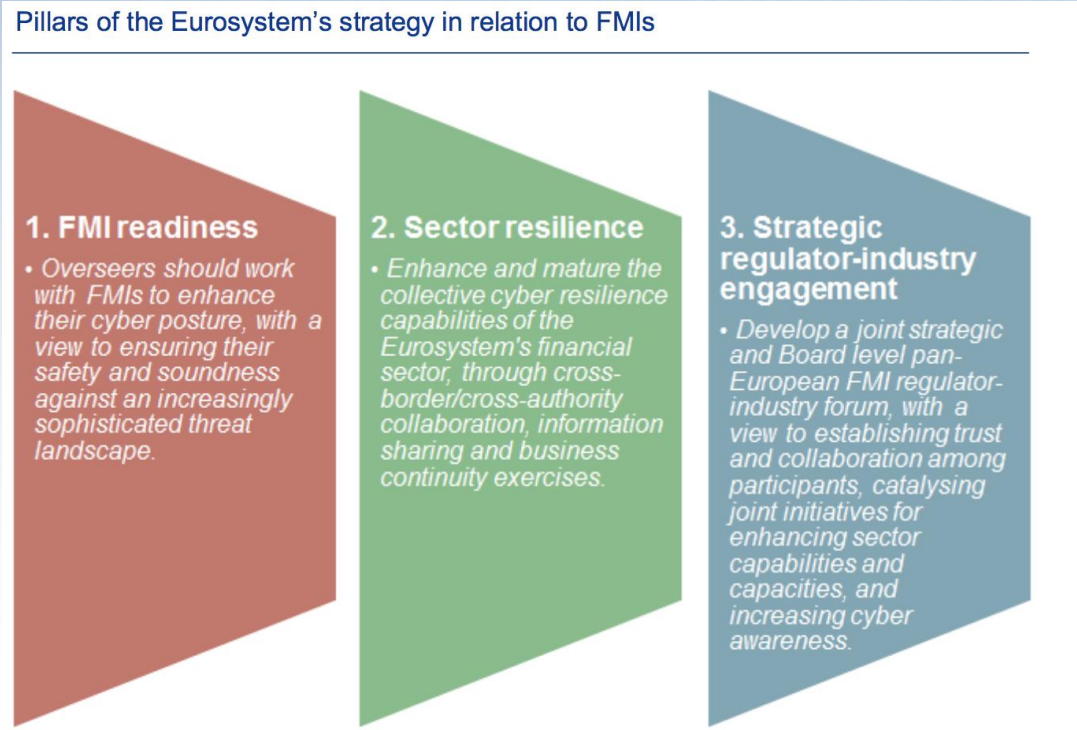

# Testing for cyber resilience

## tools & techniques for adversary simulation and improved defense

Adrian Ifrim & Teodor Cimpoesu, Deloitte

# Cyber Resilience in Focus



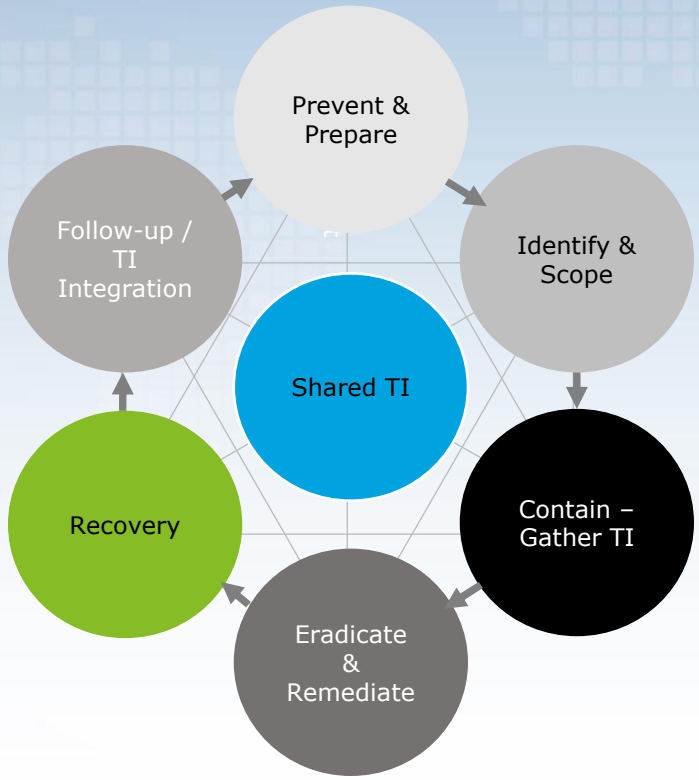

Source: ECB.

