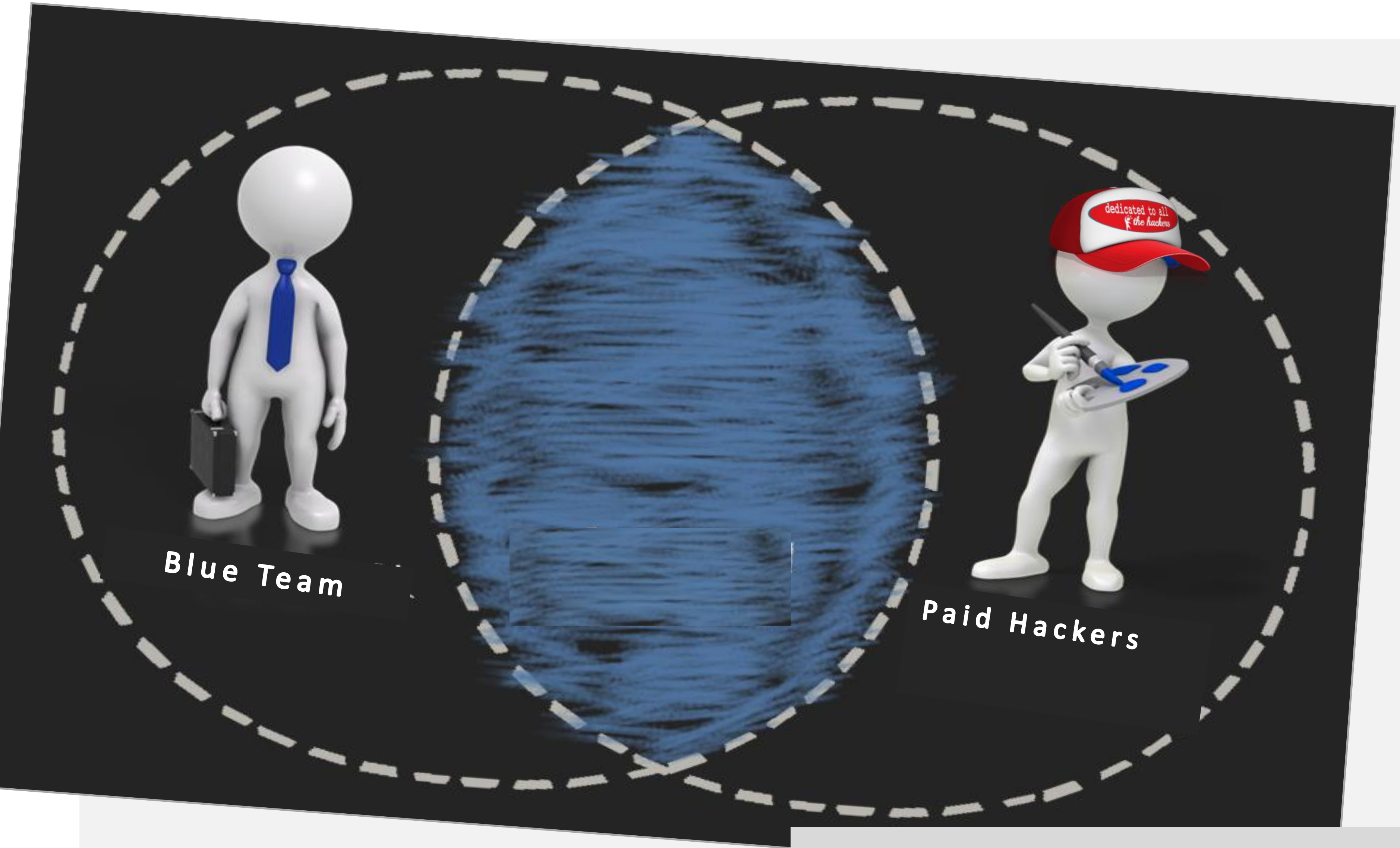
Forecast: Sunny, Clear Skies, and 100% Detection

Alissa Torres | **@sibertor**

THIR Summit
6 September 2018



Inspired by Ryan McGeehan https://medium.com/starting-up-security

One of the other companies I work with was recently breached. . . $$$$ gone in minutes.

I hear the solution is a **red team exercise...**

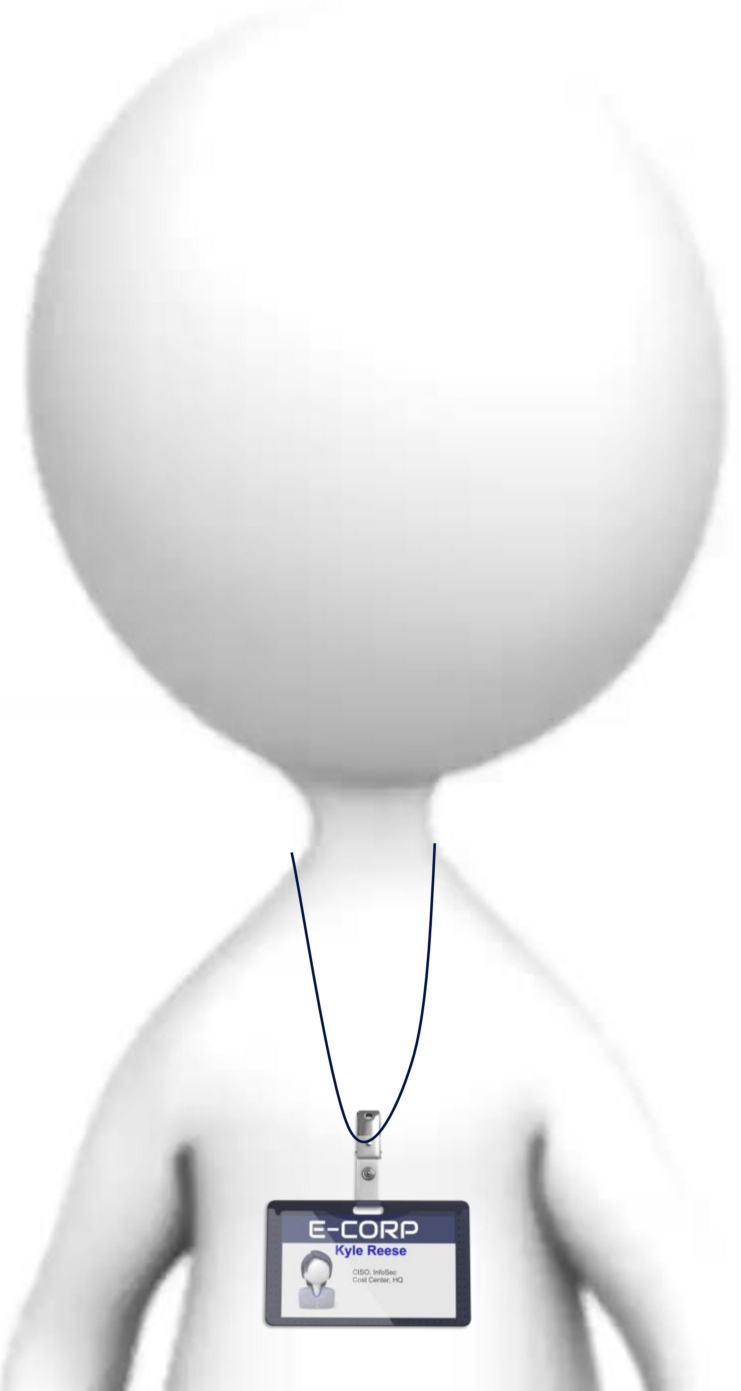
What is red teaming?

