NETWORK FORENSICS & INCIDENT RESPONSE

w/ Troy Wojewoda

About @author

Troy Wojewoda

Security Analyst/Consultant/Hunter/Tester @BHIS

Career Experience

HOST
FORENSICS
NETWORK

MALWARE ANALYST
(H|N)IDS
INCIDENT RESPONDER
SOC MANAGER
THREAT HUNTER
PENETRATION TESTING

Education/Certifications

- BS Computer Engineering & Computer Science (CNU)
- GSE, GRID, GNFA, GCFA, GCIH, GCIA, GREM, GAWN, GSEC (GOLD), CISSP

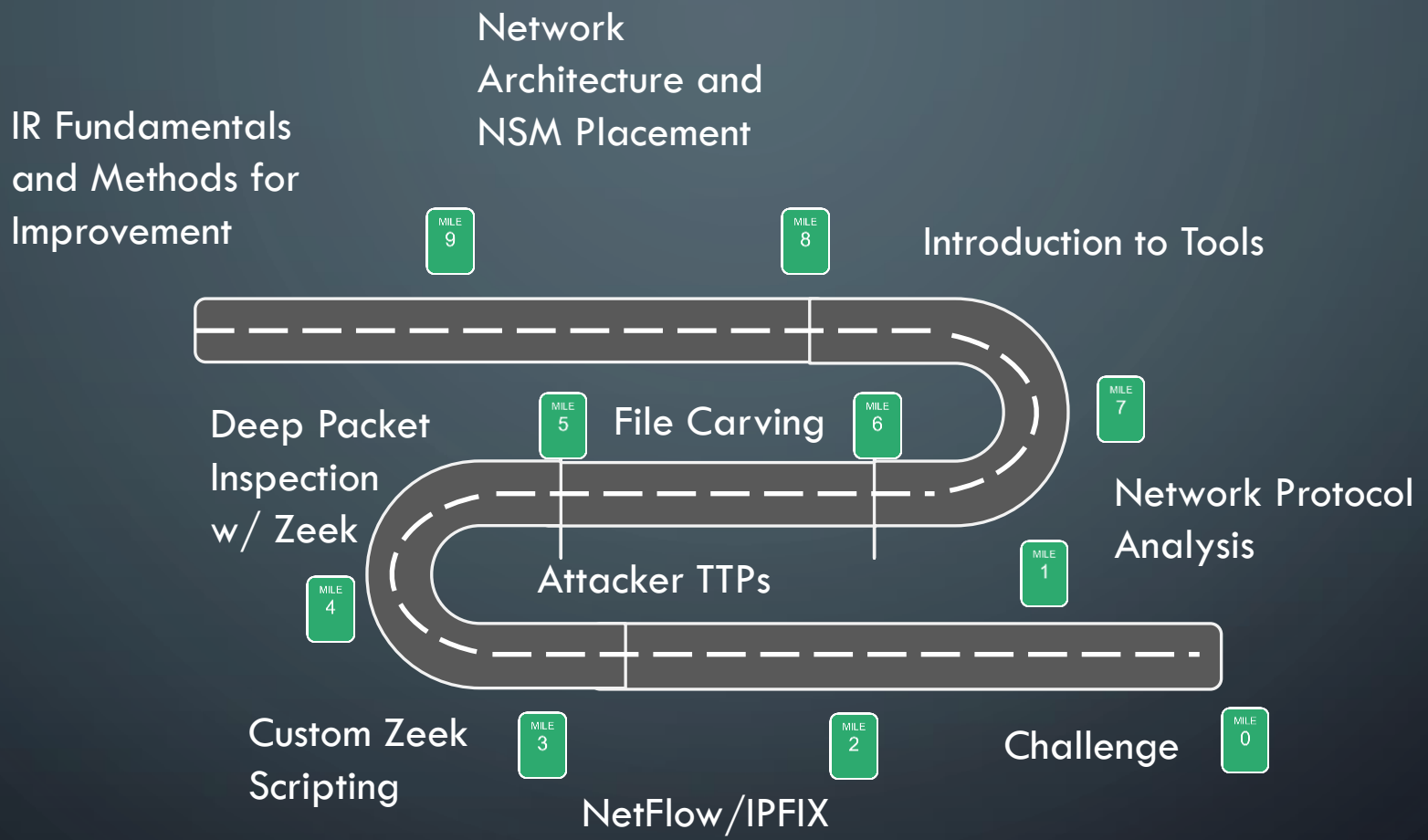
About @course

- Analyzing network packet captures with a variety of tools, techniques, and filtering options
- Extracting files and metadata from network packet captures
- Creating custom Zeek scripts to support incident response efforts
- Creating custom Zeek scripts for Zeek log enrichment
- Analyzing network flow data
- Real-world attack scenarios and techniques for response
- Methods to aid investigators when dealing with the challenges of encrypted communications
- A culminating CTF challenge combining course objectives

Day 1 – DFIR Network Forensics

- Mile markers denote progress
  - Increase: as we travel from South to North
  - Increase: as we travel from West to East
- Course will use Mile Markers as we traverse the day's material

Roadmap



DFIR Basics

- Time
- Collection
- Prioritization
- Response Steps
- Forensic Analysis
- Feedback Loop
- DFIR != eDiscovery

DFIR Basics – Time

Measurements | Metrics

t_0 = Incident Start

tr = time to respond

tc = time to contain

tR = time to remediate/recover

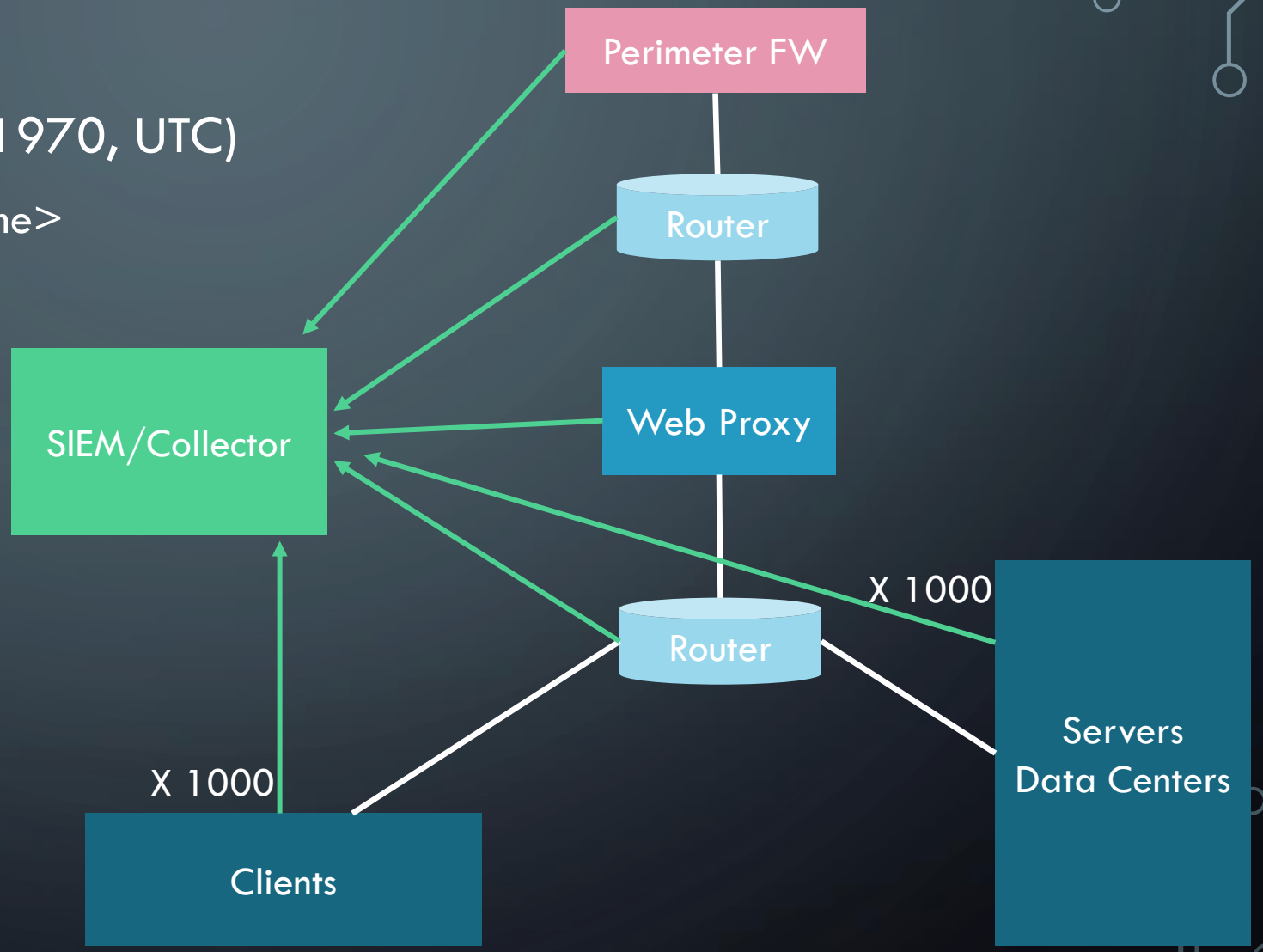
Synchronization

- Network Time Protocol (NTP)
- Trusted source
- Required for proper correlation

"You're not thinking 4th dimensionally, Marty!"

