Incident Handling
- Basic concepts and PICERL dissection -

October 24th, 2018

Cristian Zaharia
Gigi Bocaneala

Intro

Incident handling (IH): organized approach to addressing and managing the aftermath of a security breach or attack. IH refers to the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach

The goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.

An IH plan: policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs. Without an incident response plan in place, organizations may either not detect the attack in the first place, or not follow proper protocol to contain the threat and recover from it when a breach is detected.

IH Response Stages

Preparation	• Assembling a team and creating incident response procedures. The team must be educated to know their responsibilities
Identification	• Identify that a potential security incident has occurred.
Containment	• Prevent the security incident from becoming a bigger problem: limit the damage caused to systems and prevent any further damage from occurring.
Eradication	• Identify steps to mitigate the incident. Ensure there is a clean system ready to restore. Ex.: putting a antivirus protection in place or a firewall, reimage, etc.
Recovery	• When to bring the system back in to production and how long we monitor the system for any signs of abnormal activity.
Lessons learned	• Look at the big picture and see what happened and how could this be prevented?

Incident Handling – Phases

Preparation

- Policies
- Response Plan
- Communication Plan
- Systematic documentation
- Team assembly
- Tools
- Training

Identification

- **Reactive**: internal/client portal, e-mail
- **Proactive**: threat hunting, threat intelligence, user behavior analytics

Containment

- Which strategy you will use to contain the incident?
- Stop the bleeding
- Stop the attacker
- Engage the business owners
- Shut down the system or disconnect the network?
- Continue operations and monitor the activity?

Incident Handling – Phases

Eradication

- Removal and restoration of affected systems.
- In general, it's the longest phase
- Leads you to the resolution of the incident (or at least it should)

Recovery

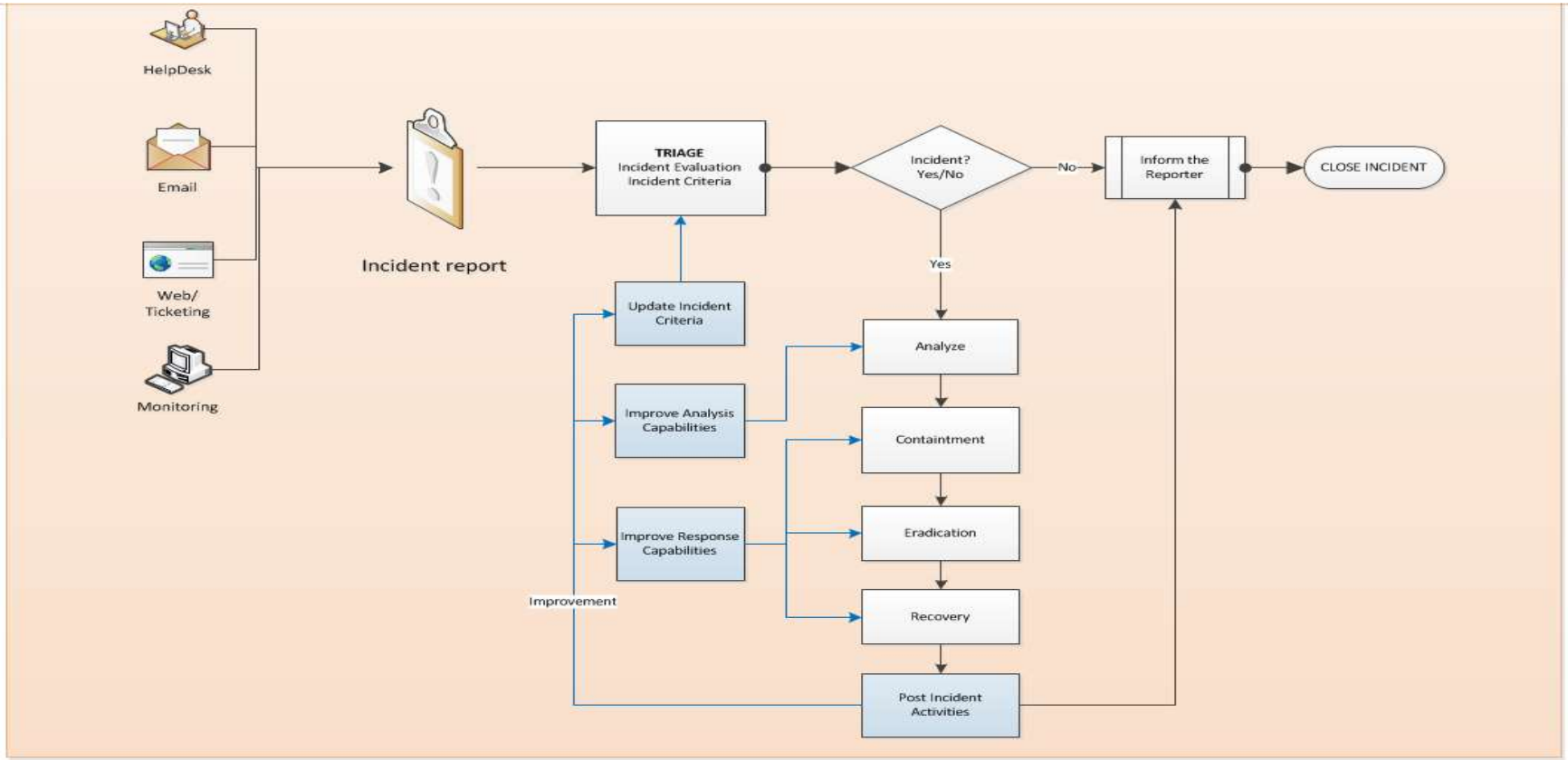
- Back in production
- Return to normal operational status
- Monitor it for a certain time period

