INSTITUTE FOR DEFENSE ANALYSES

Cyber Assessment Program Action Map Introduction

Walter R. Dodson, III, Project Leader

Jason R. Schlup

January 2022

IDA Document NS D-32938

Log: H 2022-000007

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication
This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-19-D-0001, Task BD-9-2377, "Cyber Exercises," for the Office of the Director, Operational Test and Evaluation. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments
The IDA Technical Review Committee was chaired by Mr. Robert R. Soule and consisted of Shawn C. Whetstone, Wendy-Angela S. Agata, Brian D. Vickers, Mark R. Herrera, and Jason M. Hustedt from the Operational Evaluation Division, and Jenny R. Holzer from the Science and Technology Division.

For more information:
Walter R. Dodson, Project Leader
wdodson@ida.org • (703) 845-2424

Robert R. Soule, Director, Operational Evaluation Division
rsoule@ida.org • (703) 845-2482

Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Document NS D-32938

Cyber Assessment Program Action Map Introduction

Walter R. Dodson, III, Project Leader

Jason R. Schlup

Executive Summary

DOT&E performs cybersecurity and mission assurance assessments of Combatant Command and Service networks as part of DOT&E's Cyber Assessment Program (CAP). Data from these assessments support analysis of how the cybersecurity posture across the Department of Defense changes from year to year.

DOT&E has specified data requirements that CAP participants should collect during assessment events, including an action map that describes cyber Red Team activities performed during the assessment. This briefing introduces and summarizes action maps to both new and experienced CAP members.

In the first section, we focus on the definition and requirements for an action map. Action map requirements from the CAP handbook dictate how frequently cyber Red Teams should create action maps and the required data elements that Red Teams should capture in action maps. The data elements include system descriptions of targeted hardware, technical descriptions of Red Team actions against the targeted hardware, and general notes summarizing broad red team activities. Each data element has an included example and expands on some of the most important aspects of the data.

Using MITRE's ATT&CK knowledge base of adversary tactics and techniques to describe Red Team activities is of particular note. This categorization will allow increased analysis fidelity, clearer communication of results, and easier integration with other efforts across the Department of Defense.

Next, we build on the action map requirements by creating an example action map based on data from MITRE's ATT&CK Evaluation program. The example uses a notional attack from the advanced persistent threat group APT28. First, we show how this attack may appear in an action map by creating an action map that resembles many current Red Team action map products. We then discuss how an action map that resembles recently collected action map data requires analysts to either interpret information from the provided data or ask clarification questions in an iterative manner.

We reproduce this typical action map using the ATT&CK knowledge base to define Red Team activities more completely. This fulfills data requirements from the CAP handbook while also providing a more complete technical description of Red Team activity.

Then, we describe how IDA uses an action map in analyses of the Department of Defense's cybersecurity posture. This involves creating an attack thread, a concept that links Red Team activities into a chain of actions from initial network ingress to either causing a cyber effect or being defended by network defenders. The attack threads rely heavily on the data required from action maps, including the categorization of Red Team activities. We then perform a statistical analysis of attack threads to reveal trends across different cross-sections of the Department of Defense.

We recognize that using the ATT&CK knowledge base to describe all Red Team activities in an assessment and requiring Red Teams to collect this fidelity of data will be significant. Additionally, the analysis of this quantity of data will require new techniques and models. We conclude that a development in data collection and analysis capabilities is required. DOT&E has previously explored and developed many of the required capabilities and we recommend that this development should continue.

DOT&E should also pursue development of integration techniques that will link the increased Red Team activity data collection with the automated creation of action maps and analysis capabilities. Finally, the CAP community should continue to expand the analysis techniques, especially as the CAP produces more technical data and information, to provide increasingly insightful cybersecurity findings to the Department of Defense.