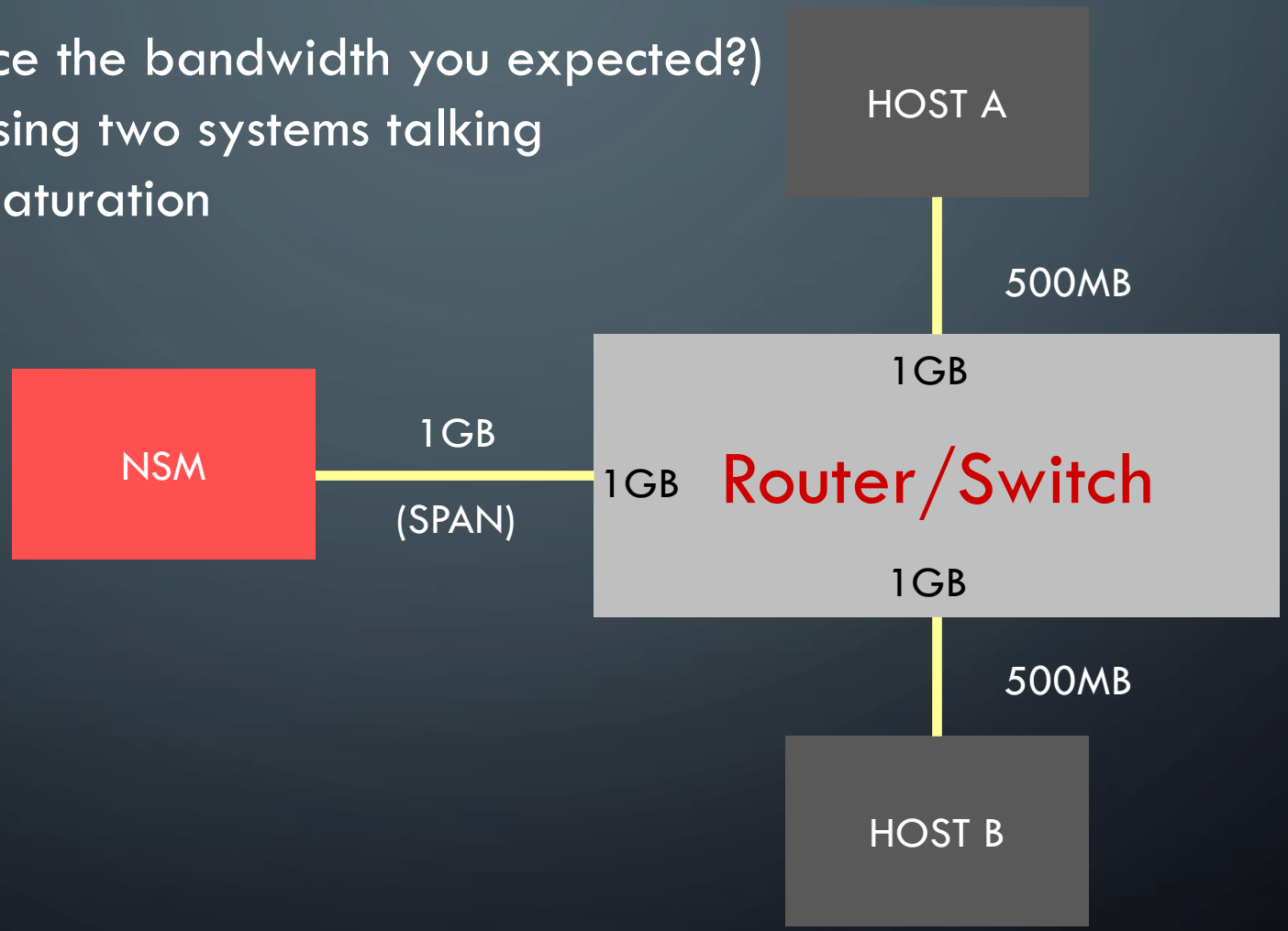
DFIR Basics – Time Formats

- Unix Epoch (t=0000 Jan 1, 1970, UTC)
  - Convert: date –d @<unix_time>
- GMT and UTC
- Zulu (0000 – 2359)
- ET – EST – EDT



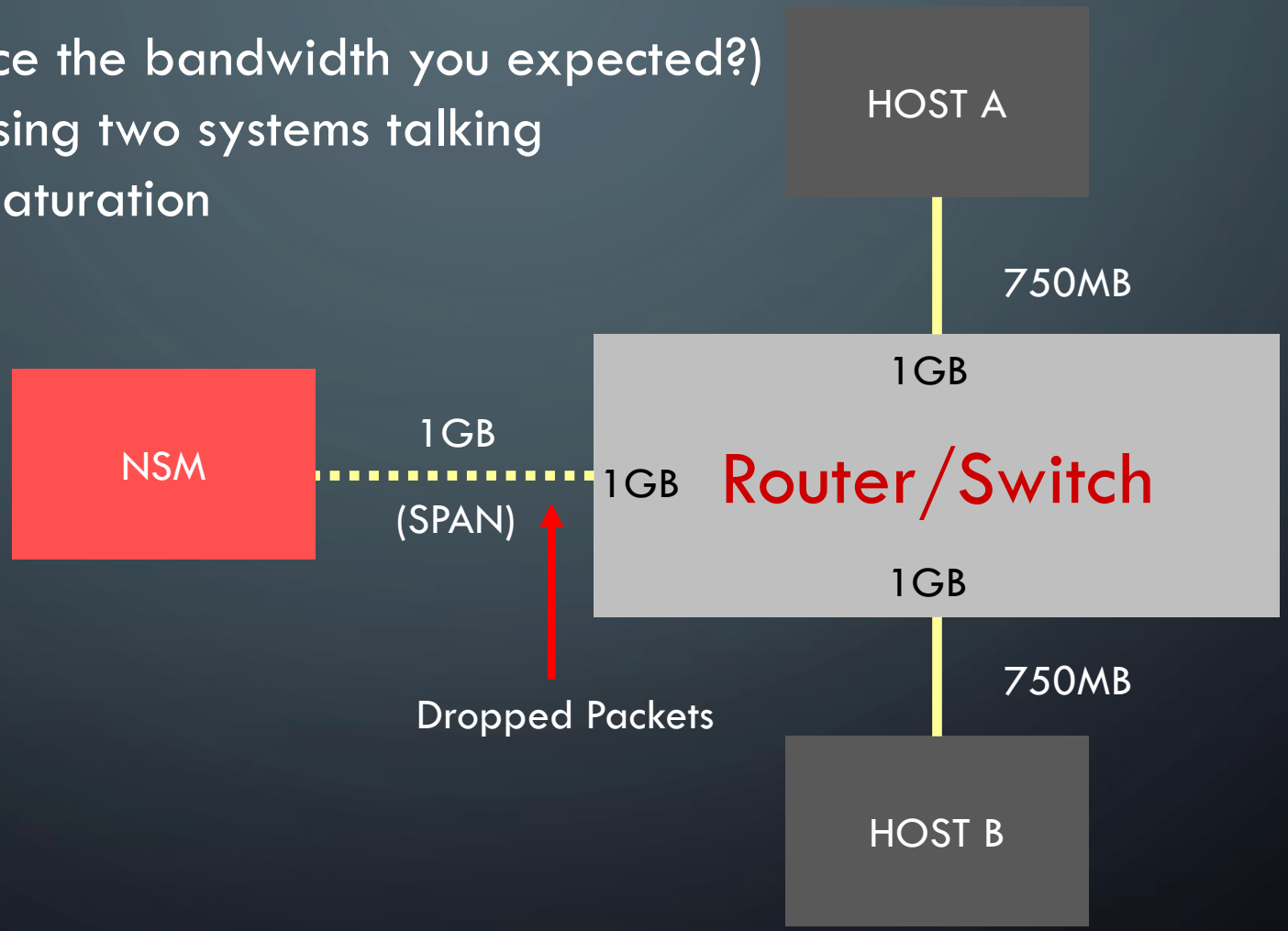
DFIR Basics – Collection

Full Duplex topic (twice the bandwidth you expected?)
- One system processing two systems talking
- SPAN/Port Mirror saturation