Lessons learned

- Reflect and document what happened
- Identify improvements
- Write your final report

Incident Handling – Roles

Incident Handling - Workflows



Incident Handling - Tools & Resources

Ticketing portals:	SIEMs:	Vulnerability Management:	HIPS/HIDS	Enterprise AV
• DSW NG Portal • ServiceNow • Remedy • Archer	• Splunk / Splunk ES • QRadar • LogRhytm • ArcSight • RSA • Tibco Log Logic	• Qualys • Nessus	• CarbonBlack • RedCloak • FireEye HX • Tanium • Cylance	• Symantec • TrendMicro • McAfee

Other open source platforms and internal client tools

Case study #1 – Phishing
Hook, Line, and Sinker

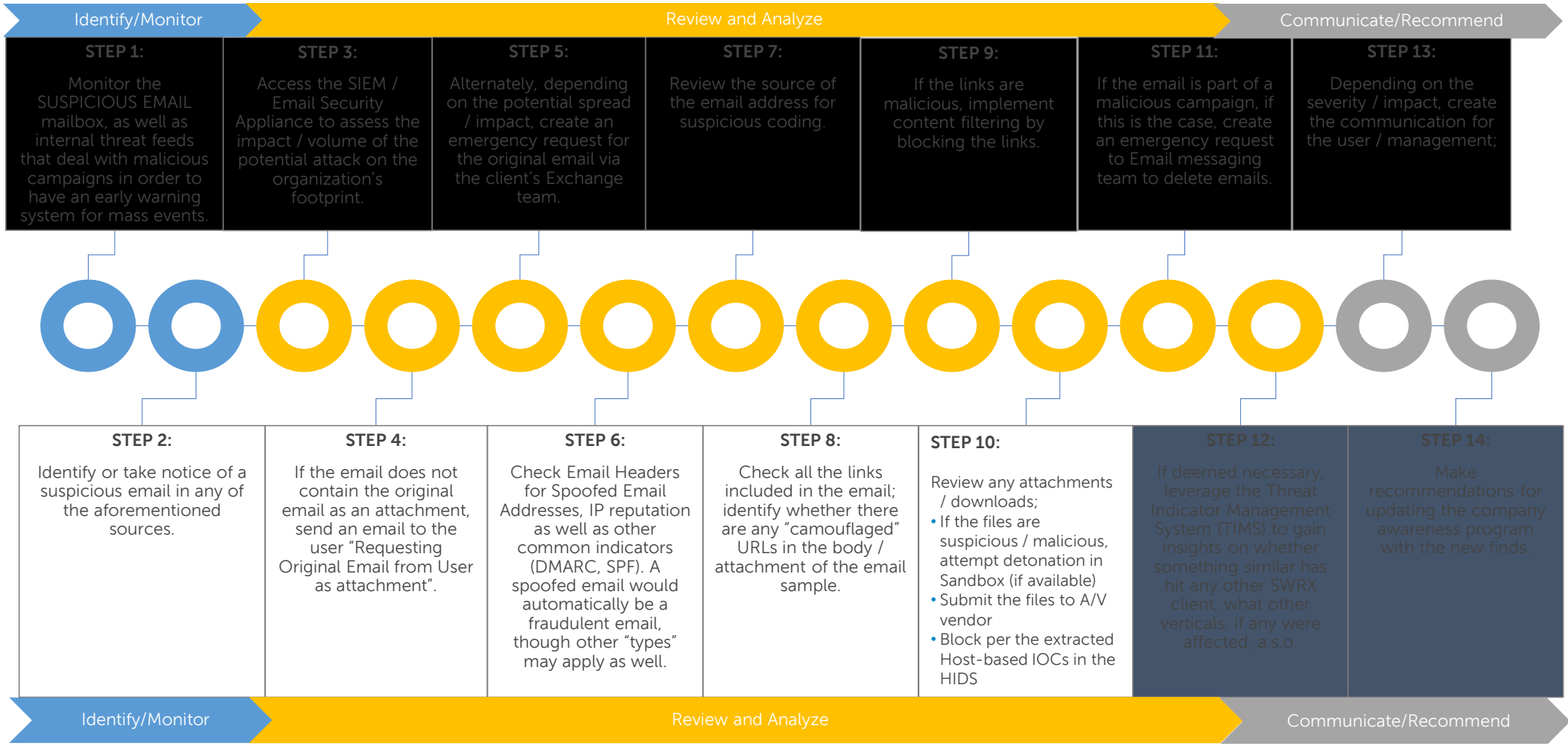
Intro:

- Is a mainstay of the SOC's activity
- One of the main vectors that are used by adversaries in their attempts to gain a foothold in the organization.
- operates at layer 8 – human layer
- The ingenuity of the malicious actors with regard to ways of making emails more attractive knows no boundaries.

Tools / resources used (samples):

- Sandboxes and toolkits: CASE, SIFT, Cuckoo, FireEye AX / MAS,
- Online Resources: VirusTotal Intelligence, PassiveTotal, MX Toolbox
- Content Filtering Solutions: BlueCoat, WebSense, Proofpoint
- A/V Solutions / Vendors: TrendMicro, McAfee, Symantec,
- SIEMs: Splunk, RSA SA, QRadar
- HIDS: CarbonBlack, RedCloak, McAfee HIPS