DOT&E Cyber Assessment Program
Action Map Introduction

Walter Dodson – Project Leader
Jason Schlup
Shawn Whetstone

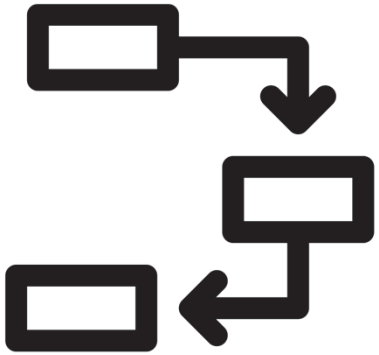
February 14, 2022

Institute for Defense Analyses
730 East Glebe Road ● Alexandria, Virginia 22305

Red Team data informs analysis of cyber defensive performance across the Department of Defense

This presentation gives Red Team data definitions, examples, and analysis methods

Definitions and Data Content



Data Collection

Data Analysis

The icons in the top left corner show the discussion topic for the given slide

DOT&E and IDA collaborate to address data collection and analysis challenges specific to the Cyber Assessment Program

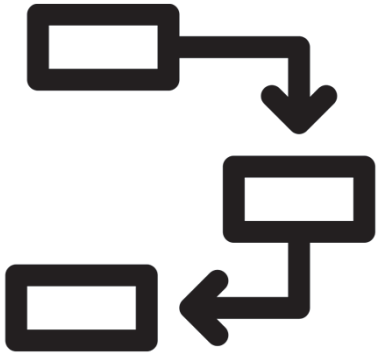
Varying missions and objectives

Unknown network ground truth

Red Team operational flexibility

Big data problem

Analysis fidelity based on available data



Existing:

Action map

Proposal:

Automated data collection

DOT&E adopted action maps to give graphical and technical descriptions of Red Team activities

DOT&E and IDA identified that data showing Red Team activity is useful for assessment outbriefs, Combatant Command reports, and Department-wide trend analyses

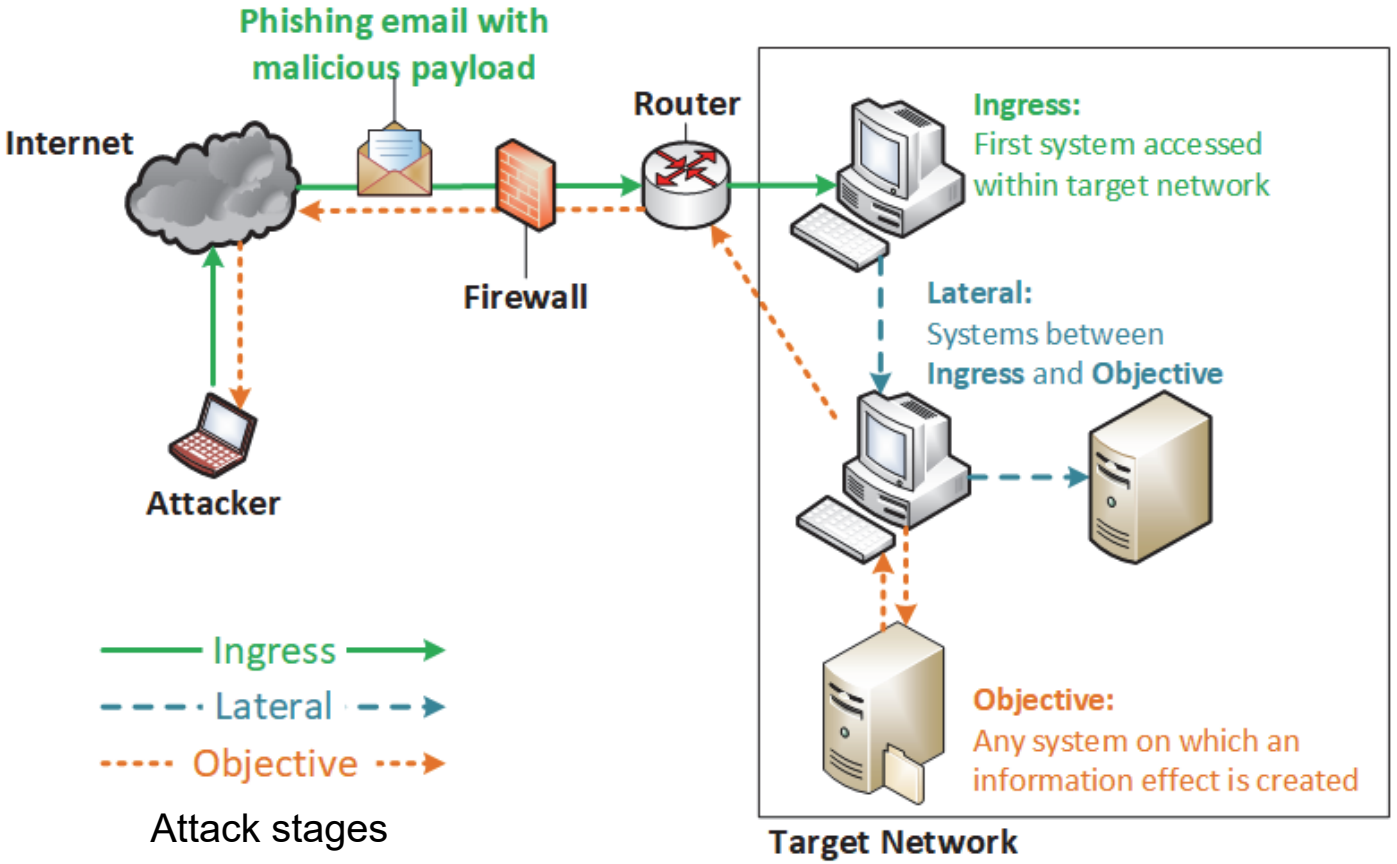
Action map defined as (see CAP Handbook[1]):

