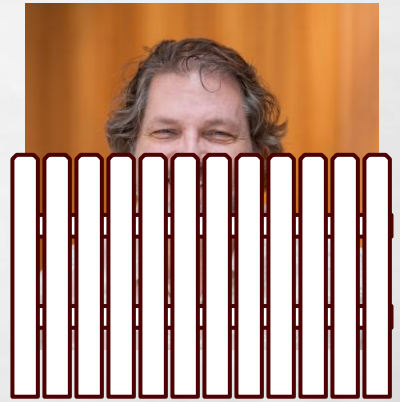
YOU WANT *ME* TO RUN A TABLETOP?

RON HAMANN

INSTRUCTOR

CONSULTANT

ABOUT ME



- RON HAMANN
  - SANS PRINCIPAL INSTRUCTOR – SECURITY 504
  - CYBER SECURITY ~~ENGINEERING SME, ANALYST, CONSULTANT,~~ … SOMETHING
    - USAF MEMBER *(LOOOONG RETIRED)*
    - SOC ANALYST
    - THREAT HUNTER
    - INCIDENT RESPONDER

WHY I'M GIVING THIS TALK

- BECAUSE I'VE BEEN THERE!
- THREE EXERCISES WRITTEN AND MODERATED OVER ABOUT A YEAR
  - ONE WENT WELL
  - ONE … NOT SO MUCH
  - ONE HIT THE TARGET

OVERVIEW

- WHAT'S THE GOAL?
- WHO'S THE AUDIENCE?
- WHERE DO I GET MY IDEAS?
- BUILDING THE SCENARIO
- THE DAY OF THE EXERCISE
- THE AFTERMATH

WHAT'S THE GOAL?

Knowing your goal – your organization's goal

What are you trying to achieve with the exercise?

- Are you training analysts?
- Are you evaluating – and what are you evaluating?
- Gap analysis?
- Compliance?

To varying levels, all of these *can* be valid goals

WHO IS THE AUDIENCE?

- THE AUDIENCE IS
  - WHO IS PLAYING
  - WHO IS WATCHING
  - WHO IS READING / FOLLOWING UP ON THE RESULTS
- KNOWING YOUR AUDIENCE ALLOWS YOU TO SELECT THE LEVEL OF DETAILS AND THE DIRECTION THE CONVERSATION GOES

WHERE DO I GET MY IDEAS?

- PROFESSIONAL SOURCES
  - INTERNET STORM CENTER
  - GOVERNING BODIES (E.G. CISA, NIST, CIS)
  - DATA BREACH REPORTS
- DAILY LIFE
  - WHAT KIND OF ALERTS ARE YOUR ANALYSTS SEEING?
  - WHAT KIND OF INCIDENTS HAVE YOU HAD?
- WORST CASE SCENARIOS
  - SUCCESSFUL RANSOMWARE
  - INSIDER THREAT

CHOOSING A STORY

- RECOMMENDATION: WHAT'S IMPORTANT TO YOUR BOSS SHOULD BE IMPORTANT TO YOU
  - WHAT ARE YOUR ORG'S CENTERS OF GRAVITY/CROWN JEWELS?
  - WHAT ARE THE NIGHTMARE SCENARIOS?
  - WHAT COULD BE AN EXISTENTIAL THREAT TO THE ORG?
  - WHAT KINDS OF ALERTS ARE CAUSING THE MOST TROUBLE?

Or as my director likes to say – what's making your customer's (or boss's) head hurt?

WRITING THE EXERCISE

- SELECT THE SCENARIO, THEN BRAINSTORM
- WHAT DID THE ATTACKER DO?
  - WHAT TACTICS DID THEY USE?
    - INITIAL ACCESS/LATERAL MOVEMENT/PERSISTENCE METHODS ATTEMPTED?
  - WHAT SYSTEMS HAVE BEEN AFFECTED?
  - WHAT DATA DID THEY ACCESS/TRY TO ACCESS?
  - HOW LONG WERE THEY IN THE ENVIRONMENT?

WRITING THE SCENARIO

- MAKE SURE YOU CREATE A TIMELINE OF EVENTS
  - TIMELINE SHOULD BE FROM THE *ATTACKER'S* POINT OF VIEW
  - CHOOSE A POINT ON THE TIMELINE FOR THE DETECTION
- THEN, IDENTIFY WHAT EVIDENCE THE ATTACKER WOULD LEAVE IN YOUR CURRENT ENVIRONMENT
  - LEVEL OF DETAIL DEPENDS ON THE PLAYERS AND THE GOAL OF THE TTX
  - HIGH LEVEL FOR MANAGERS AND DECISION MAKERS, OR LOW LEVEL FOR ANALYSTS AND INVESTIGATORS

TIMELINE

Event time	Action	Systems affected	Evidence
2025 Jul 25 1800CDT	Initial phishing message	User laptop	MS365 logs
2025 Jul 26 0917CDT	User saves attachment from message: “Scheduler.ISO”	User laptop	Sysmon event: file creation
2025 Jul 26 0919CDT	User mounts ISO	User Laptop	Proofpoint logs
2025 Jul 26 0920CDT	User opens file inside ISO	User Laptop	Sysmon process event Word opening file