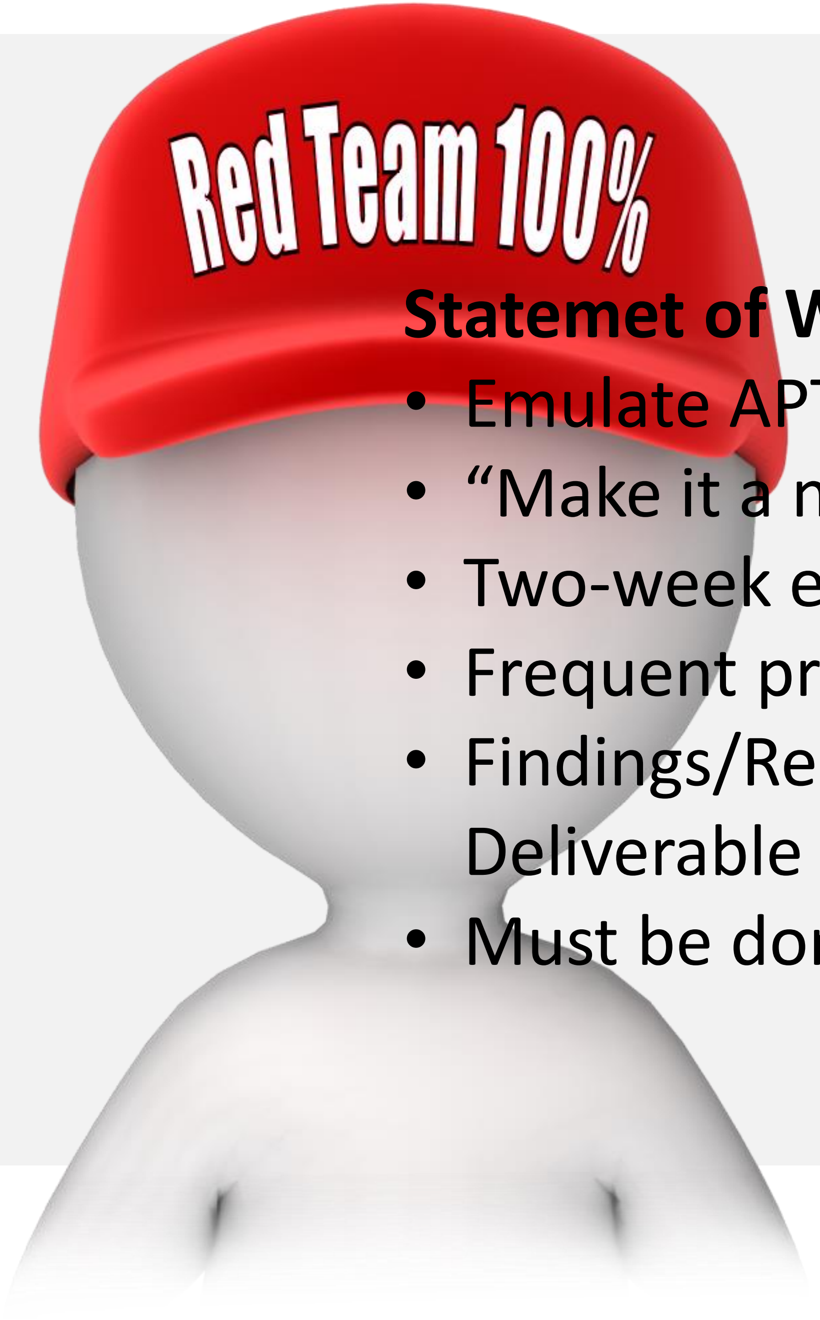
Red Team Exercise

"An exercise reflecting real-world conditions that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization."

- NIST SP800-53 REV.4

QI



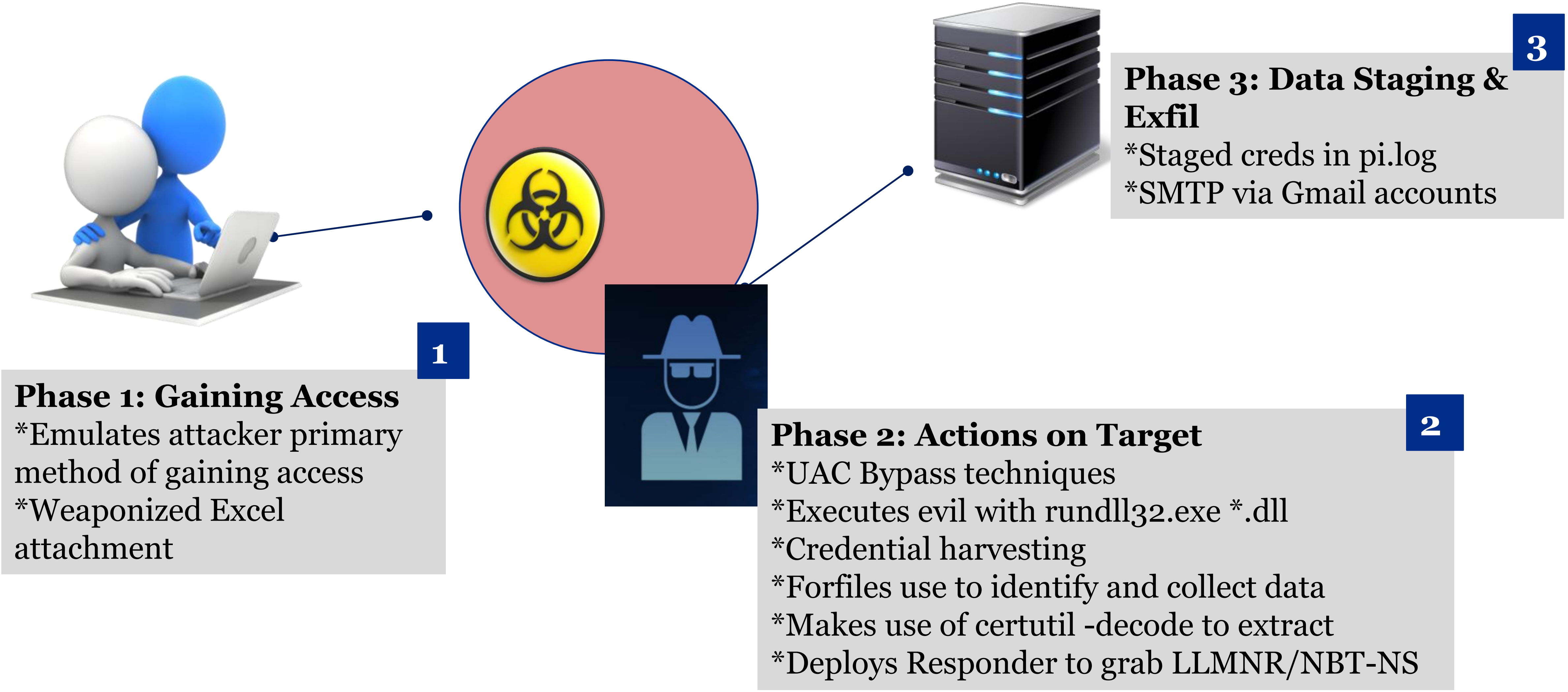


Statemet of Work

- Emulate APT28 Fancy Bear
- “Make it a nightmare scenario”
- Two-week engagement
- Frequent progress meetings
- Findings/Recommendations Deliverable
- Must be done within the 1st Quarter