> "…the working report for Cyber Red Team activities during all operations, including during the reconnaissance phase. Action Map nodes and links will include data elements that describe the Red Team activities, position, and access."

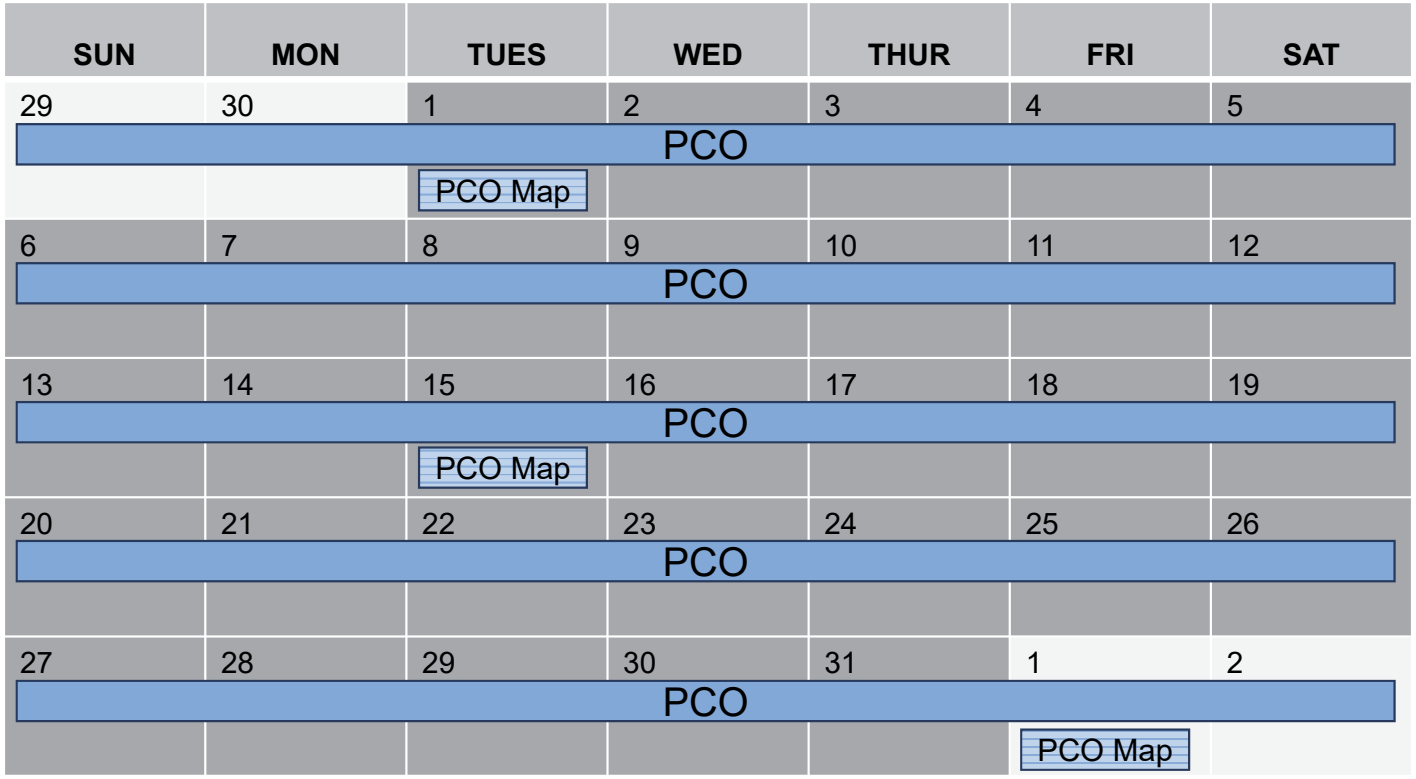
[1] DOT&E, "Cyber Assessment Program Handbook Version 4.1," May 2021.