WRITING THE SCENARIO

- CREATE EVIDENTIARY SUPPORT DOCUMENTS
  - LOGS
  - ALERTS
  - REGISTRY KEYS
- ANYTHING THAT YOU'D NEED TO TRIAGE AND INVESTIGATE
- CREATE INJECTS
  - SMALL PIECES OF DATA THAT SUPPORT OR EXTEND THE SCENARIO
  - INCLUDE THEM ON YOUR TIMELINE

```
Date: 2025-07-20T15:49:05Z
Event ID: 20001
Task Category: Device Install (PnP)
Level: Information
User: FIINC\AdamSmith
Computer: XCZ2019-44
Description:
Driver Management has concluded the process to install driver Kingston USB [

MountPoint: E:\
Device Type: Removable Storage
Serial Number: 12376544
Friendly Name: Kingston SpeedStick
Vendor ID: Kingston
User SID: S-1-5-21-3947621105-2498710933-1294387812-1001
IP Address: 192.168.204.12
Network Context: Corporate LAN
```

```
RecordType: SharePointFileOperation
CreationTime: 2025-07-20T16:37:45Z
Operation: FileDownloaded
UserId: adam.smith@fii.com
UserType: Regular
Workload: SharePoint
ClientIP: 192.168.204.12
UserAgent: Microsoft.Office.Client (16.0.16026.20238)
SiteUrl: https://financeinc.sharepoint.com/sites/Projects
SourceFileName: Wealth of Nations (draft).docx
SourceFilePath: Projects/inprogress/books/Wealth of Nations (draft).docx
FileExtension: docx
DestinationFilePath: E:\FinanceInc\Wealth of Nations (draft).docx
MachineName: XCZ2019-44
OrganizationId: FinanceInc
IsAdminOperation: false
ClientNetworkConnection: LAN
AdditionalDetails: {"DownloadType":"Save to removable media","ConnectionType
```

THE ACTUAL PLAYTIME WILL LIKELY GO FASTER THAN YOU THINK, PLAN FOR THIS WHILE WRITING!

WRITING THE SCENARIO

- WRITE QUESTIONS IN ADVANCE
  - THINK OF THE QUESTIONS AS A MODERATOR YOU WILL NEED TO ASK THE PLAYERS
  - QUESTIONS CAN BE USED TO DRAW PLAYERS OUT, OR LEAD PLAYERS THAT MAY BE STUCK
- RECOMMEND MORE DETAILED RATHER THAN LESS DETAILED
  - CONSIDER ALL RELEVANT DATES, TIMES, SYSTEMS AFFECTED
  - YOU CAN ALWAYS CHOOSE NOT TO USE THE DETAILS, BUT MAKING THEM UP ON THE SPOT IS A LOT HARDER!
- DETERMINE AN END STATE (FOR AN IR EXERCISE)

GAME DAY!

- ROLES
- PLAYTHROUGH
- INJECTS
- CLOSING

ROLES

- MODERATOR: LEADS THE DISCUSSION. MAINTAINS FLOW, DISPELS ARGUMENTS IF NECESSARY
  - MOST LIKELY WILL BE YOU THE AUTHOR
- RECORDER: TAKES DETAILED NOTES ON HOW THE EXERCISE WENT
  - QUESTIONS ASKED BY PLAYERS
  - ACTIONS TAKEN BY PLAYERS
- PARTICIPANTS: ACTIVE PLAYERS IN THE TTX
- OBSERVERS AND EVALUATORS
  - ANYONE WATCHING BUT NOT PLAYING

INTRODUCTION

- EXPLAIN THE PURPOSE OF THE TTX, EVEN IF YOU'VE DONE THIS BEFORE
- INTRODUCE PARTICIPANTS AND IDENTIFY WHAT ROLES THEY ARE TAKING
- INTRODUCE SCENARIO TO TEAM
- ASK FOR QUESTIONS

EVENT PLAYTHROUGH

- OPENING
  - PROVIDE THE INITIAL DATA FOR THE INCIDENT
  - TURN OVER DISCUSSION TO PLAYERS
- KEEP THE DISCUSSION FLOWING
  - ASK HOW THEY WOULD PROCEED
  - IT'S OK TO PROMPT FOR PROGRESS
- USE INJECTS AS NECESSARY
  - TO KEEP THE STORY GOING, TO ADJUST THE FLOW, TO DRAW IN OTHER PLAYERS

CLOSING DISCUSSION

- WRAP UP THE SCENARIO
- EXPLAIN THE FULL DETAILS
  - IF THE PLAYERS HAVE NOT ANSWERED ALL THE QUESTIONS OR REACHED THE END STATE
- DISCUSSION
  - WHAT WAS DISCOVERED
  - WHAT SHORTFALLS DID THEY ENCOUNTER
- STAKEHOLDER COMMENTS

AFTERMATH

- SOLICIT FEEDBACK
  - FROM PLAYERS
  - FROM STAKEHOLDERS/EVALUATORS/OBSERVERS
- WRITE REPORTS
  - USE THE NOTES!
- PLAN FOLLOW-ON ACTIVITIES
  - ALIGN FOLLOW ON ACTIVITES TO THE TTX GOAL

SUMMARY

- DO'S
  - IDENTIFY THE GOAL EARLY
  - UNDERSTAND YOUR ORGANIZATION'S NEEDS
  - BUILD A TIMELINE
- DON'TS
  - UNDERESTIMATE THE PLAYERS

RESOURCES

- STOIC
  - https://hefestis.ac.uk/nbstoic-ttx/
  - https://www.youtube.com/results?search_query=stoic+ttx
- CISA TTX scenarios
  - https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
- NIST 800-84
  - https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pd
- www.montance.com/resources
  - https://mgt517.com/tt