DFIR Basics – Collection

Full Duplex topic (twice the bandwidth you expected?)
- One system processing two systems talking
- SPAN/Port Mirror saturation



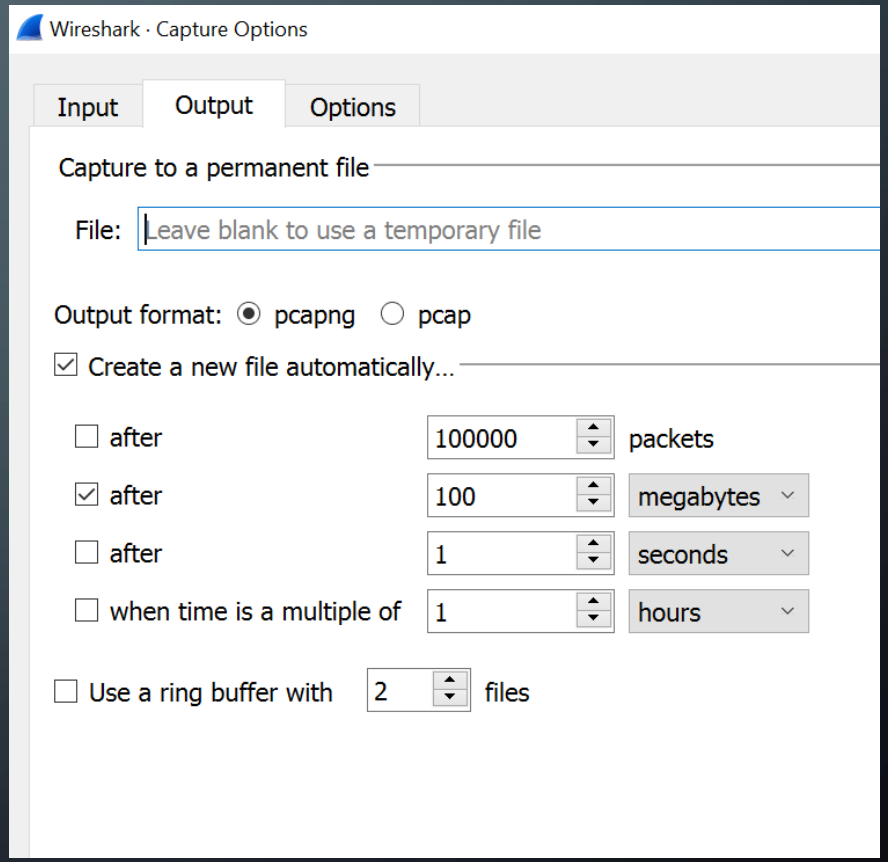
DFIR Basics – Collection

Tools to aid us along the way…

- Wireshark/Tshark
- Tcpdump
- Zeek
- Commercial tools

DFIR Basics – Collection

- Capture on the fly (in a jam)
  - Wireshark: Capture -> Options -> Output tab



DFIR – Events & Incidents

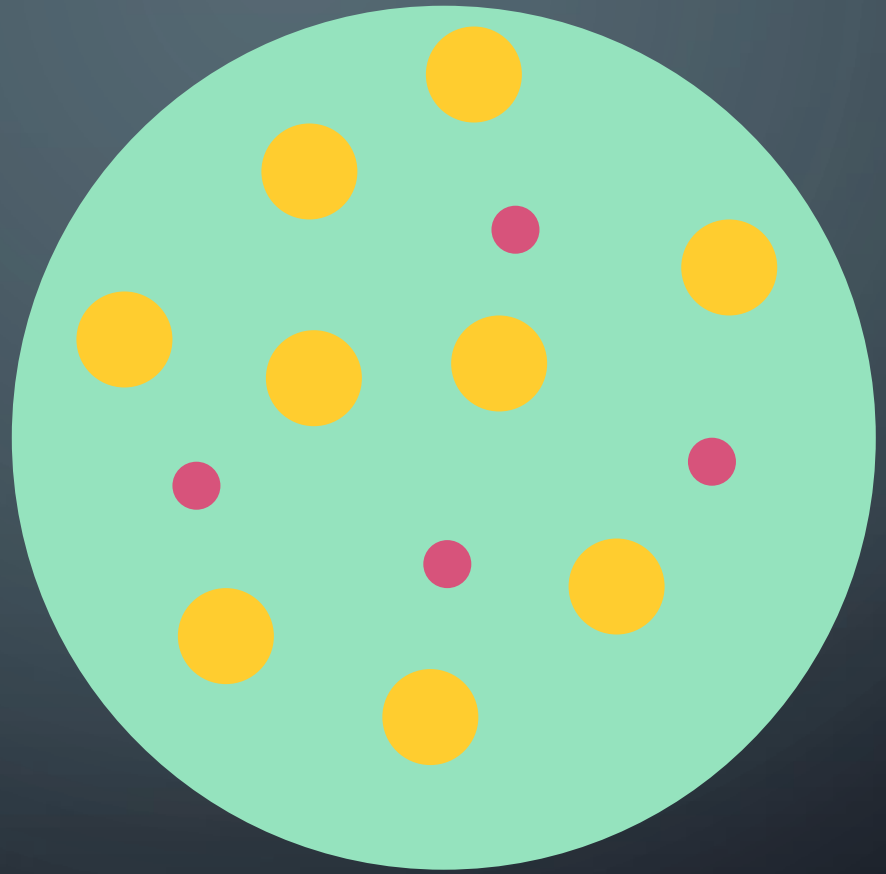
- An event is …
  - Something happened.
- An incident is …
  - An incident is compromised of one or more events
  - Not all events are incidents!
- There is a third state: Events of Interest (EOI)