CAP – Cyber Assessment Program

An action map provides a graphical depiction and technical detail of Red Team activities and their attack thread



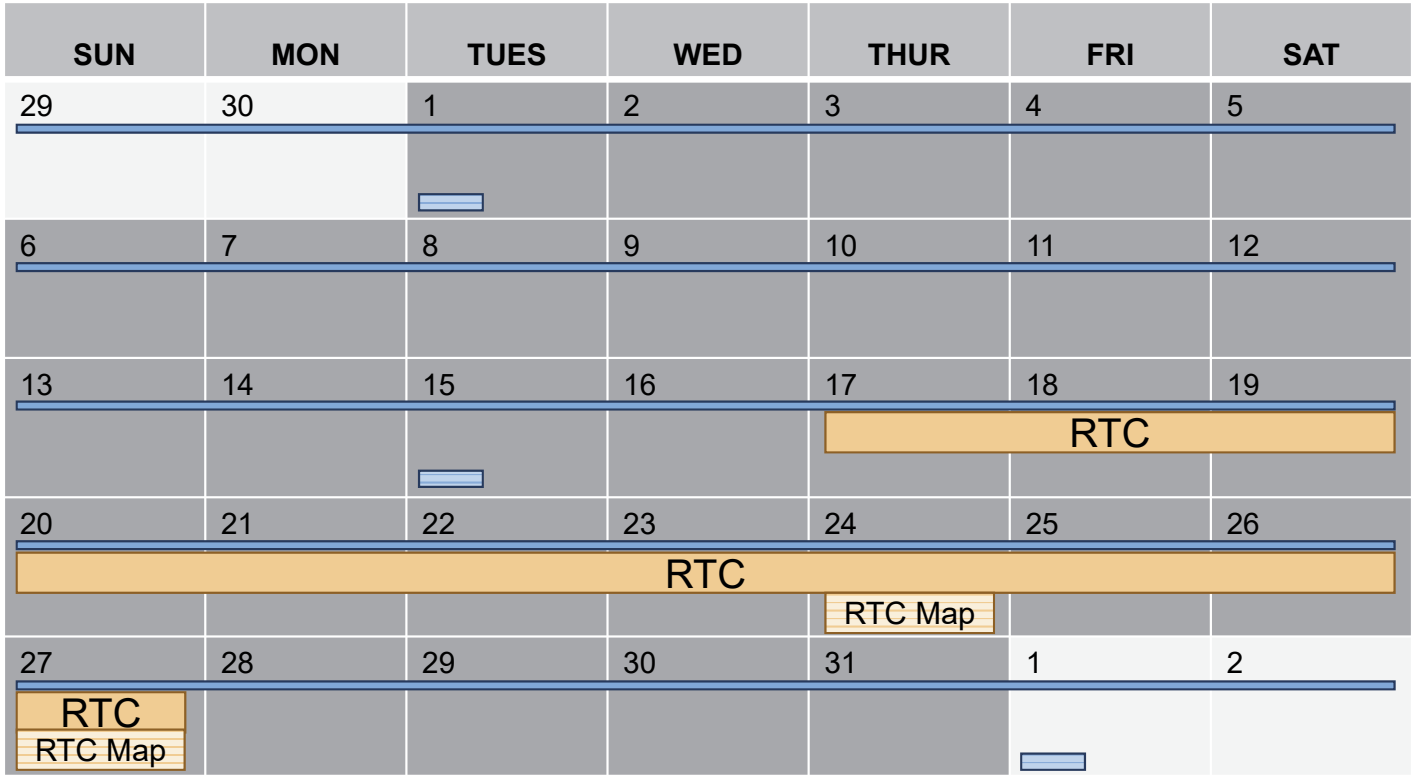
Action maps are created on a regular basis depending on the Red Team mission (approximately daily/weekly/monthly)



PCO action map frequency may vary and should be closely coordinated to ensure timely and efficient reporting.