- **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, Cybercrime: from fiction to reality, IN FOCUS issue #2, 2017

OWASP
Open Web Application Security Project

# 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 devel
- DFIR – Forensic Analysis vs. Threat Hunting (see Live IR)
- Recall: cyberspace favors offense

OWASP
Open Web Application Security Project

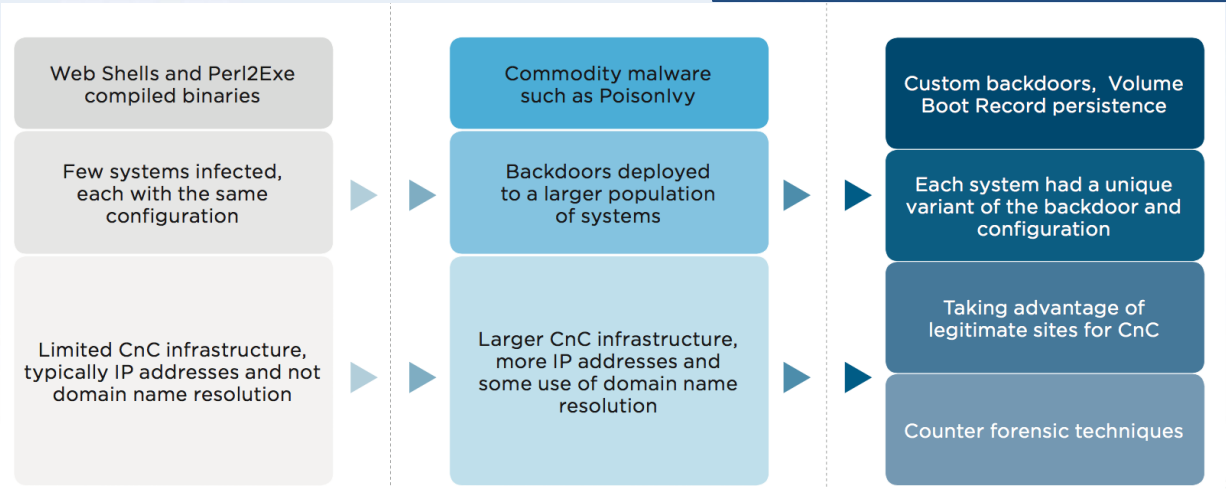
# What is now, before next

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)

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)

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)

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)

OWASP
Open Web Application Security Project

# 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 cyber*security*, 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).

**Red Team**

Realistic, simulated attack, following the profile of an actual threat actor to the organization. The red team will try and achieve a number of agreed objectives without raising any detection or response.

**Purple Team**

Combining the red and blue team efforts in an interactive setting: by performing an attack while the blue team is actively watching which elements are and are not detected. Afterwards, both blue and red team improve their approaches and retry.

**Blue Team**

Continuous monitoring of and response to indicators of attacks and compromises. To this end, the blue team establishes and improves on detection measures in the IT infrastructure and defines and implements specific "use cases" to monitor for.