Case study #1 – Phishing Hook, Line, and Sinker



Case study #2 – Infected devices

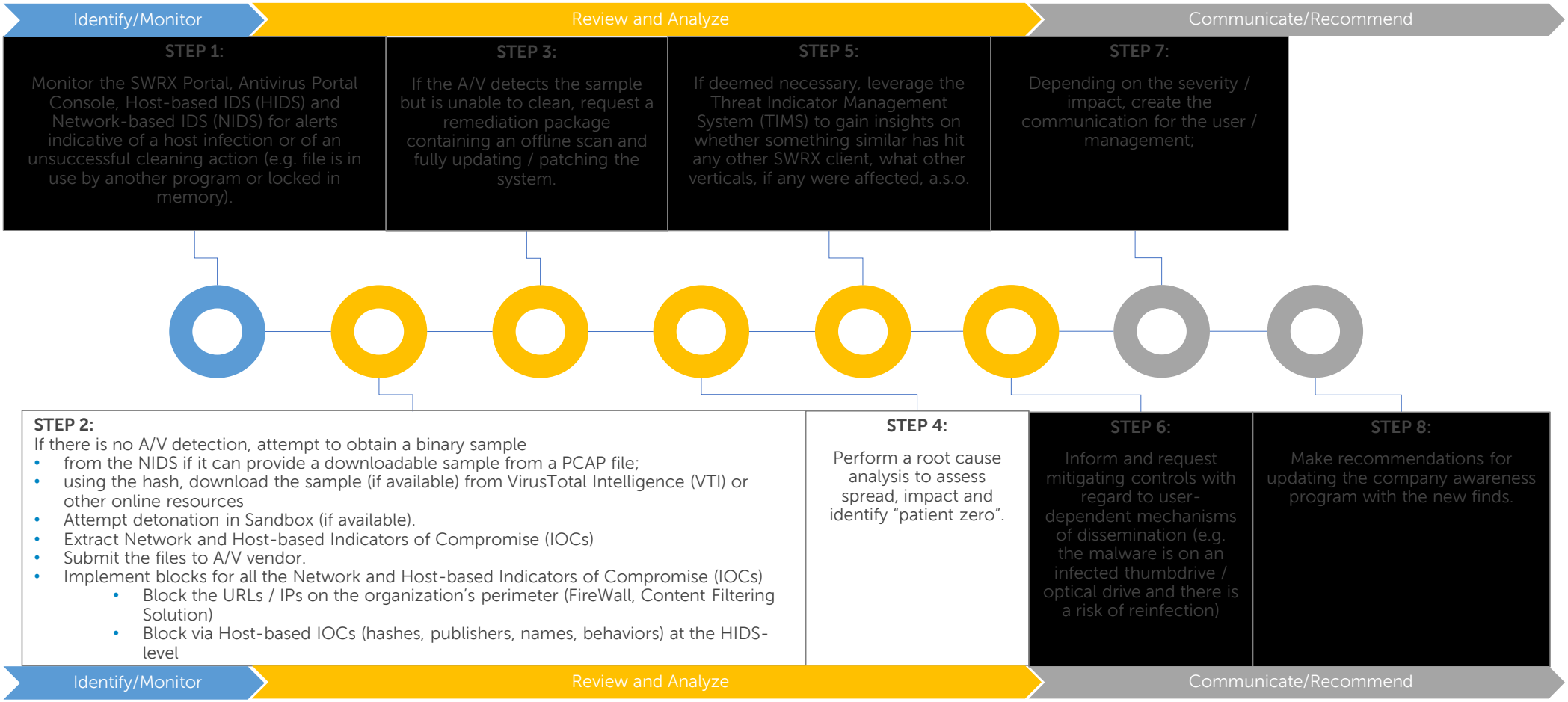
Intro:

- In an ideal world, the antivirus solution would clean infections for which there are detections in place.
- Often triggered when the client has an loose BYOD policy
- More challenging when seeing a C2 callback - host has already been compromised and the malicious payload attempts to "phone home"
- The most common situation is when the malware binary is detected (but not blocked) by the Network-based IDS (NIDS) and the A/V has no detection whatsoever.

Tools / resources used (samples):

- The SecureWorks Portal
- Sandboxes and toolkits: SIFT, Cuckoo, FireEye AX / MAS,
- Online Resources: VirusTotal Intelligence, PassiveTotal, MX Toolbox
- Content Filtering Solutions: BlueCoat, WebSense,
- A/V Solutions / Vendors: TrendMicro, McAfee, Symantec,
- SIEMs: Splunk, RSA SA, QRadar
- HIDS: CarbonBlack, RedCloak, McAfee HIPS

Case study #2 – Infected devices



Case study #3 – Compromised Accounts

Case study – IH procedure applied

Synopsis: A student obtained the authentication credentials of some of his class professors, being able to modify his grades. By doing this, not only he passes all the exams with high grades, but also gained some financial aid from the university.