APT28 Adversary Emulation

Objective: Steal Crown Jewels/Intellectual Property

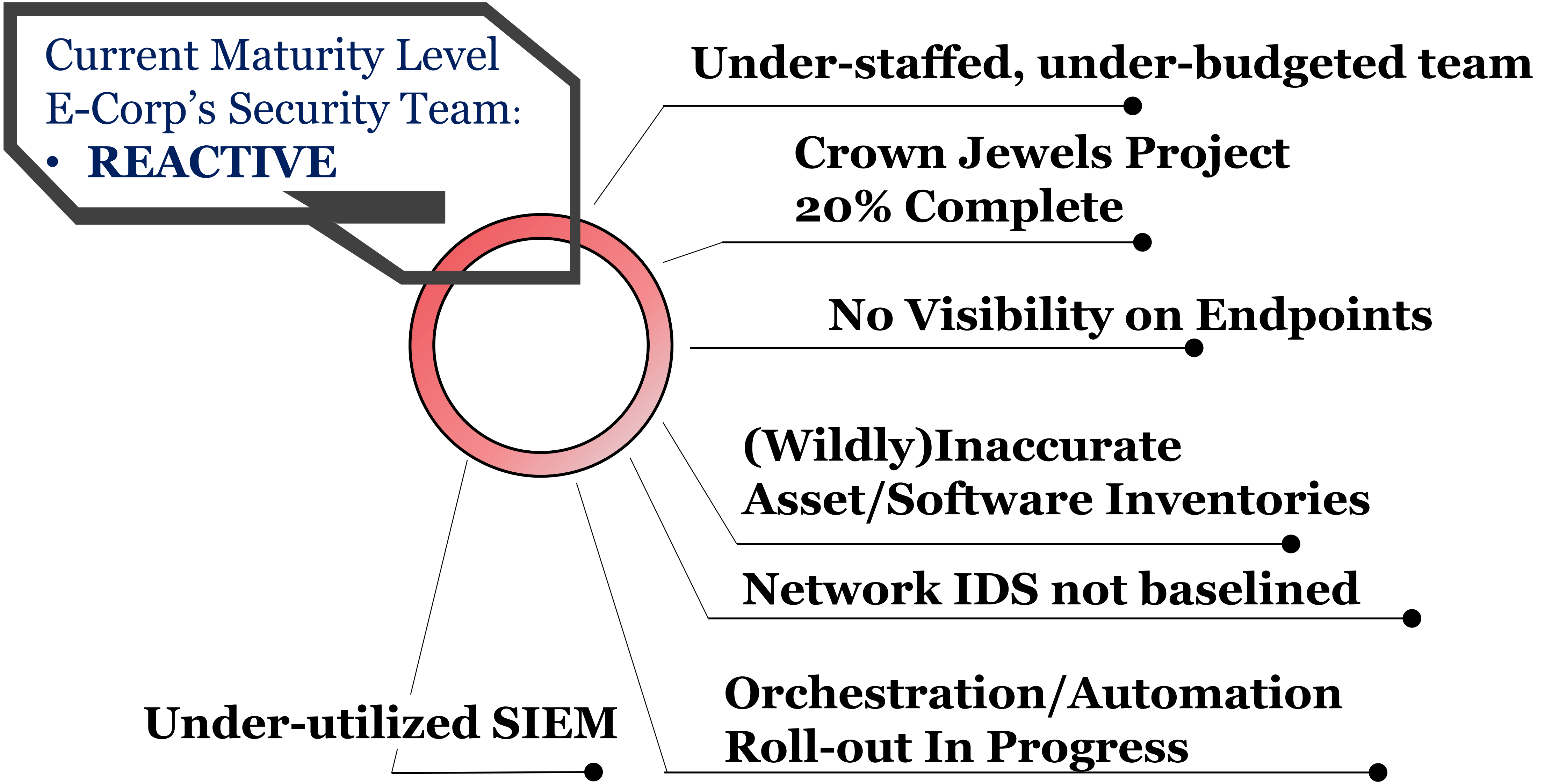


Phase 1: Gaining Access
*Emulates attacker primary method of gaining access
*Weaponized Excel attachment

Phase 2: Actions on Target
*UAC Bypass techniques
*Executes evil with rundll32.exe *.dll
*Credential harvesting
*Forfiles use to identify and collect data
*Makes use of certutil -decode to extract
*Deploys Responder to grab LLMNR/NBT-NS

Phase 3: Data Staging & Exfil
*Staged creds in pi.log
*SMTP via Gmail accounts

State of E-Corp Security Team



Current Maturity Level
E-Corp's Security Team:

- **REACTIVE**

Under-staffed, under-budgeted team

Crown Jewels Project 20% Complete

No Visibility on Endpoints

(Wildly)Inaccurate Asset/Software Inventories

Network IDS not baselined

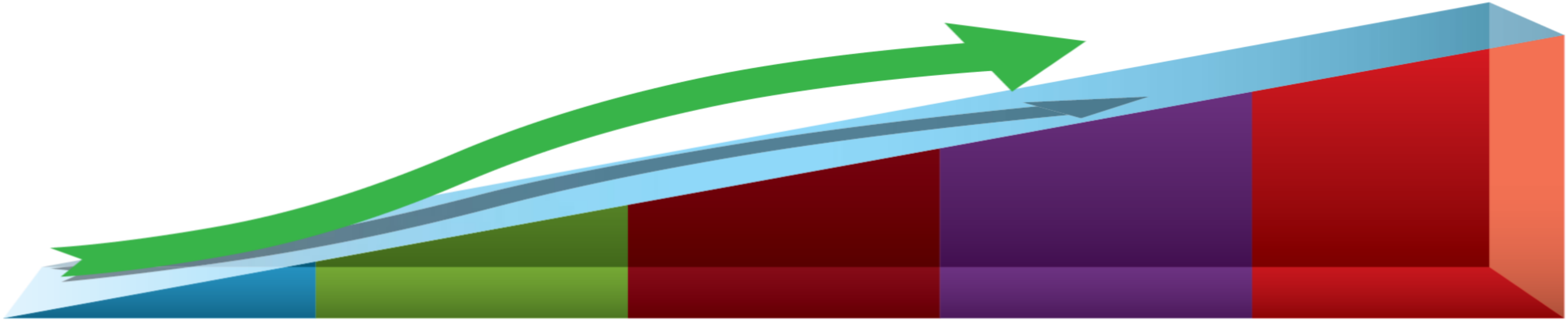
Orchestration/Automation Roll-out In Progress

Under-utilized SIEM

Red Team Engagement Lessons Learned

When to Implement Attack Simulations

depends on organization's maturity



LEVEL 1
Random, or Disorganized

LEVEL 2
Reactive, or Tactical

LEVEL 3
Preventative

LEVEL 4
Organized, or Directed

LEVEL 5
Proactive, Comprehensive, Continuous and Measurable

G.Mark Hardy, "Behind the Curve? A Maturity Model for Endpoint Security",
www.sans.org/reading-room/whitepapers/analyst/curve-maturity-model-endpoint-security-36342

Growing an Experienced Security Team

- ~~Time, Experience and Casualties~~
- Tabletops/Walk-throughs of process/procedures
- Blue Team Hardening
- Attack Path Verification
- Attack Simulations