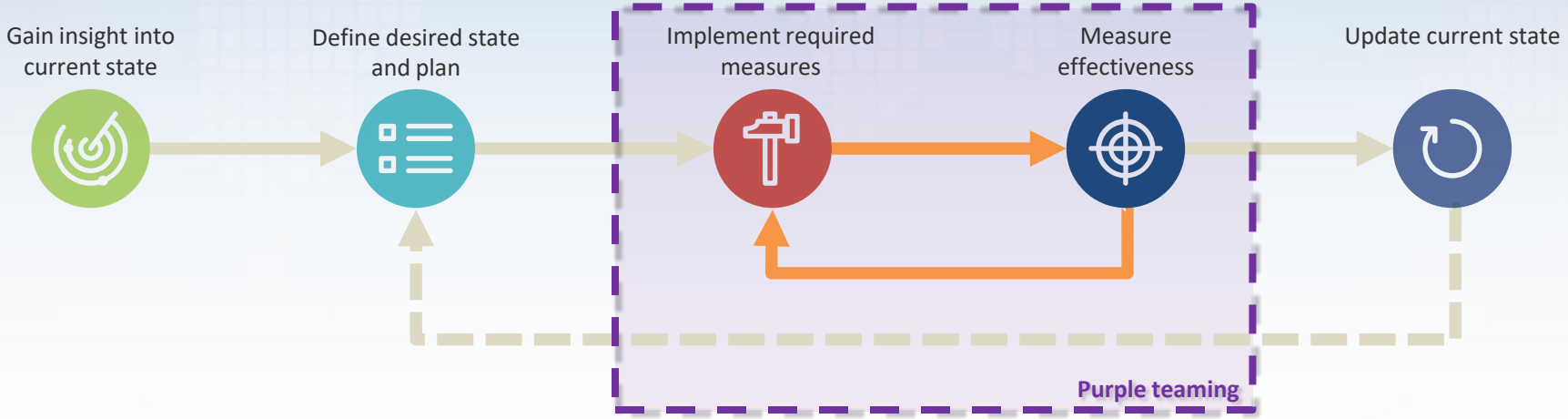
OWASP
Open Web Application Security Project

# Purple teaming as a build-up for cyber resilience

Measuring your progress during (large) security transformations

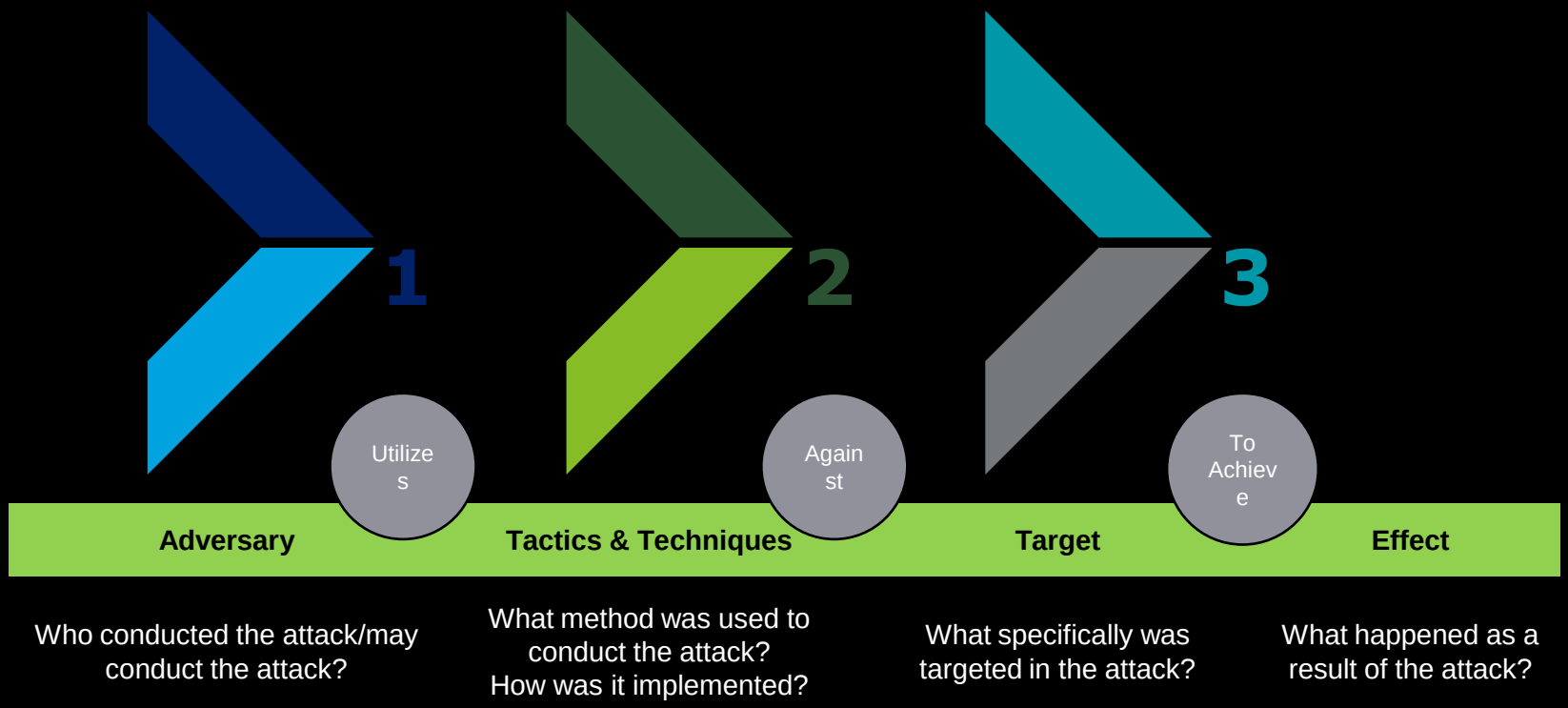
- Purple teaming is a perfect tool to measure progress during multi-year security transformation projects. By leveraging regular purple teaming engagements, recently implemented measures can be tested for effectiveness in a very targeted way. A change in threat landscape will automatically be covered 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**