DFIR – Events & Incidents

EVENTS

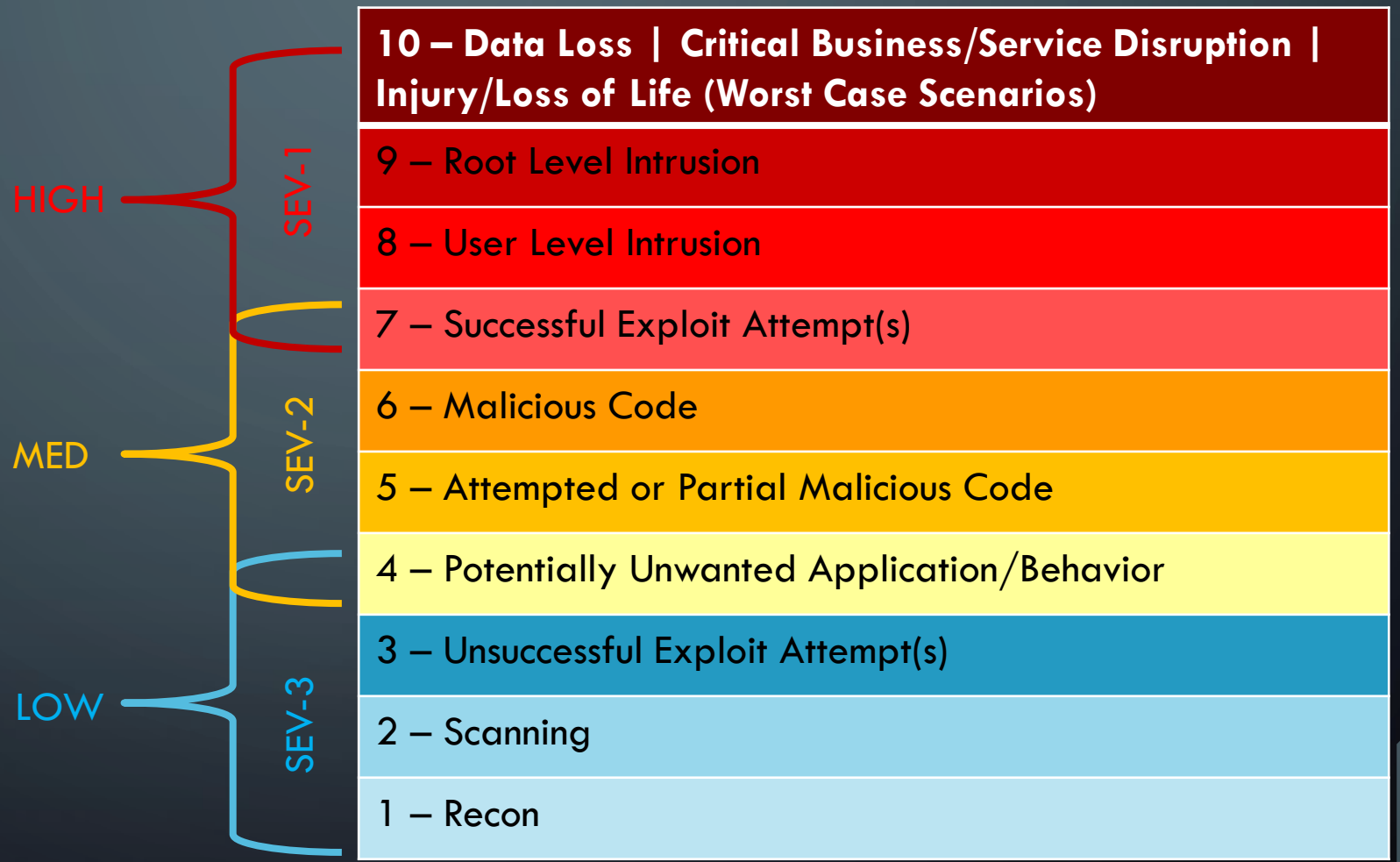
EOI

Incidents



DFIR Basics: Prioritization

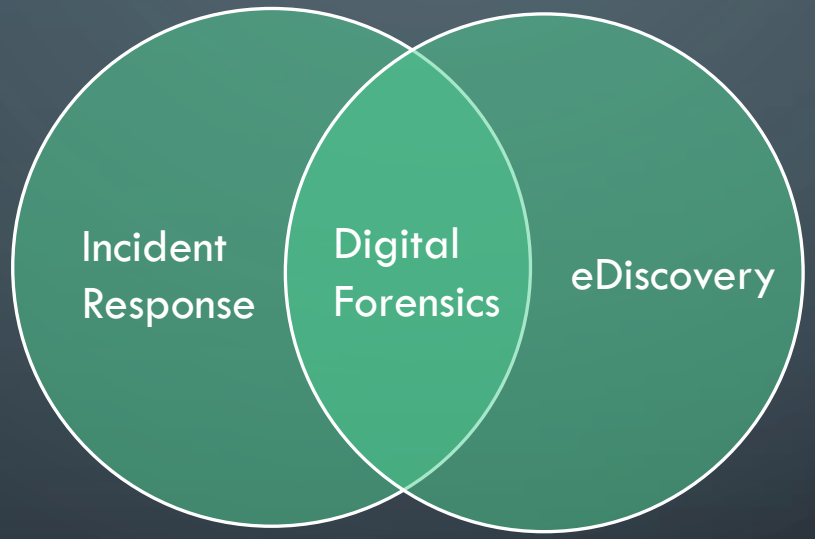
- Kill Chain Mapping
- Severity Chart (1-10)
  - Used for prioritization



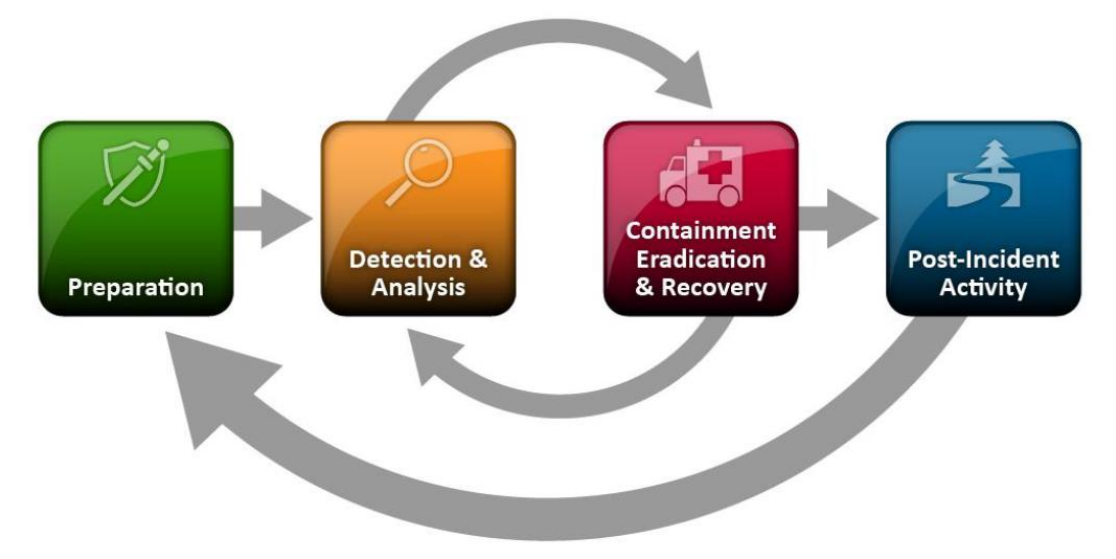
DFIR Basics: Forensics Analysis

DFIR Basics: Forensics Analysis

DFIR Forensics != eDiscovery



DFIR



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

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

Preparation
- People
- Notes
- Relationships
- Policies
- Procedures
- Coms plan
- Tools
- Mgt Tng
- Training
- Jump Bag

Identification
- Awareness
- Need to Know
- Unusual processes
- Unusual Security Evts
- Alert Early
- Use OOB Comms
- New Accts / Privs
- Primary IR Handler
- Passive monitoring
- Odd Sch Tasks
- Unusual Files
- Analyze Logs
- Chain of Custody

Containment
- Stop Bleeding
- Categorize
- Notify Mgt
- Remove LAN Cbl
- Memory Captures
- Chg Pswds
- Short-term
- Criticality
- Asgn Primary IRH
- FW/IDS Filters
- Adjacent Host Logs
- Kill Backdoors
- Back-up
- Sensitivity
- Low Profile
- ISP coord
- Patch Exploited Vuln(s)
- Long-term
- Document Actions
- Infected Vlan
- Forensic Images

Eradication
- Del Artifacts
- Apply All Patches
- Black Hole IP's
- Root Cause
- Addl FW / IDS Filters
- Seek other Host footholds
- Restore Back-up
- Chg DNS Names
- Wipe/Format/Rebuild
- Remove Malware
- Rescan network

Recovery
- Return to Ops
- Monitor (signs/shells/artifacts/events)
- Test /Doc Baseline
- Move to Production (Approval)
- Script searches for attacker artifacts

Lessons Learned
- Document Incident
- All affected parties review / comment on draft
- Finalize Report
- Seek Required Changes
- Immediately upon recovery Phase
- Provide Exec Summary
- Seek Funding
- Assign to on-Scene IRH
- Reach Report Consensus
- Address Process not people
- Update Procedures

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

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!