When to Implement Attack Simulations

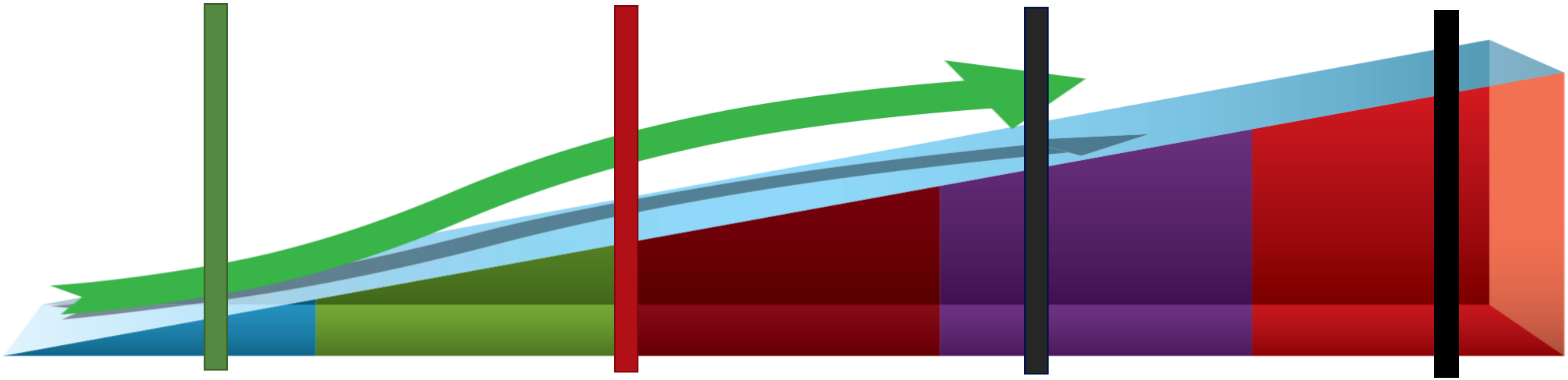
depends on organization's maturity

Tabletop Scenarios

Blue Team Hardening

Attack Path Verification

Attack Simulation



LEVEL 1
Random, or Disorganized

LEVEL 2
Reactive, or Tactical

LEVEL 3
Preventative

LEVEL 4
Organized, or Directed

LEVEL 5
Proactive, Comprehensive, Continuous and Measurable

G.Mark Hardy, "Behind the Curve? A Maturity Model for Endpoint Security",
www.sans.org/reading-room/whitepapers/analyst/curve-maturity-model-endpoint-security-36342

Tabletop Exercise

What is the Mission?

Goals include:

- To test incident response procedures, communication flow, business continuity plans across stakeholders
- To identify gaps and weaknesses in people, process and technology
- To gain the ability to predict likelihood of future attacks

Groce, E. “Knowing Your Battle Space - Part 1” https://security-storm.com/playbook/2017/9/14/knowing-your-battle-space-part-1

SEC504 Tabletop Exercise

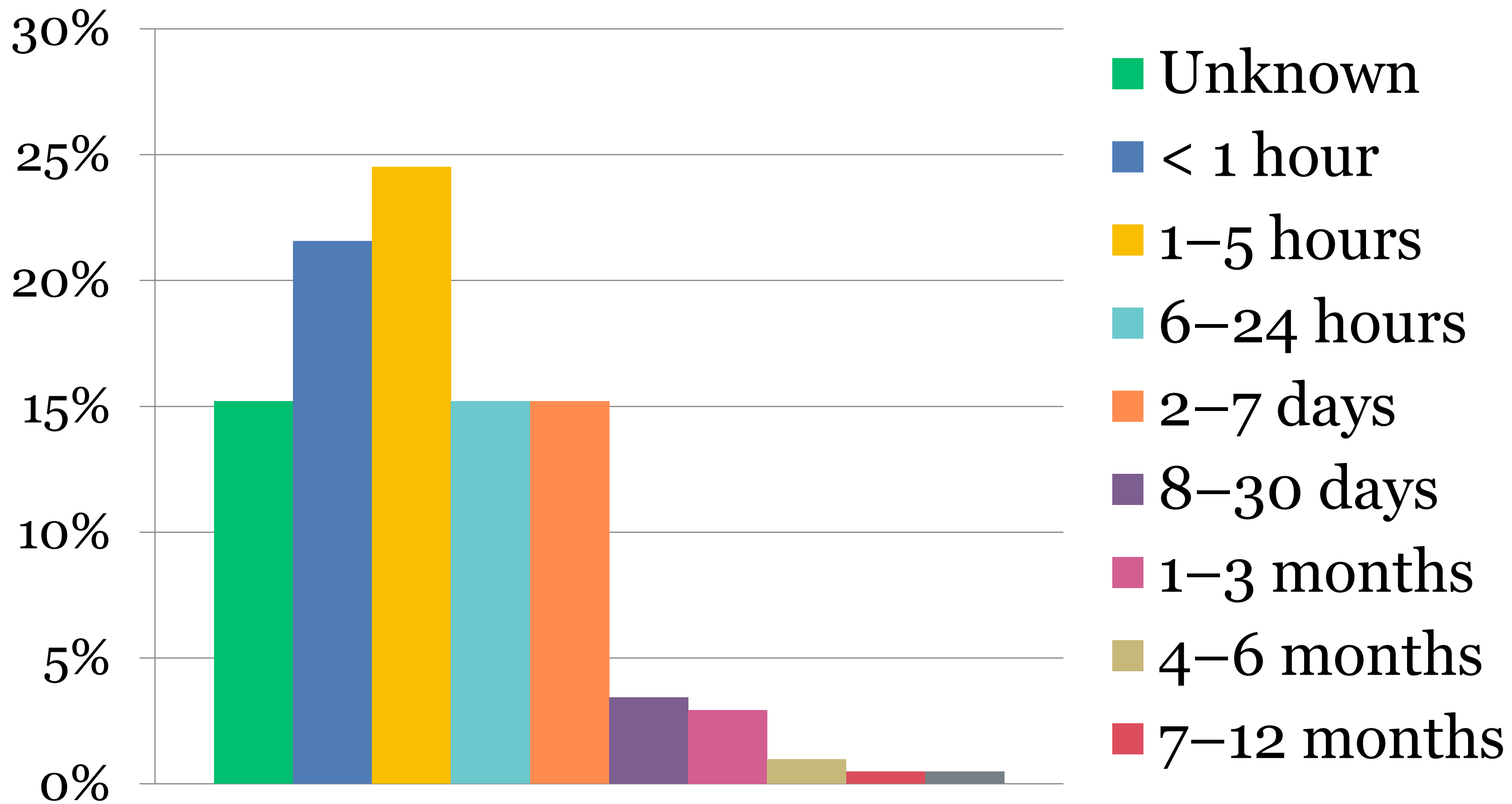
Rules of Engagement:

- Grouped with team members who are strangers
- Success of response activities decided by the roll of a 20-sided die
- +3 Factor if process is defined
- +2 Factor if skillset exists amongst team members
- Injects are introduced at will by incident master
  - Firewall stops logging, SIEM collapses, No AV logs, intern kills target system, lead handler goes on paternity leave, distractionary DDOS

Time to Detection: Self Reported

SANS State of Endpoint Security Survey 2018

Length of time (on average) for you to detect an endpoint exploit?