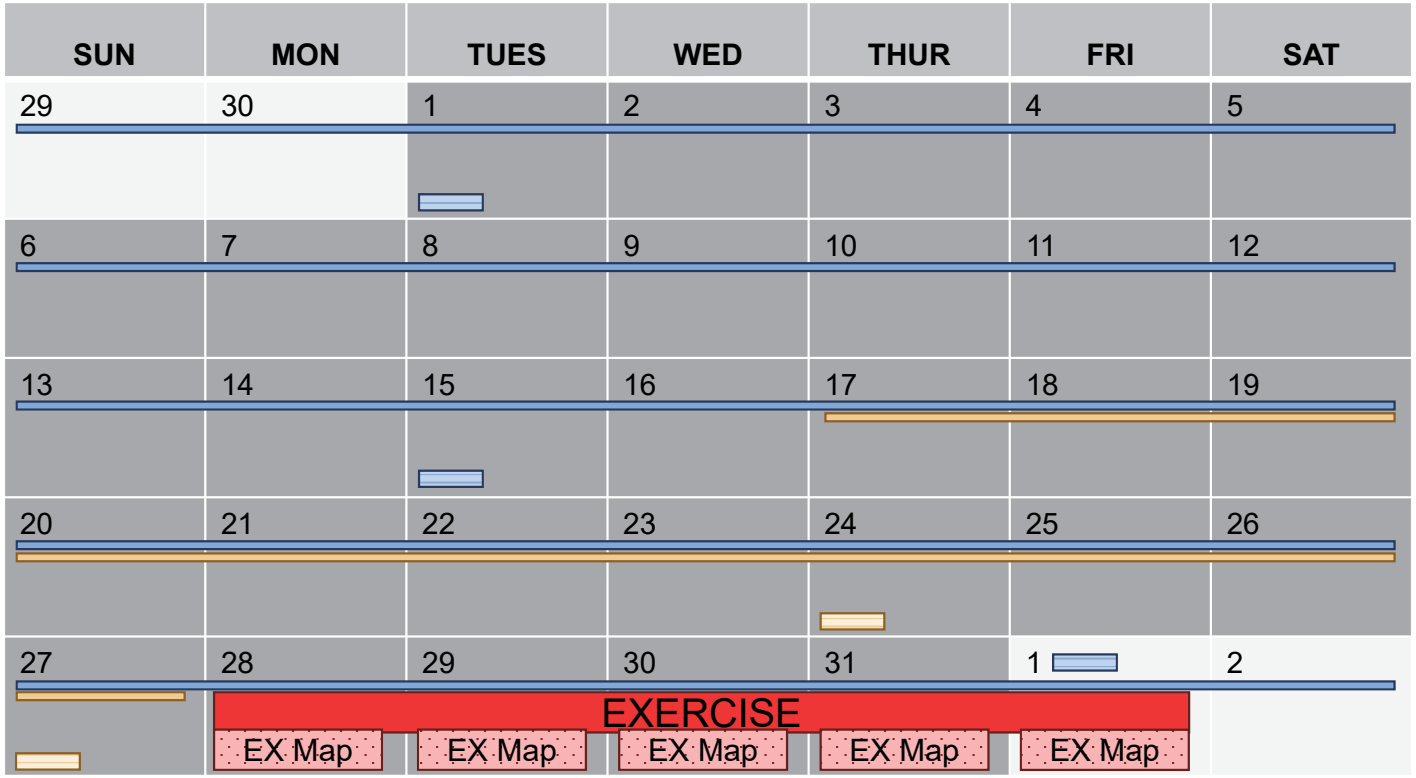
PCO – Persistent Cyber Operations

Action maps are created on a regular basis depending on the Red Team mission (approximately daily/weekly/monthly)