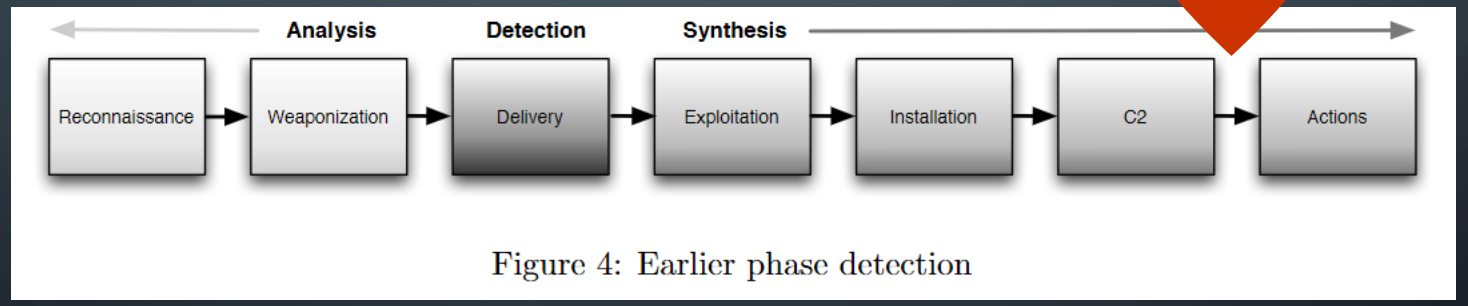
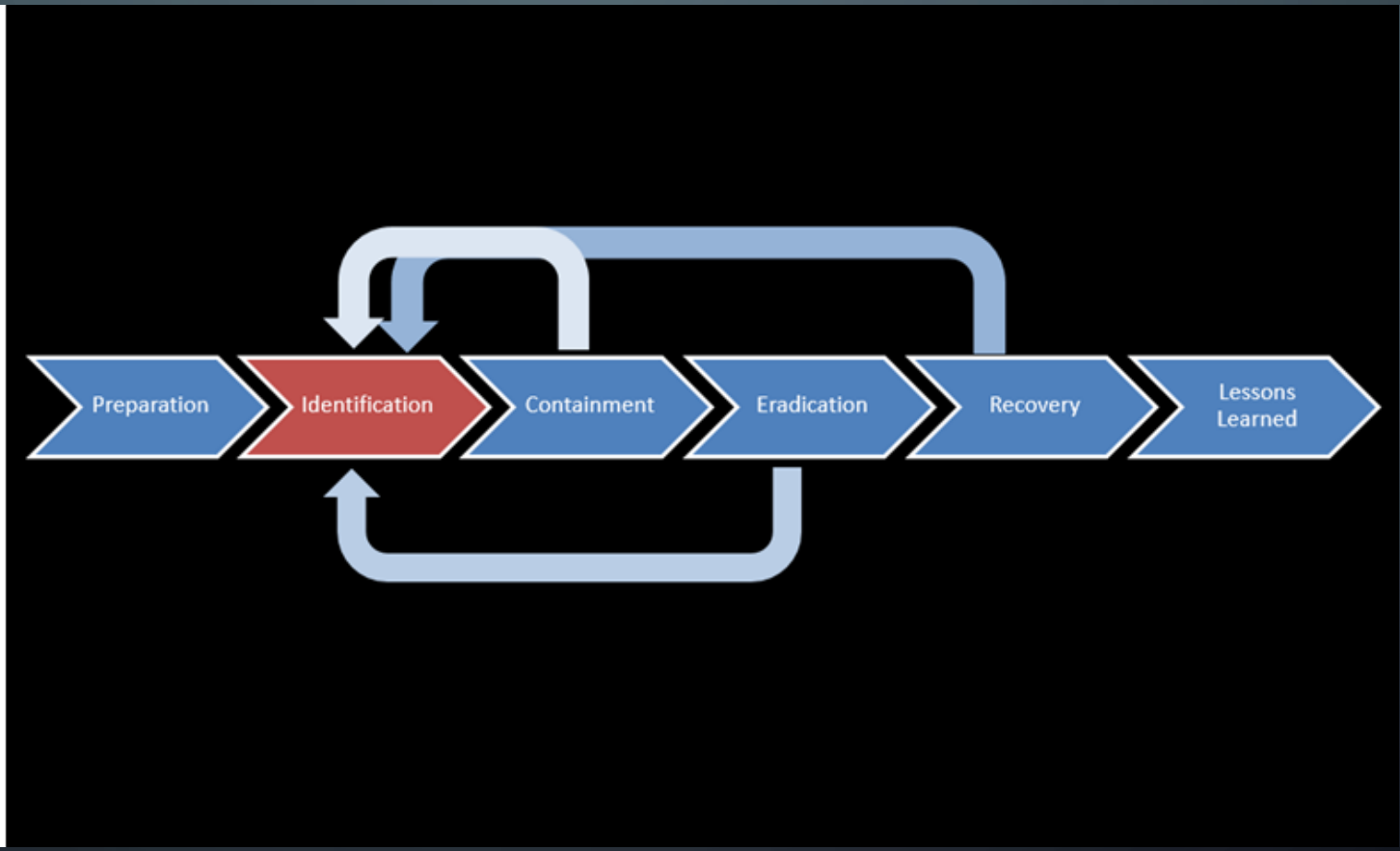


Figure 4: Earlier phase detection

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

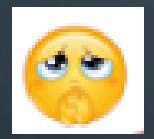
DFIR



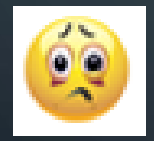
Killz Chains

"Keep 'em coming –
we're catching it all!"

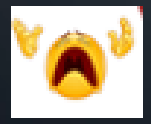
"Ugh, a little clean up is needed, but
it could be worse!"



"I have a bad feeling about this…"



"Honey, leave the light on…it's going
to be a late night"



"Hey friend, you guys hiring?"

Weaponization

Exploitation

C&C

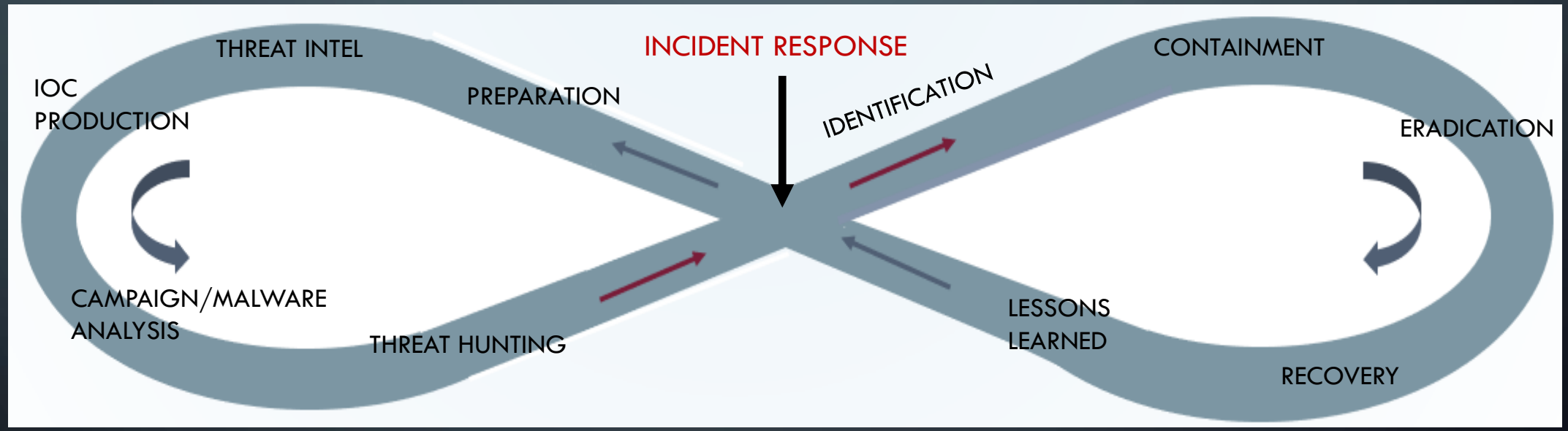
Recon

Delivery

Installation

Mission Accomplished

DFIR 2.0



Prepare to be Prepared – Left side

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?!"