Client expectations for the SOC team:

- find out the impact of this incident: how many professors' accounts have been compromised
- how many grades did he modify? Were these changes able to help the student in gaining some financial aids from the university?
- did he have any accomplices who had helped him?
- is this a practice among the students?
- a complete timeline of this incident

Case study – IH procedure applied #1

- Discussed with the client about who's in charge of handling this incident. Requiring all the log sources which could have any tracks about what happened. Agreeing on what steps should we follow and in which order.

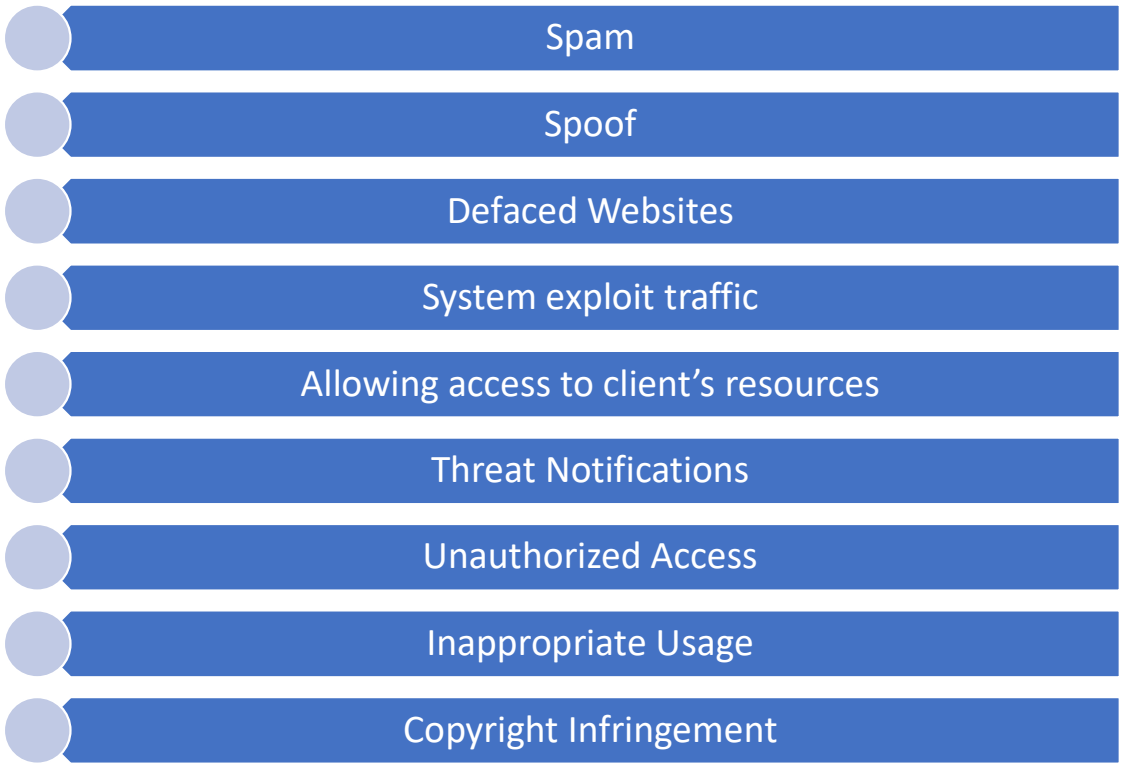
- First searches to identify how many accounts were implied, the duration of this unauthorized access and what was the impact for the student evolution.

- Locked all the accounts which were implied in this incident and changed the password for them.

