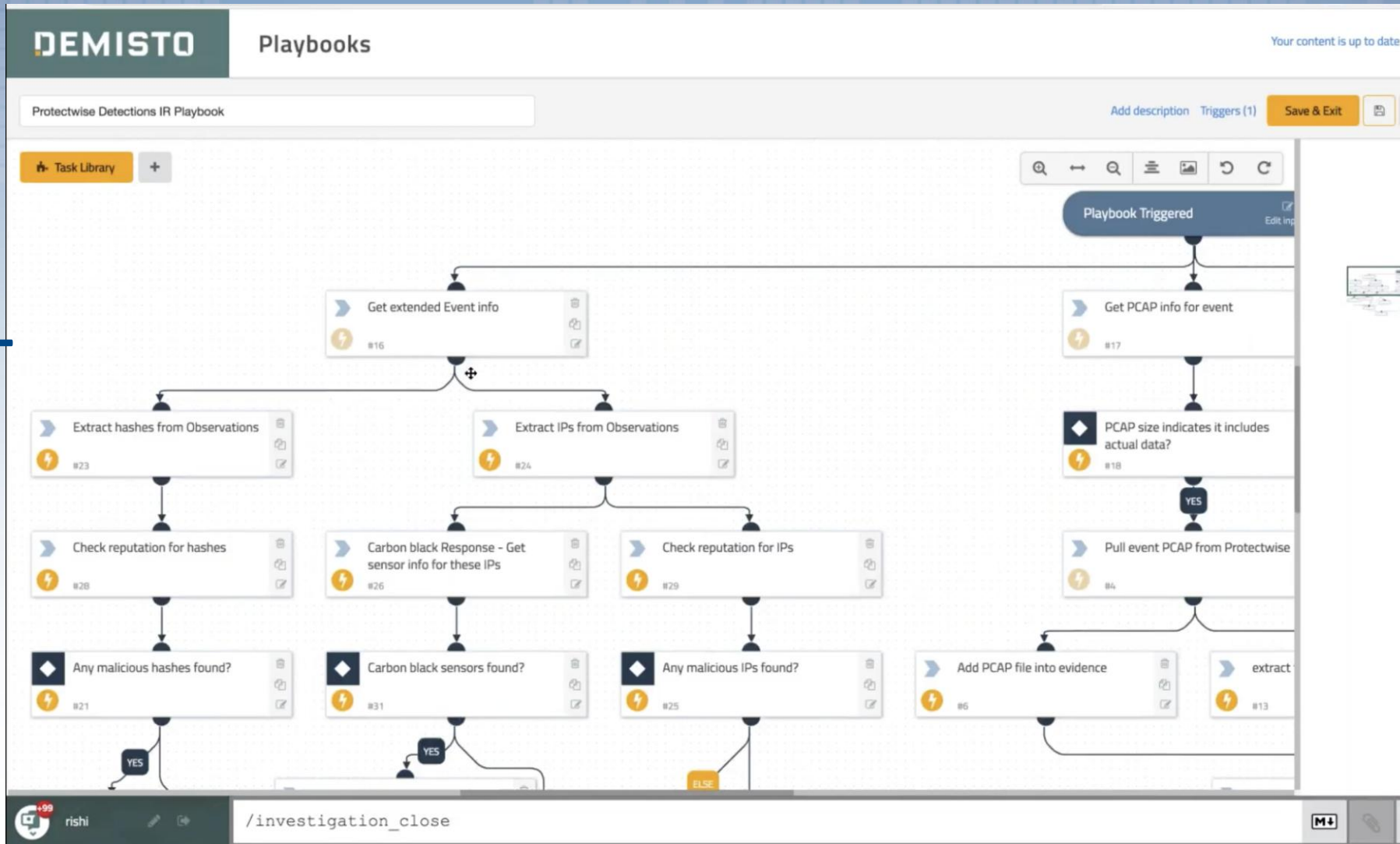
# IR Automation

In your opinion, what are the incident response challenges at your organization? (Percent of respondents, N=100, three responses accepted)



Source: Security Orchestration and Automation: Closing the Gap in Incident Response (ESG, 2016)

Example





# Thank you

~~Questions?~~

What will you do next?

@cteodor || in/cteodor

@unbaiat || in/adrianifrim