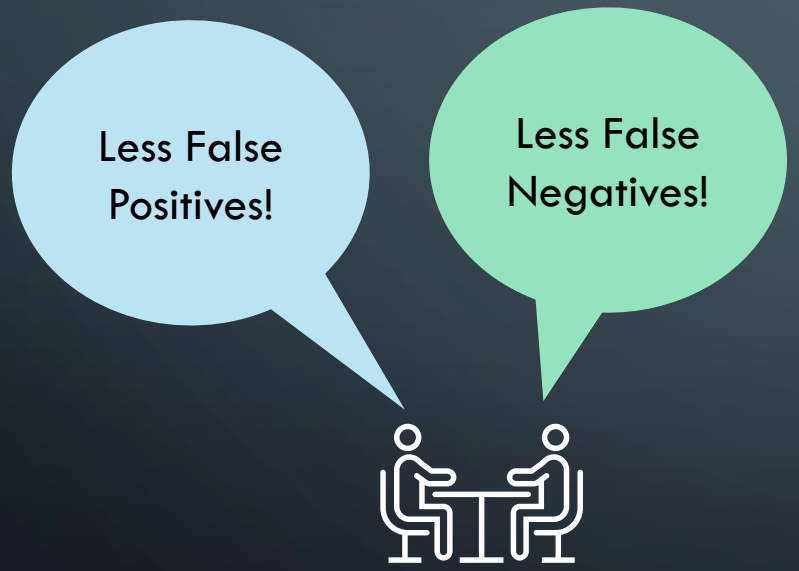
Fighting Enough Fires?

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.

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
- Don’t Wait…Simulate!

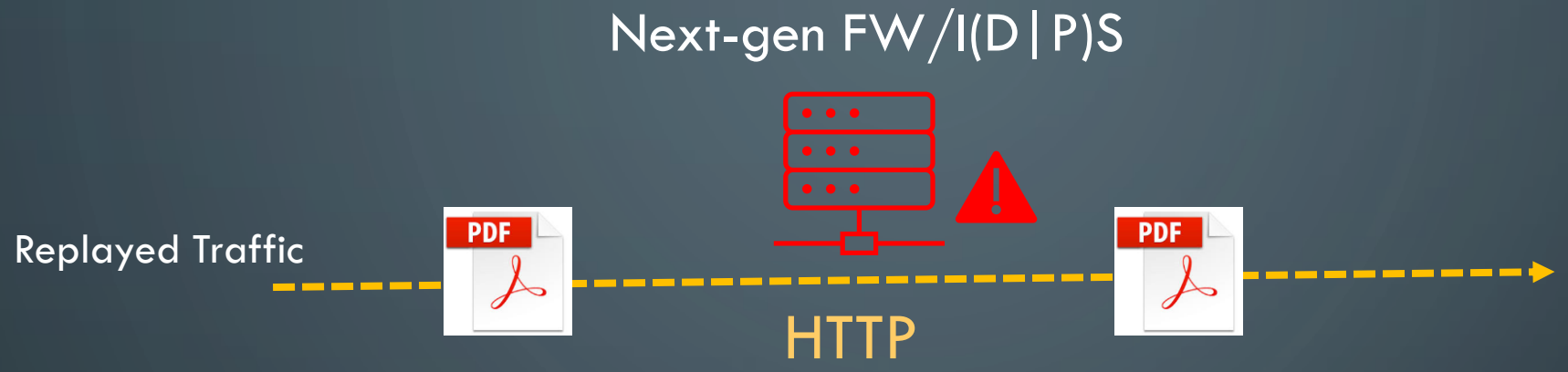
myArray[yolo]