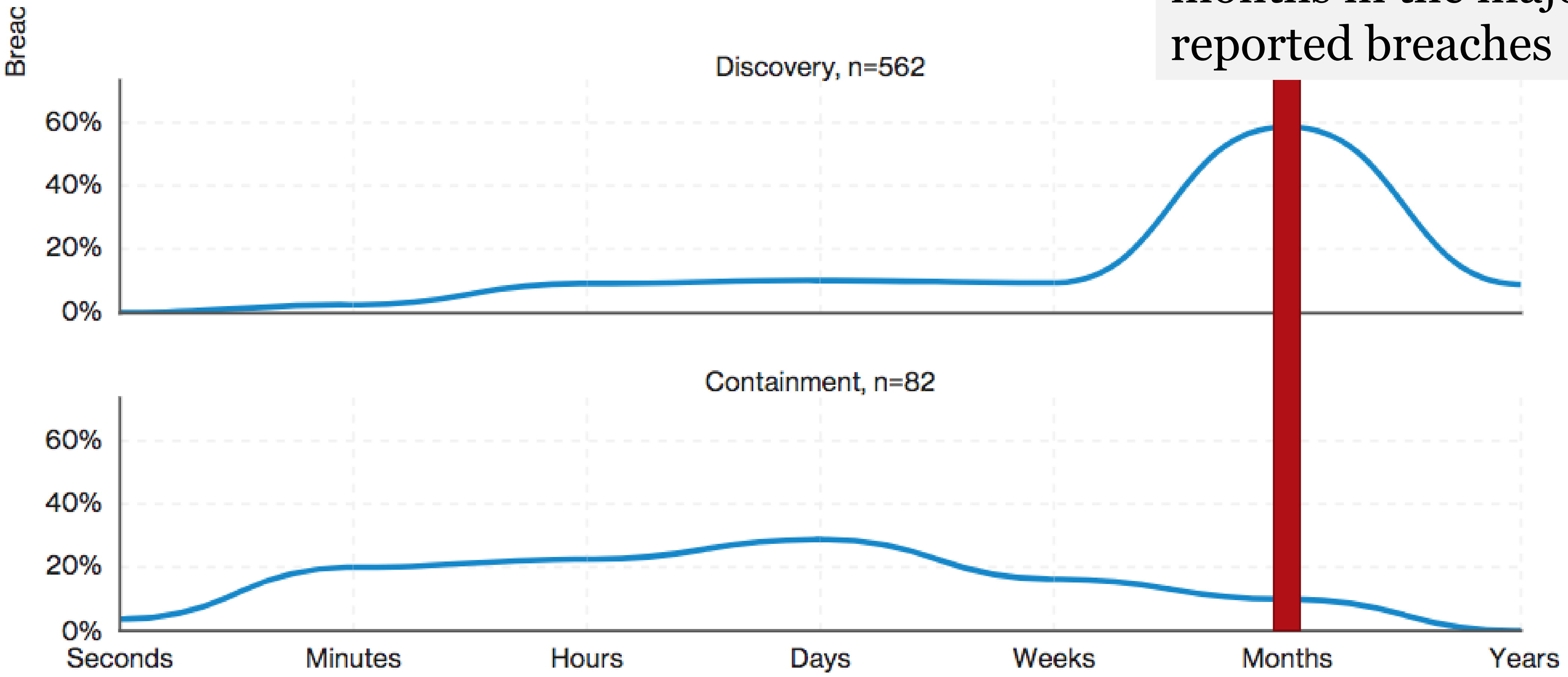


45%

Detected endpoint exploit in <=5 hours

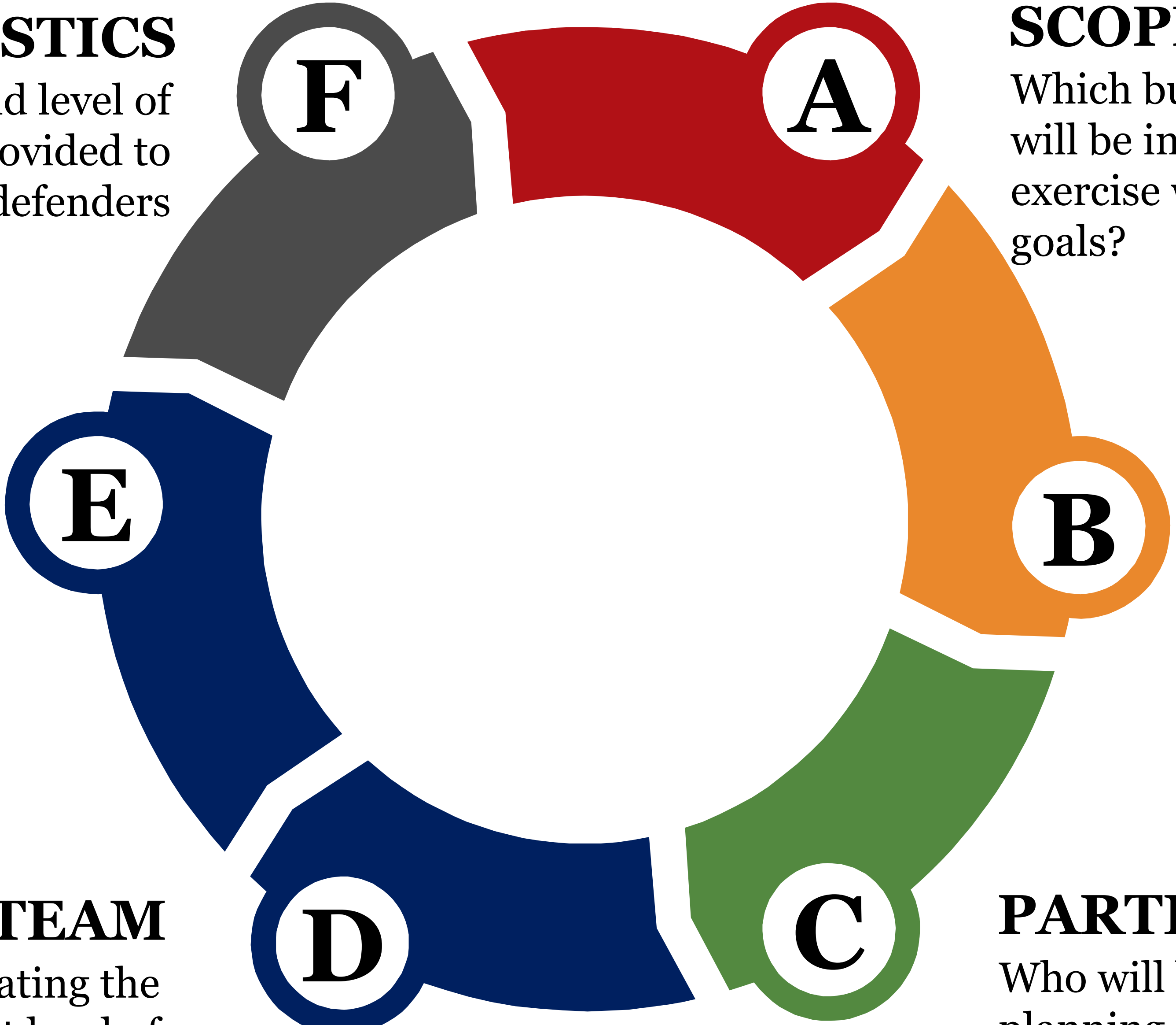
Survey Results Don’t Align

Verizon Data Breach Investigations Report 2018



Discovery was weeks or months in the majority of reported breaches

6 STEP SIMULATION PLANNING



SCOPE

Which business units will be involved? Align exercise with business goals?