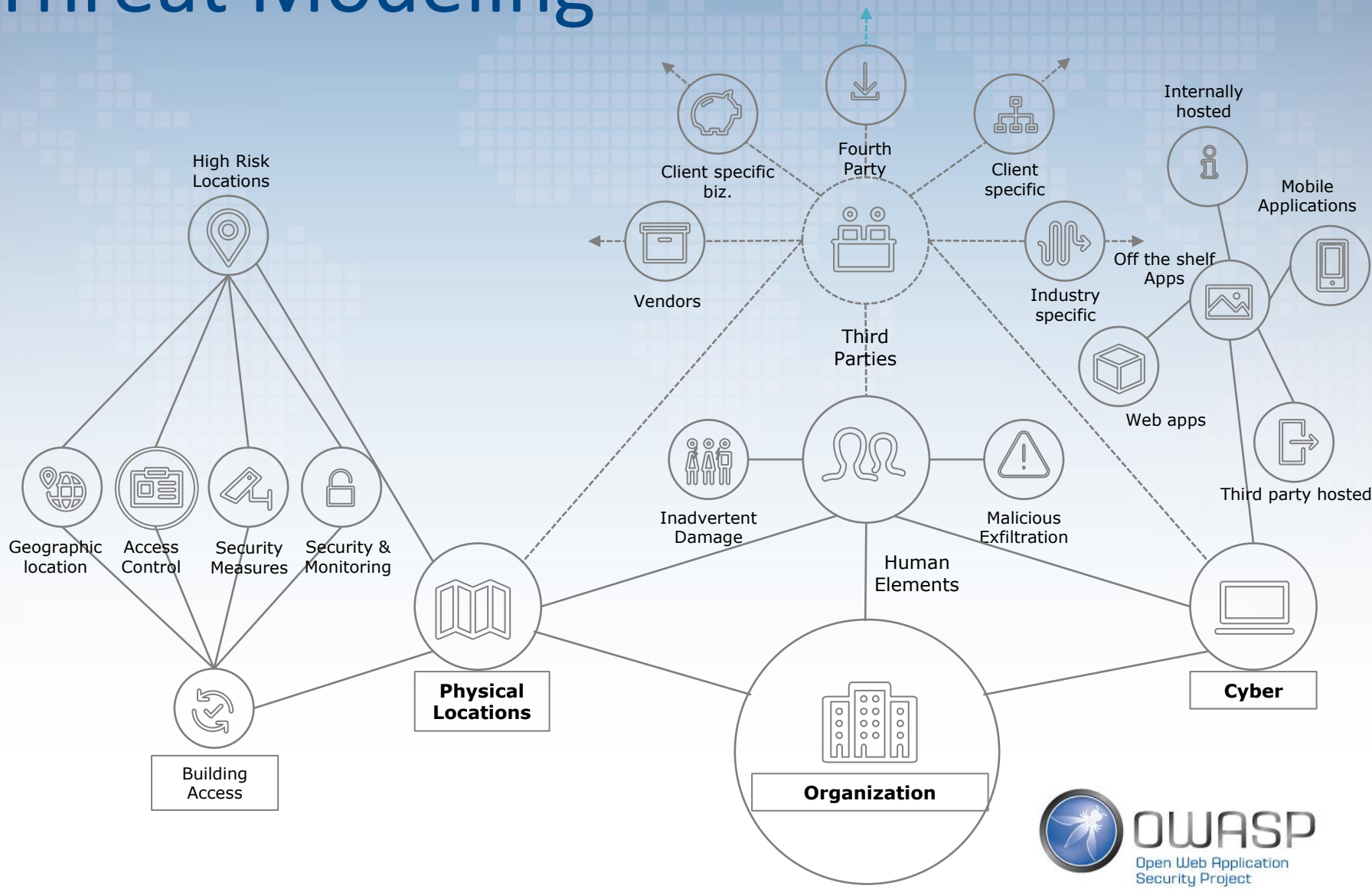



OWASP
Open Web Application Security Project

# Threat Modeling Methodology



# Threat Modeling




OWASP
Open Web Application Security Project

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





MITRE

OWASP
Open Web Application Security Project

# Exploitation - Attack

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

OWASP
Open Web Application Security Project

# 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-phant0m)

# Exfil / C&C

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

Sample_Account_Spreadsheet

Sample Accounts

Accounts

| | id | team | email | name | password | active |
|---|---|---|---|---|---|---|