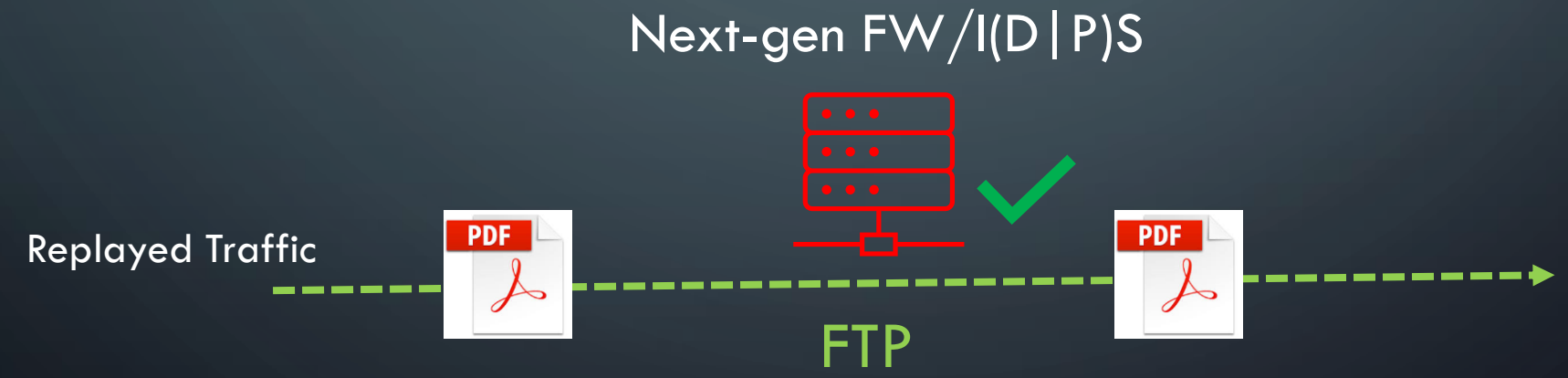
Array Indexing Changed from 0 to 1, back to 0

```
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



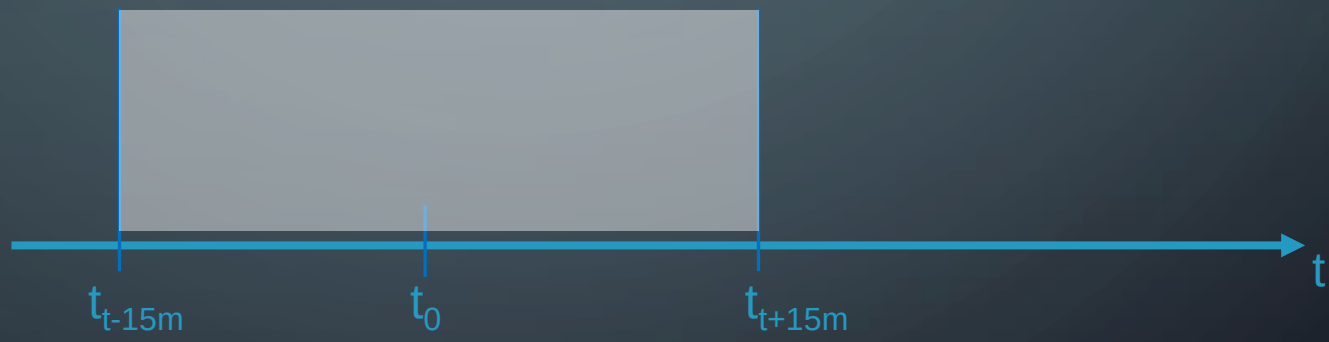


Adversarial Simulation

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

Response – Right Side of the Curve

- Time sampling - 30-minute rule:
  - 15 mins before
  - 15 mins after
  - Reevaluate



CHECKPOINT

Architecture

Architecture

- What does your environment look like? <insert chaotic/messy image>
  - Traditional (on-prem)
    - Centralized or Decentralized
  - Cloud
  - Hybrid

Living off the ether…

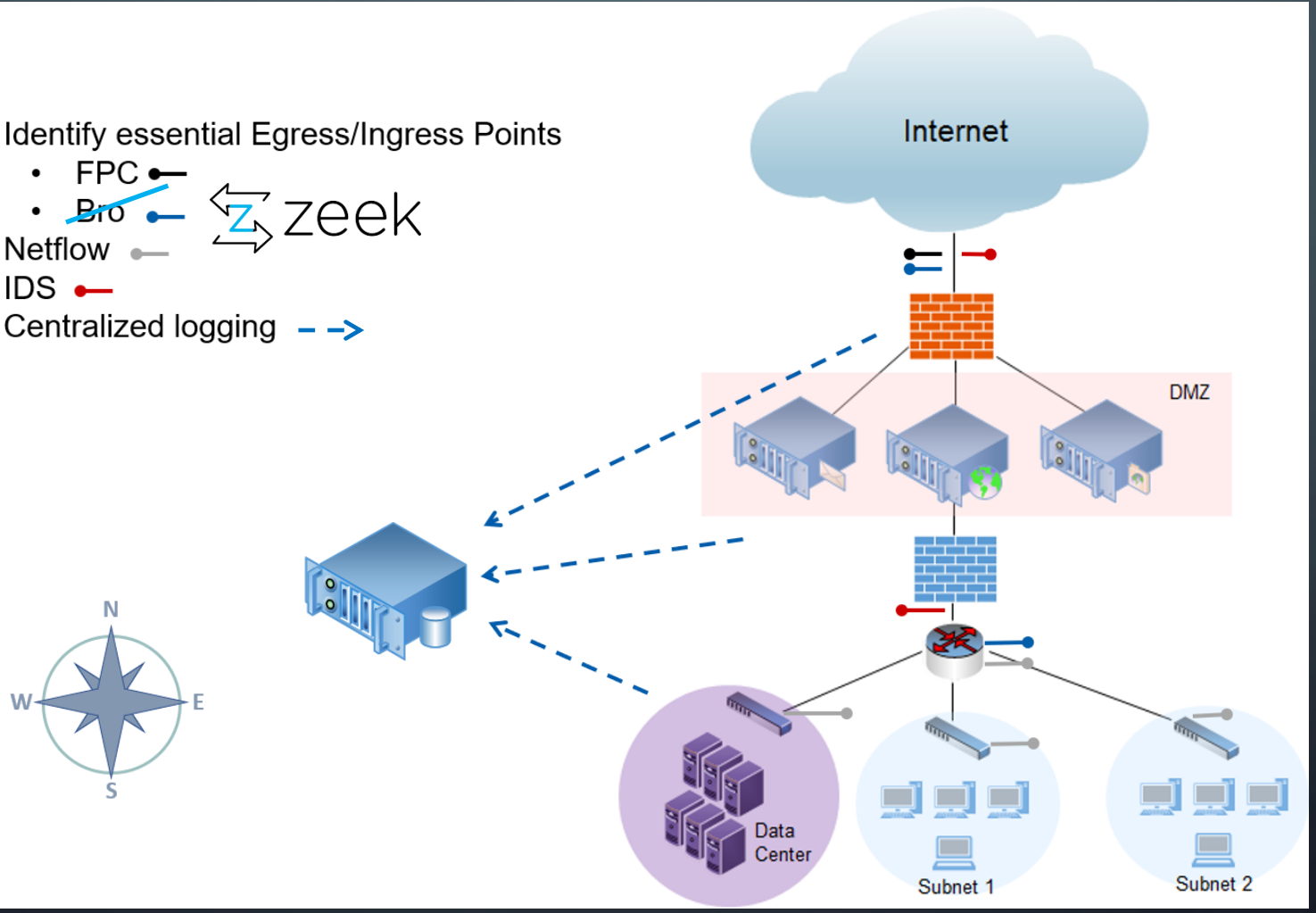
- NSM Stack
  - Placement (Strategic vs. Tactical)

> Get-Viz

- Visibility will dictate detections…or hunting…or forensics
- Can't detect, hunt, or forensicate what we can't see/capture/collect/retain

Architecture

- Identify essential Egress/Ingress Points
  - FPC
  - ~~Bro~~ zeek
- Netflow
- IDS
- Centralized logging



Network Stack

- FPC
- Zeek (fka Bro IDS)
- Application/Proxy Logs
- Firewall Logs (Perimeter)
- Firewall Logs (Enclaves/Segmentation)
- Router Logs