OBJECTIVE

What areas of the security program are being assessed?

PARTICIPANTS

Who will be included in the planning and execution of the engagement?

EXECUTION TEAM

Who will be simulating the threat actors, what level of access will they have?

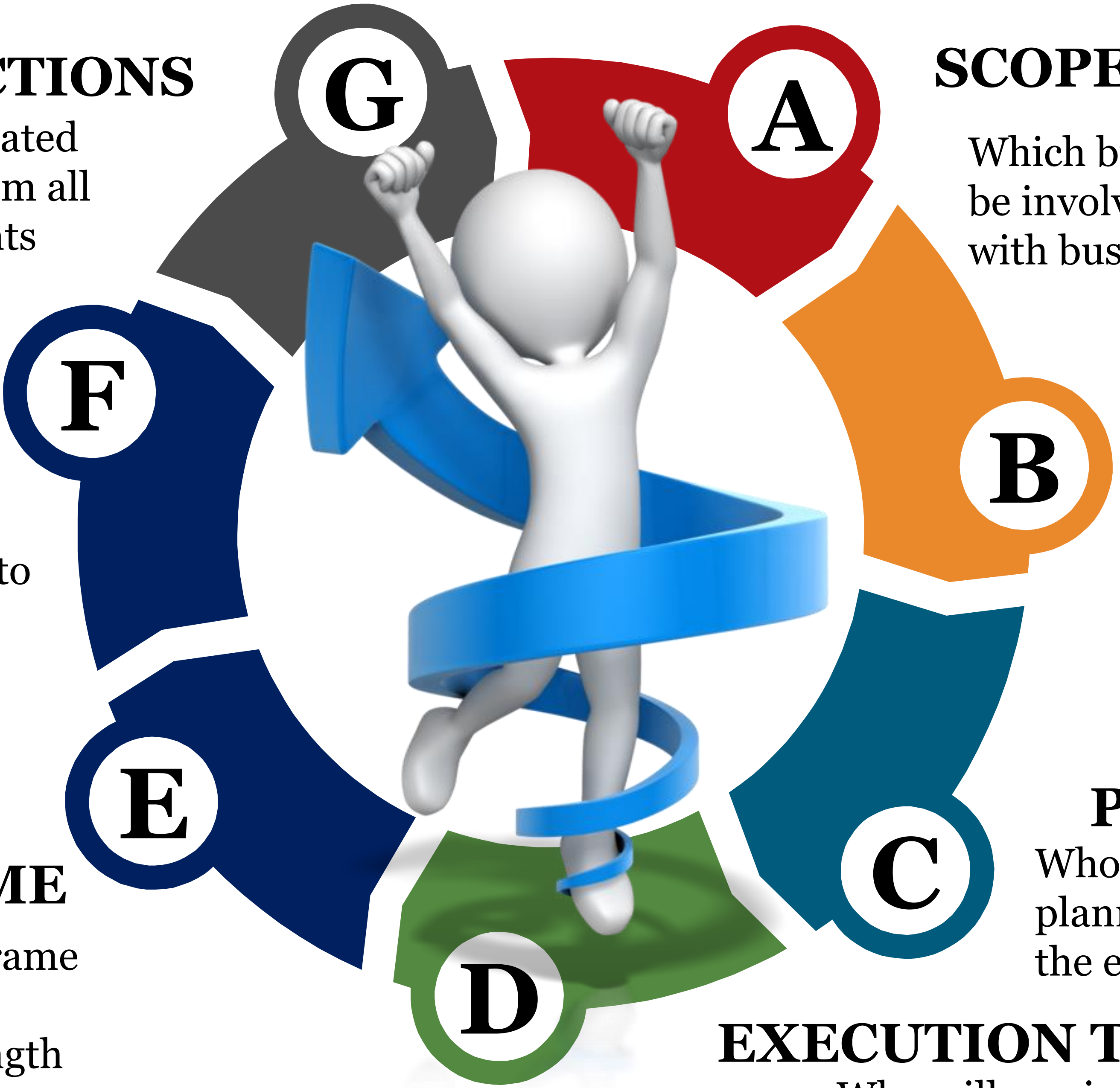
TIMEFRAME

Define the timeframe of the active engagement, length of each attack stage

LOGISTICS

Details and level of access to be provided to red team, defenders

7 STEP SIMULATION PLANNING



SCOPE

Which business units will be involved? Align exercise with business goals?

OBJECTIVE

What areas of the security program are being assessed?

PARTICIPANTS

Who will be included in the planning and execution of the engagement?

EXECUTION TEAM

Who will receive status updates and when?

TIMEFRAME

Define the timeframe of the active engagement, length of each attack stage

LOGISTICS

Details and level of access to be provided to red team, defenders

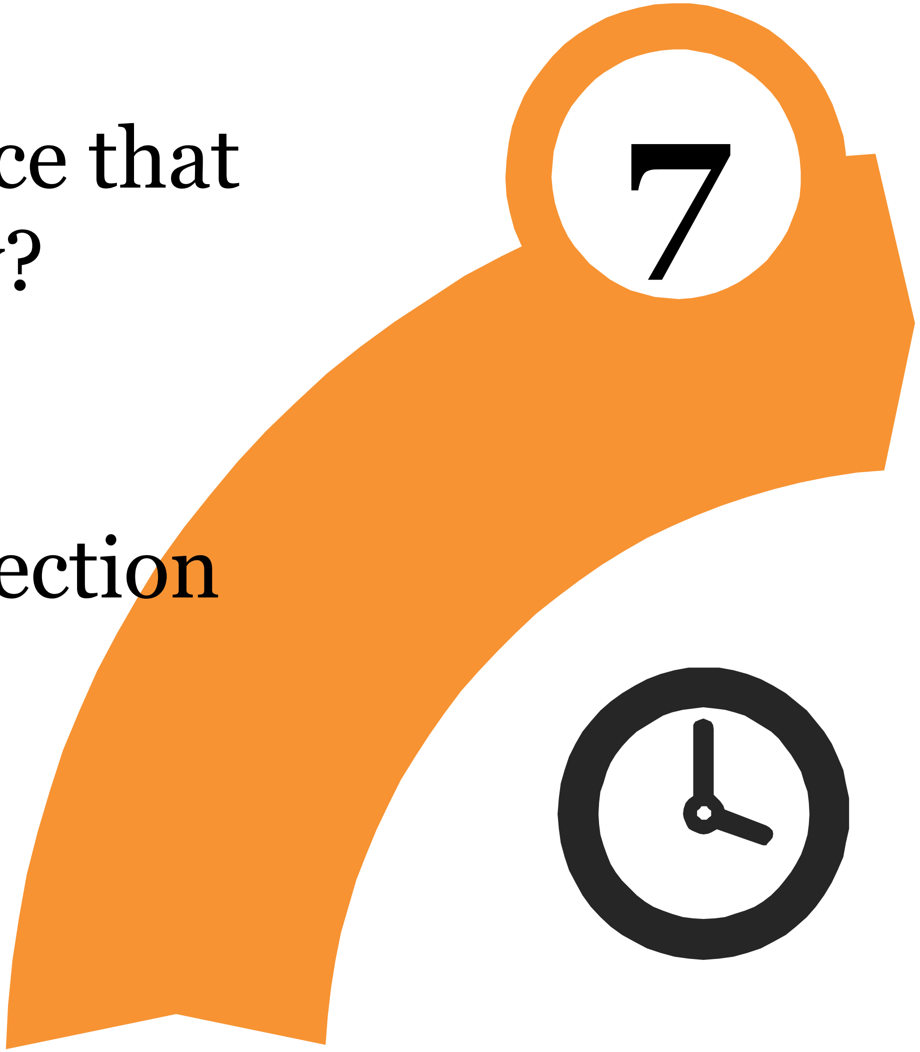
PREDICTIONS

Solicit estimated outcomes from all participants

STEP 7: PREDICTIONS

Based on the proposed scenario:

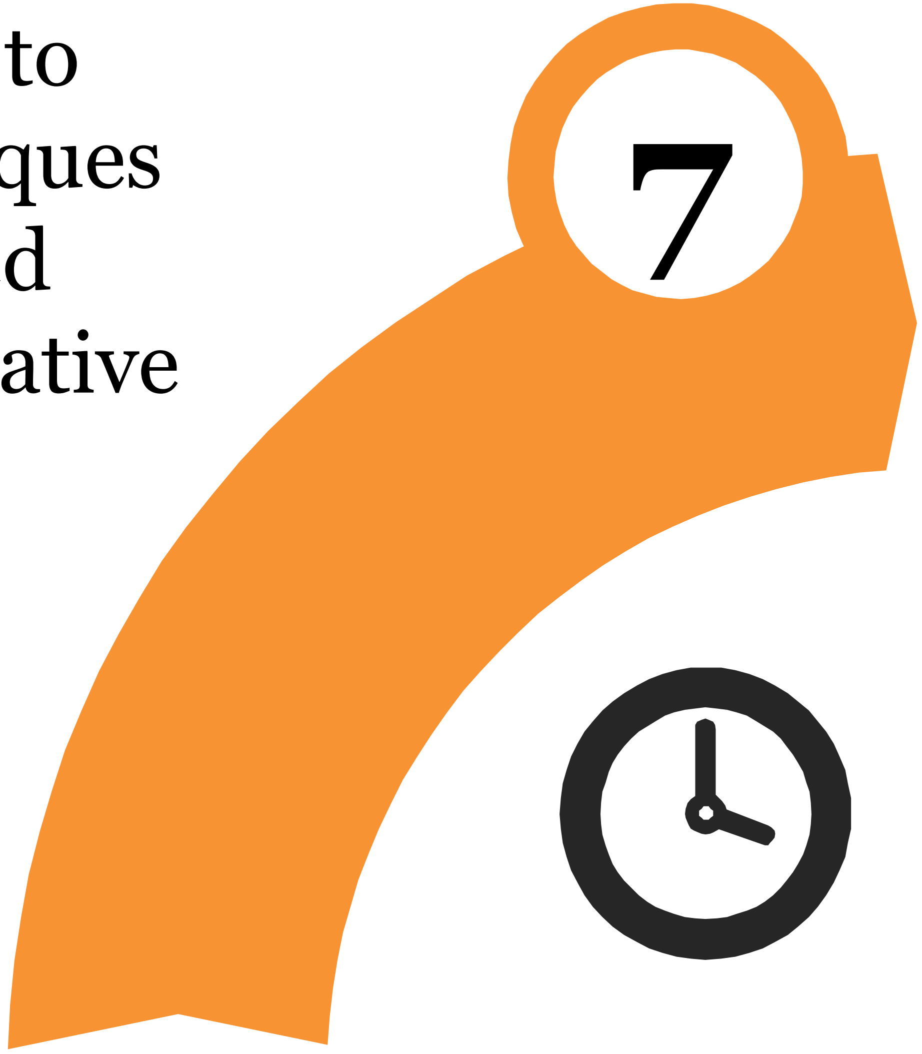
- How will you detect this attack?
- What technologies do you have in place that will provide visibility into this activity?
- How fast can you detect this activity?
- Can you identify attack origins?
- What is your expected success for detection and response?



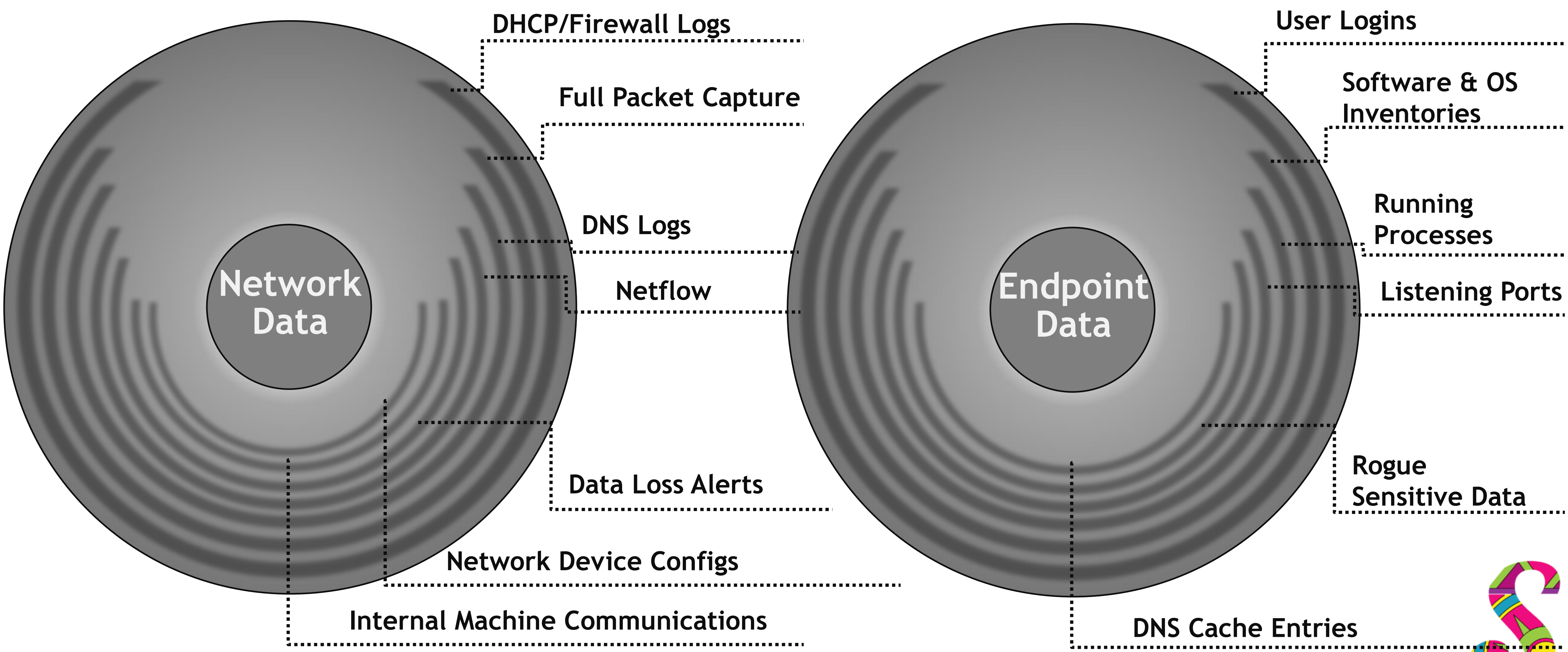
STEP 7: PREDICTIONS

GOALS:

- Increase value of simulation exercise to better refine objectives, attack techniques
- Gather expectations and self-perceived strengths and weaknesses for comparative analysis during lessons learned



Map your Technologies to Assess your Visibility Gaps



Network Data

DHCP/Firewall Logs

Full Packet Capture

DNS Logs

Netflow

Data Loss Alerts

Network Device Configs

Internal Machine Communications

Endpoint Data

User Logins

Software & OS Inventories

Running Processes

Listening Ports

Rogue Sensitive Data

DNS Cache Entries

Blue Team Hardening
What is the Mission?