| 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 | 512b53d89adbc7c4754f8a46740e471e | 1 |
| 8 | 19 | 5 | sample7@googlemail.com | azablade | a6dcf6ca61cbac98858bd31c43116fb5 | 1 |
| 9 | 21 | 1877 | sample8@hotmail.com | tincho11 | 08a71ae2e5c9759705cfcc61de937ebc | 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

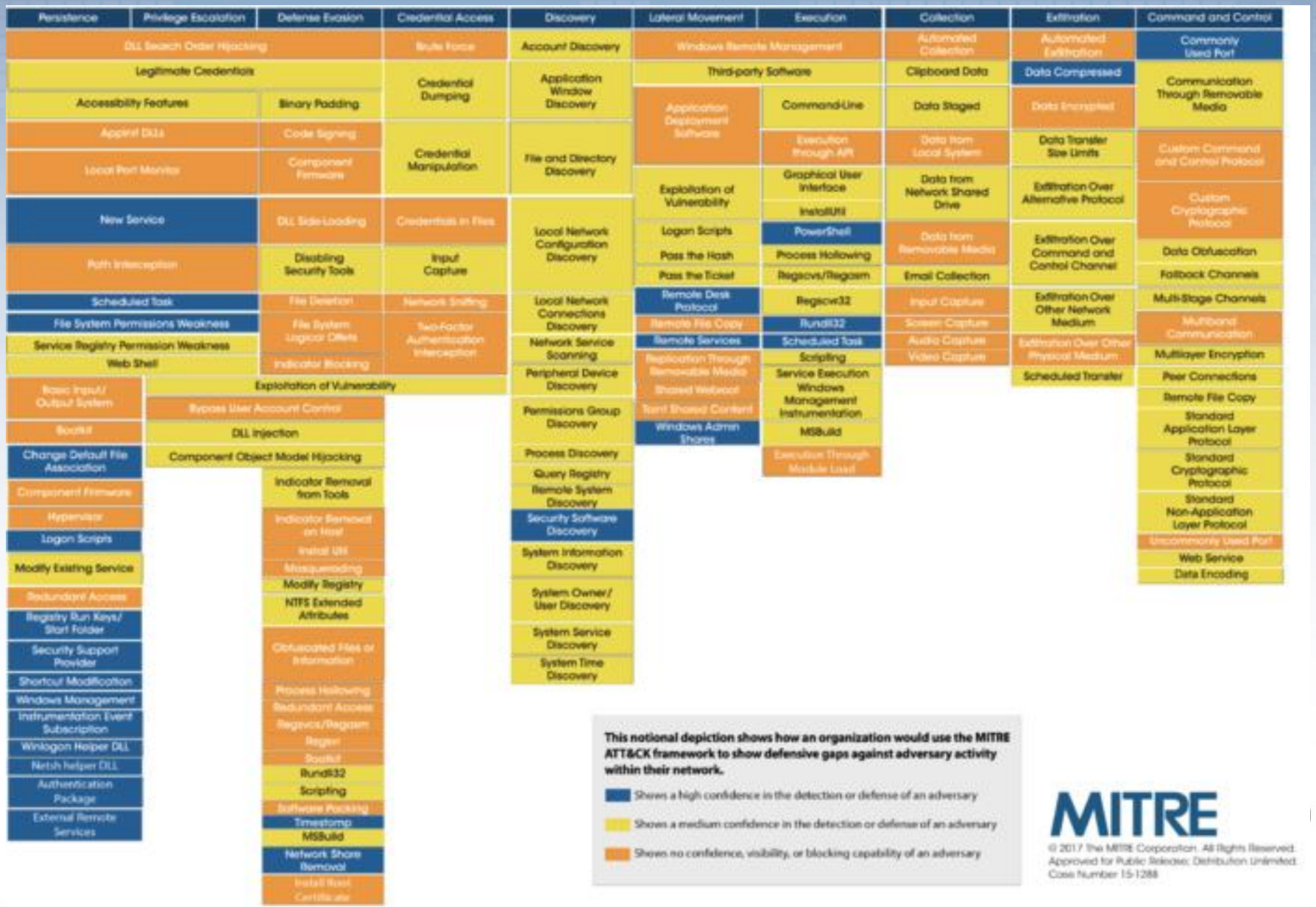
```
39.871636 -104.609451 Horsea
40.047236 -104.883651 Growlithe
40.025636 -104.630651 Onix
39.964036 -104.931851 Drowzee
40.106836 -104.927851 Vulpix
39.845036 -104.685851 Seel
39.951836 -104.835051 Hitmonlee
40.095436 -104.629851 Shellder
40.023636 -104.966651 Psyduck
39.805236 -104.854651 Psyduck
39.808236 -104.857051 Poliwag
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
```