Case study – IH procedure applied #2

- All the lab devices which were used by the professors were reimaged and the inputs devices were verified for hardware keyloggers.
- All the grades were changed to the original state. The student was notified about this incident and the state police was announced.
- Created an alert for some specific fields from the logs in order to be announced when some grades are changed

Other incident categories



Defense Approach - The Kill Chain

Intelligence-driven Computer Network Defense

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Continual Service Improvement Program

- Monthly Recommendations
- Part of the “Lesson Learned” phase
- The analyst with the most recommendations: Consultancy Demeanor Champion
- 900 recommendation during the last two years

Tier 3 – Advanced analysis and investigation

Tier 3 – Incident Response

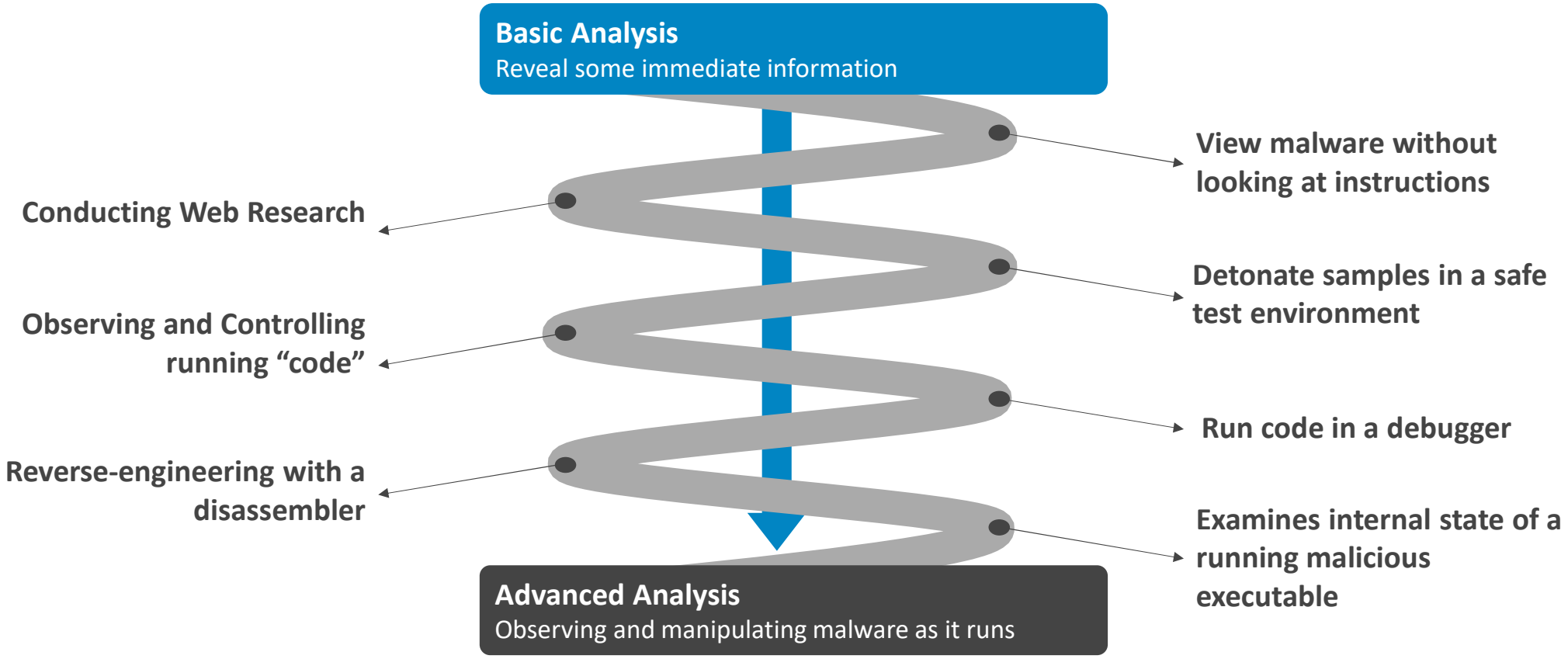
End to end analysis based on the following

Tier 3 – Threat Intelligence

Slide 20

Tier 3 – Reverse Engineering

Malware Analysis



Question?


THANK YOU!
EVERYDAYIDERP.TUMBLR.COM