- NetFlow & IPFIX
- Endpoint Logs
- IDS

NSM Placement - Strategic

The Khyber Pass

- 20-mile path through the Hindu Kush mountain range
- Between Afghanistan and Pakistan
- Strategic military pass for centuries

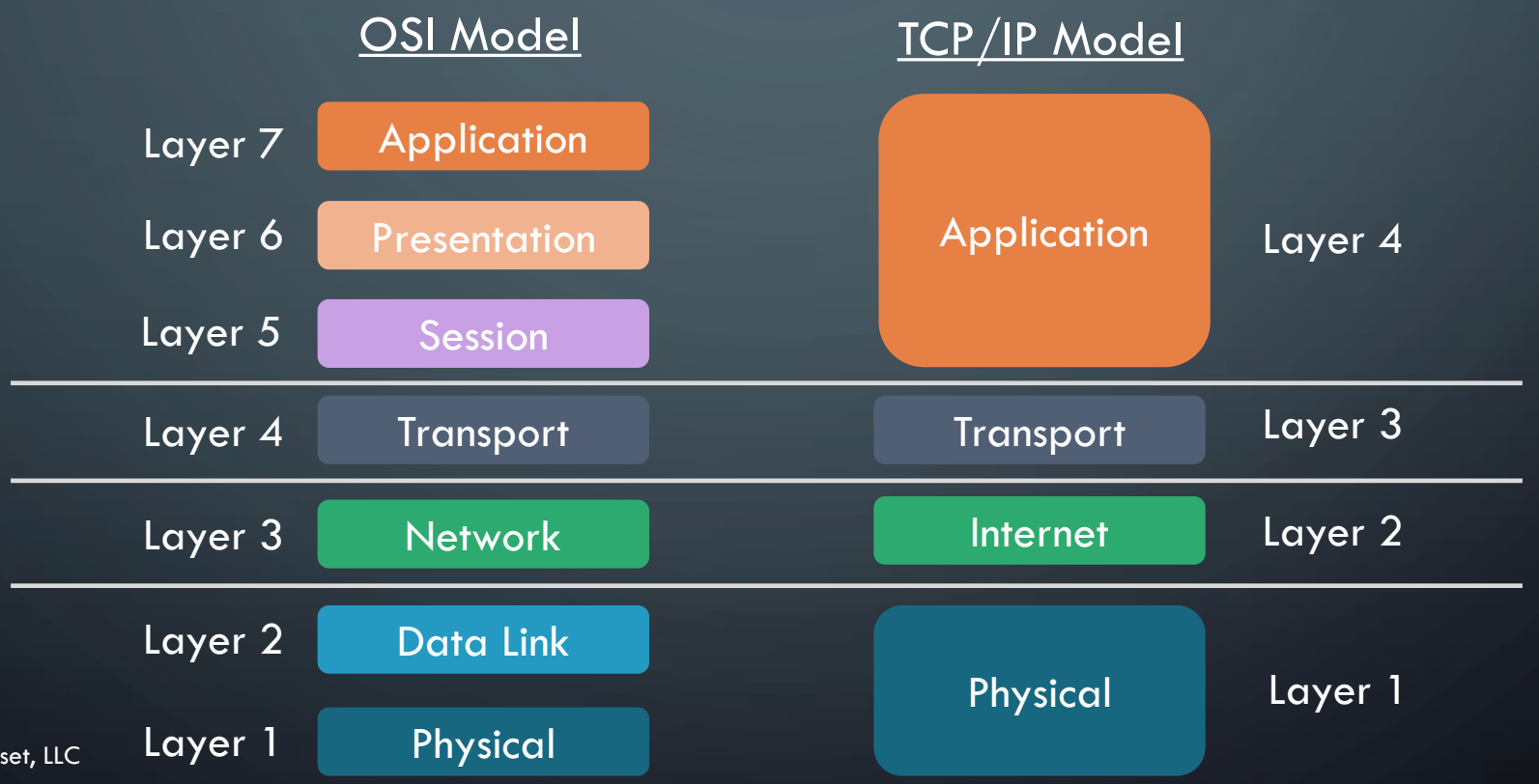
Source: https://www.nationalgeographic.org/media/khyber-pass/

It's Primer Time!

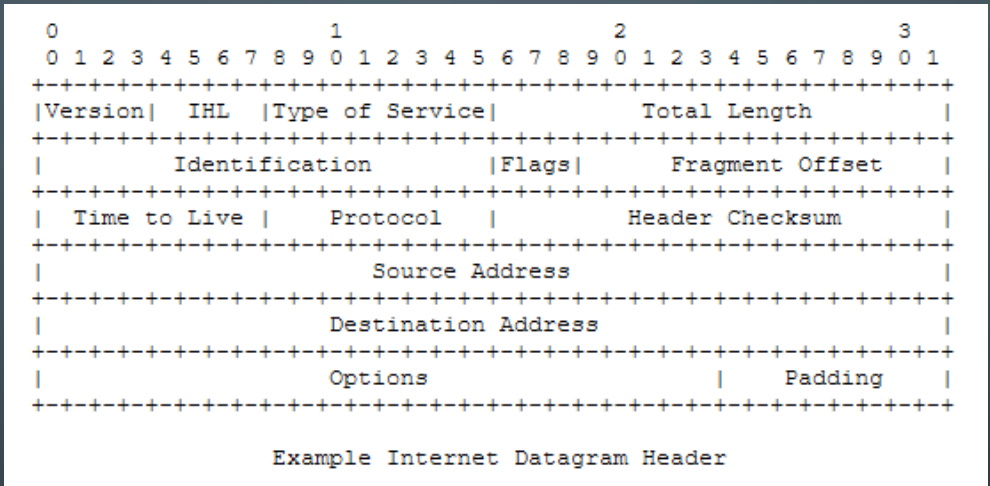
- OSI and TCP/IP Models
- IPv4
- TCP/UDP

OSI & TCP/IP

- Open System Interconnect (OSI)
- Transmission Control Protocol (TCP)/Internet Protocol (IP) models



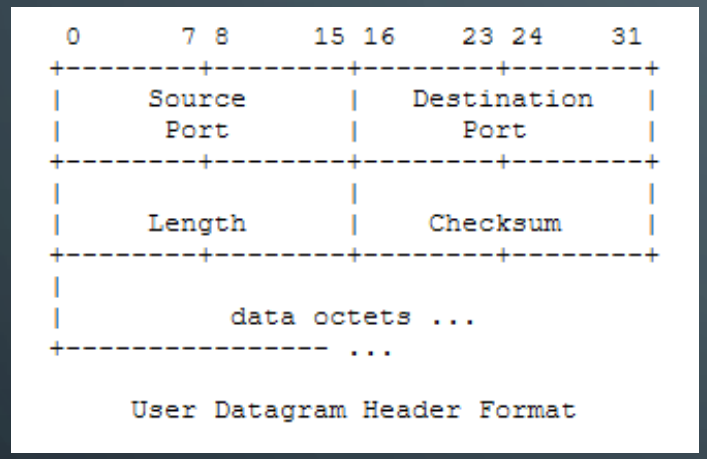
IPv4

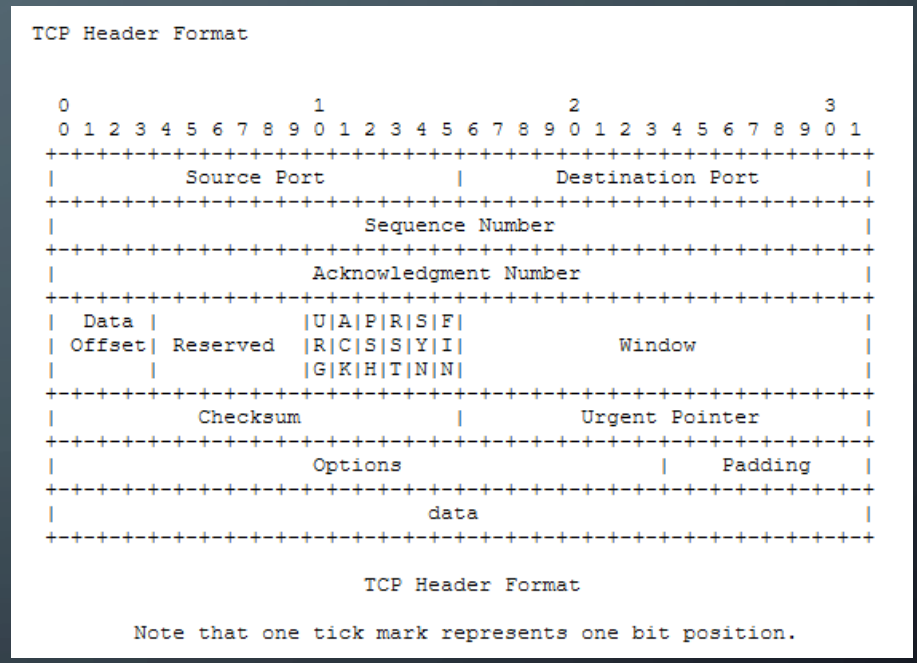


Example Internet Datagram Header

RFC 791

UDP/TCP





Fingerprinting/Profiling

- Operating System (OS) Profiling
- Application Profiling

Host Profiling

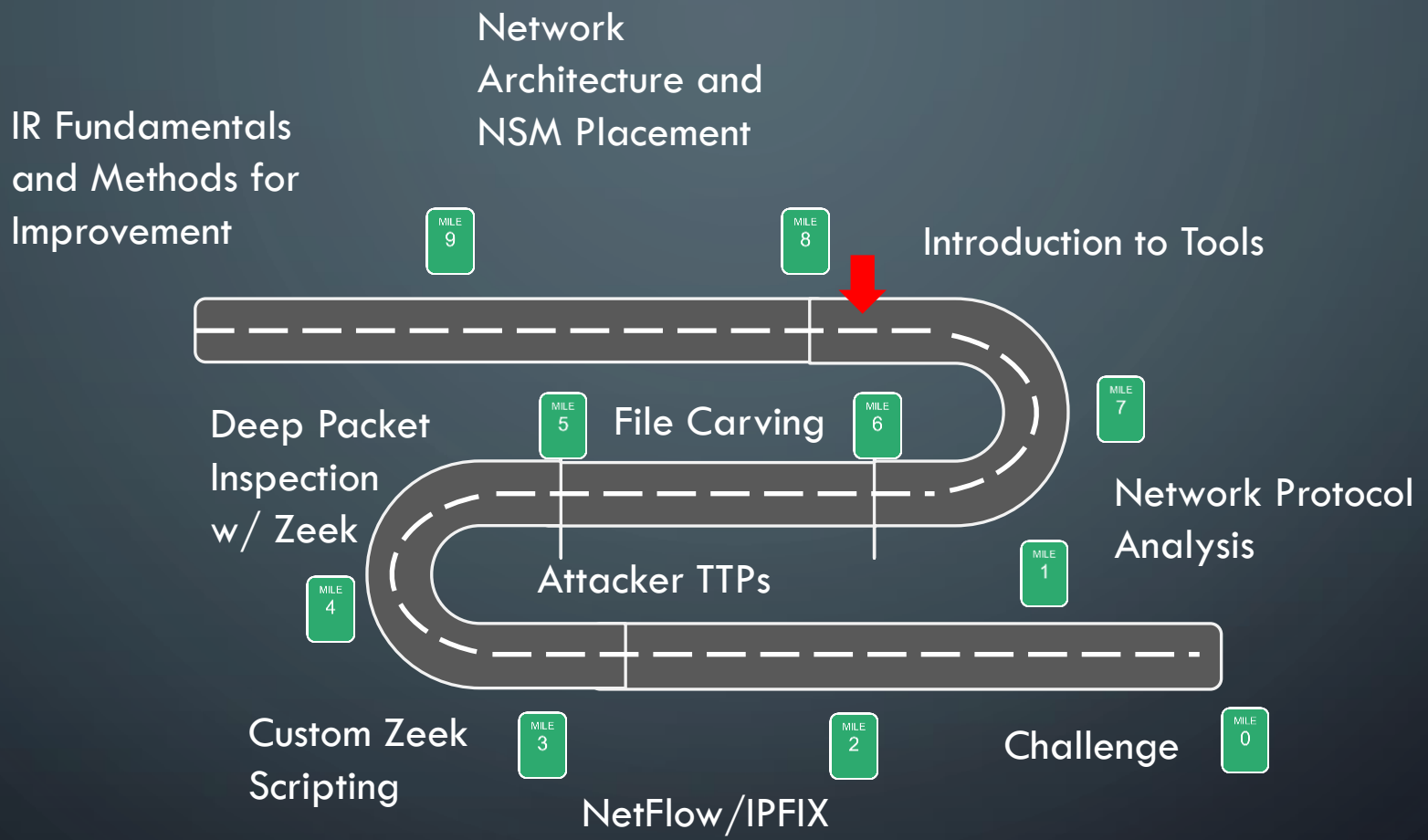
- TTL (IP TTL not DNS TTL)
- TCP Window Sizing
- But wait, there's more…
  - HTTP User-Agents
  - DNS Traffic
  - NTP Traffic

Lab 0000 – VM Check

- ✓ Download VM
- ✓ Open OVF…
- ✓ Login
- ✓ Elevate to root
- ✓ Check Lab Artifact/Evidence Files
- ✓ Mount Additional Storage

CHECKPOINT

Roadmap



End Day 1

DAY 1 END