OWASP
Open Web Application Security Project

# 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



# 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/*

OWASP
Open Web Application Security Project

# 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

OWASP
Open Web Application Security Project

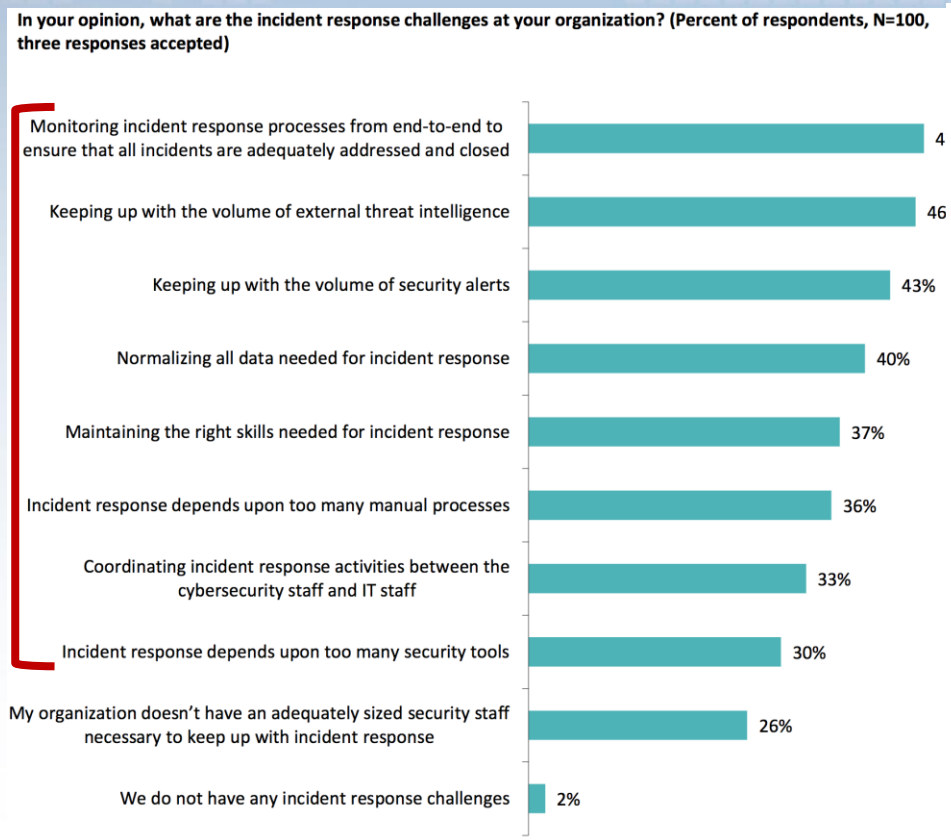
# About (Play|Run)books*

- **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