Goals include:

- To test detection and response methods devised to alert on specific adversary behavior
- To validate new alarms, rules for specific tactic
- To measure proof of concept technology implementations
- To verify coverage of one cell in ATT@CK Matrix

Groce, E. “Knowing Your Battle Space - Part 1” https://security-storm.com/playbook/2017/9/14/knowing-your-battle-space-part-1

Alert: Detecting wmiexec.vbs

WMIEXEC.VBS - tool used for Windows system management

Source host: The source that executes wmiexec.vbs
Destination host: The machine accessed by the wmiexec.vbs
*Network Traffic: 135 TCP/445 TCP
*Prefetch File Creation
*Sysmon Execution History
*File Creation/Delete History
*Confirmation of Execution Success: Destination host: The "WMI_SHARE" share has been created and deleted.

"You can not grade your own homework"

Reference: "Detecting Lateral Movement Through Event Logs" JPCERT Coordination Center

Attack Simulation
What is the Mission?

Goals include:

- To test monitoring, detection and response capabilities by profiling well-known attacks/threat actors
- To **train** and measure an organization’s security implementations of people, process and technology
- To test resilience of threat detection and response
- To measure proof of concept technology implementations
- To gain the ability to predict likelihood of future attacks

Groce, E. “Knowing Your Battle Space - Part 1” https://security-storm.com/playbook/2017/9/14/knowing-your-battle-space-part-1

Attack Simulation

What it is:

- Execution of *planned* well-defined Tactics, Techniques and Procedures (TTPs) to mimic real-world attackers
- Wholistic view of organization's attack surface
- Security implementation validation
- "Environmental Drift"[1] detection
- Great attack simulation teams "generate experience"[2]

(1) Contos, B. "Environmental Drift and Continuous Security Validation" https://verodin.com/environmental-drift-2018-winter-olympics

(2) Gates, C & Nickerson, C. "Successful Internal Adversarial Simulation Team" BruCon 0x08 https://www.youtube.com/watch?v=Q5Fu6AvXi_A

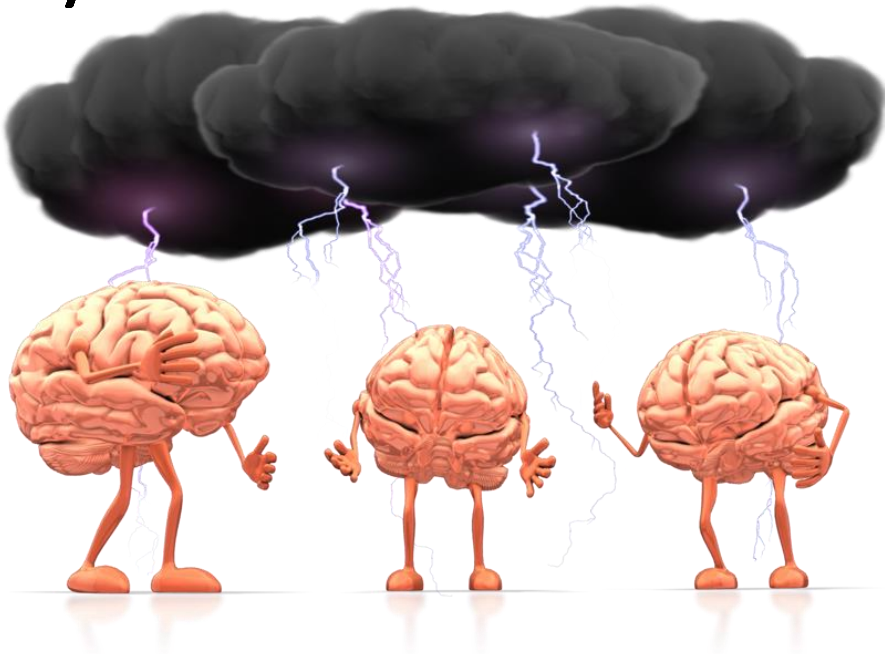
Attack Simulation
Uncovering Unanticipated Gaps

- IR Plans not up-to-date
- Communication processes flawed
- Responsibilities/roles not clearly defined
- Logs not being aggregated/preserved
- Data retention back-ups failed
- Security services not running
- Systems not remotely accessible for analysis
- Tools not compatible with target systems

Simulations Forecasts

Gather predictions from varied team perspectives

- Threat Hunting Analysts
- Threat Intel Analysts
- Cyber Scouts/Red Team/Pentesters
- Security Operations/Response Analysts
- Content Developers
- System/Application Owners
- Infrastructure Teams
- Management



Simulation Lessons Learned

Assess Prediction Data

- How accurate were predictions?
- Did the following elements meet expections?
  - Technologies
  - Monitor/Detection/Response Processes/Procedures
  - Escalation/TTD/TTR Timeframes
  - Intra/Inter-Team Communications
- Whose perspective best forecasted exercise results?
- Were exercises objectives realistic?

After-action Tasker: Uncover reasons for disconnects

Possible Causes for Flawed Forecasts

How to Use Prediction Data

- “Supposed to be there, never checked”
- Insufficient detection/response process
- Limited view into other teams’ processes
- Absence of validation steps for data collection
- Lack of visibility into retention limits

Action Items Derived from Failed Forecasts

How to Propel Maturity

- Address technologies that fell short of expectations
- Scope groups with wildly inaccurate predictions
- Schedule follow-ups on process/procedure development & vetting
- Capture overly optimistic estimations, blind spots of security posture
  - ”Thought we were patched for that!”
  - “Wait, no DNS logs?”

References

- Ryan McGeehan @Medium ”Starting up Security”, https://medium.com/starting-up-security
- “Guide to Test, Training and Exercises Planning” NIST SP800-84 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf
- Koegler, S. “How an Effective Incident Response Plan Can Help You Predict Your Security Future”, https://securityintelligence.com/how-an-effective-incident-response-plan-can-help-you-predict-your-security-future/
- JPCERT “Detecting Lateral Movement through Tracking Event Logs” https://www.jpcert.or.jp/english/pub/sr/20170612ac-ir_research_en.pdf
- Contos, B. “Environmental Drift and Continuous Security Validation” https://verodin.com/environmental-drift-2018-winter-olympics
- Gates, C & Nickerson, C. “Successful Internal Adversarial Simulation Team” BruCon 0x08 https://www.youtube.com/watch?v=Q5Fu6AvXi_A
- Verizon Data Breach Report 2018 https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf
- Groce, E. “Knowing Your Battle Space - Part 1” https://security-storm.com/playbook/2017/9/14/knowing-your-battle-space-part-1

FOR526

Advanced Memory Forensics
& Threat Detection