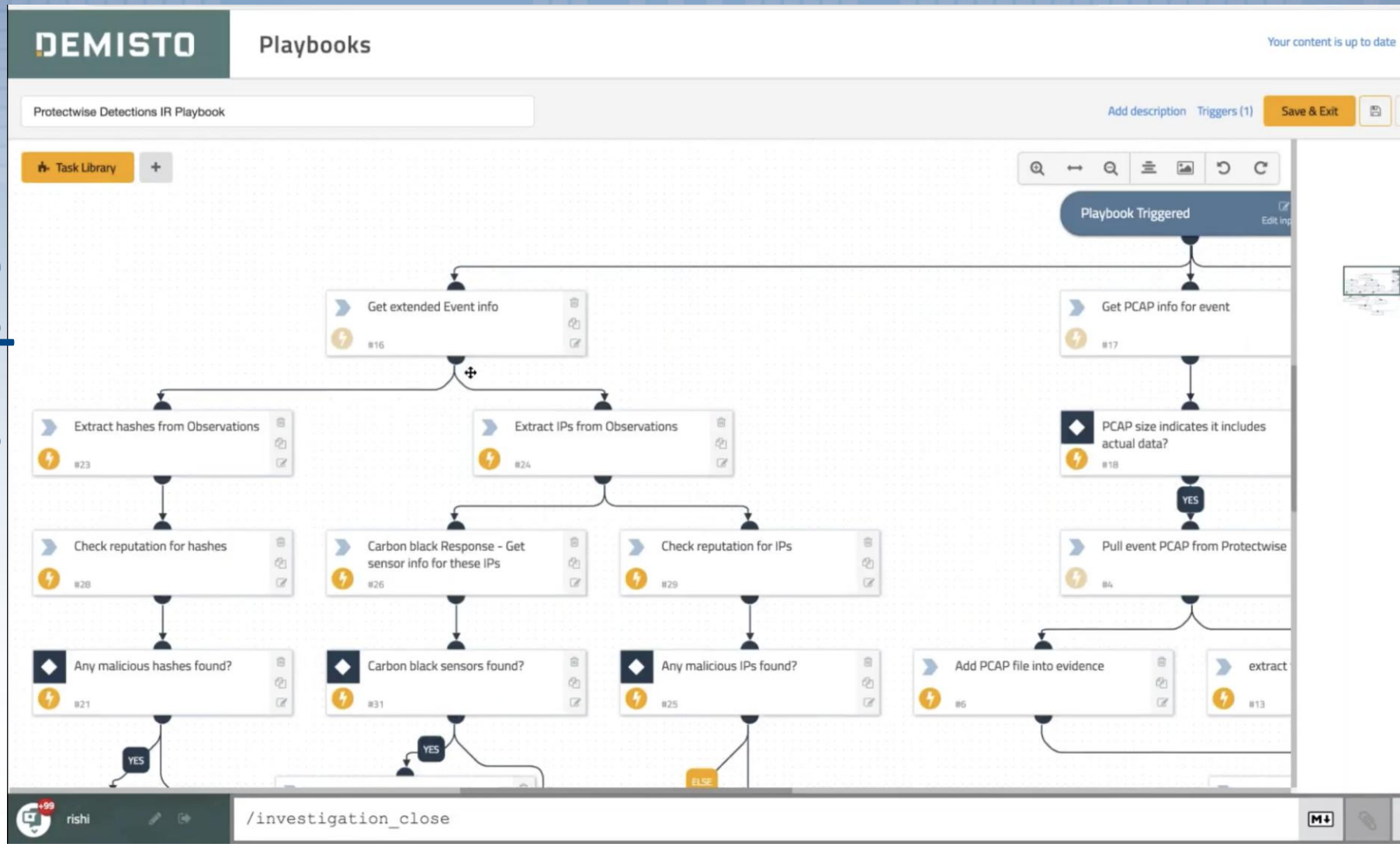




Source: Security Orchestration and Automation: Closing the Gap in Incident Response (ESG, 2016)

OWASP
Open Web Application Security Project

# Example




OWASP
Open Web Application Security Project

# Thank you

~~Questions?~~

What will you do next?

@cteodor || in/cteodor
@unbaiat || in/adrianifrim

OWASP
Open Web Application Security Project