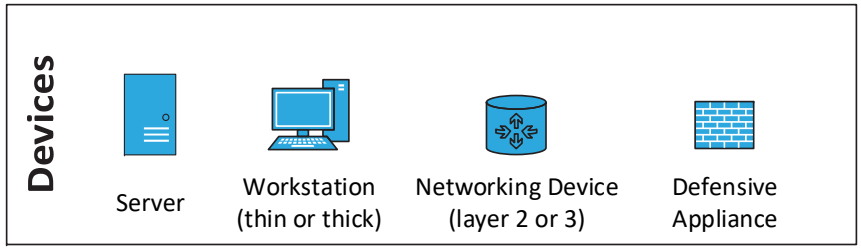
RTC – Road to Conflict

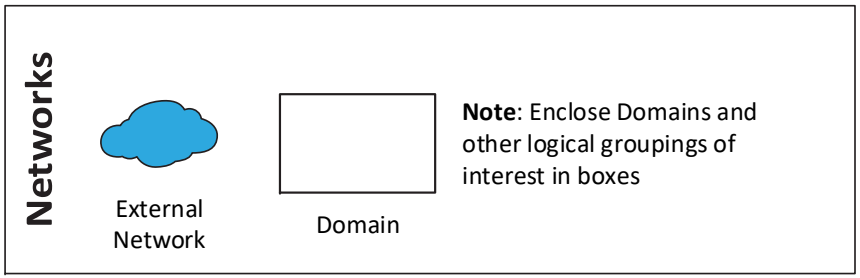
Action maps are created on a regular basis depending on the Red Team mission (approximately daily/weekly/monthly)

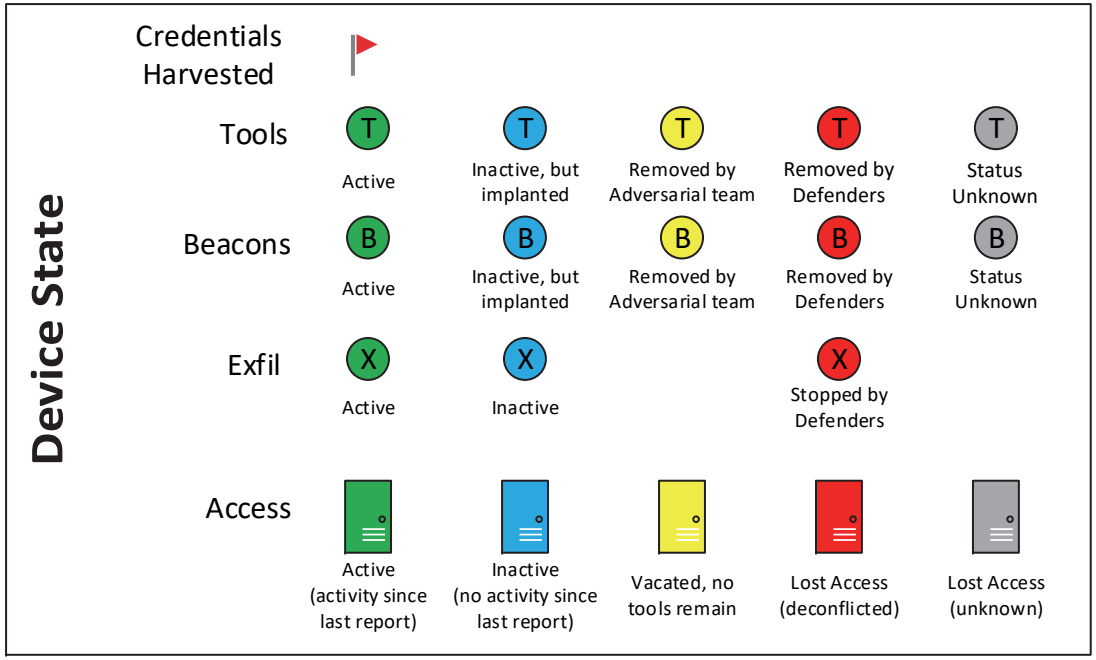


EX – Exercise

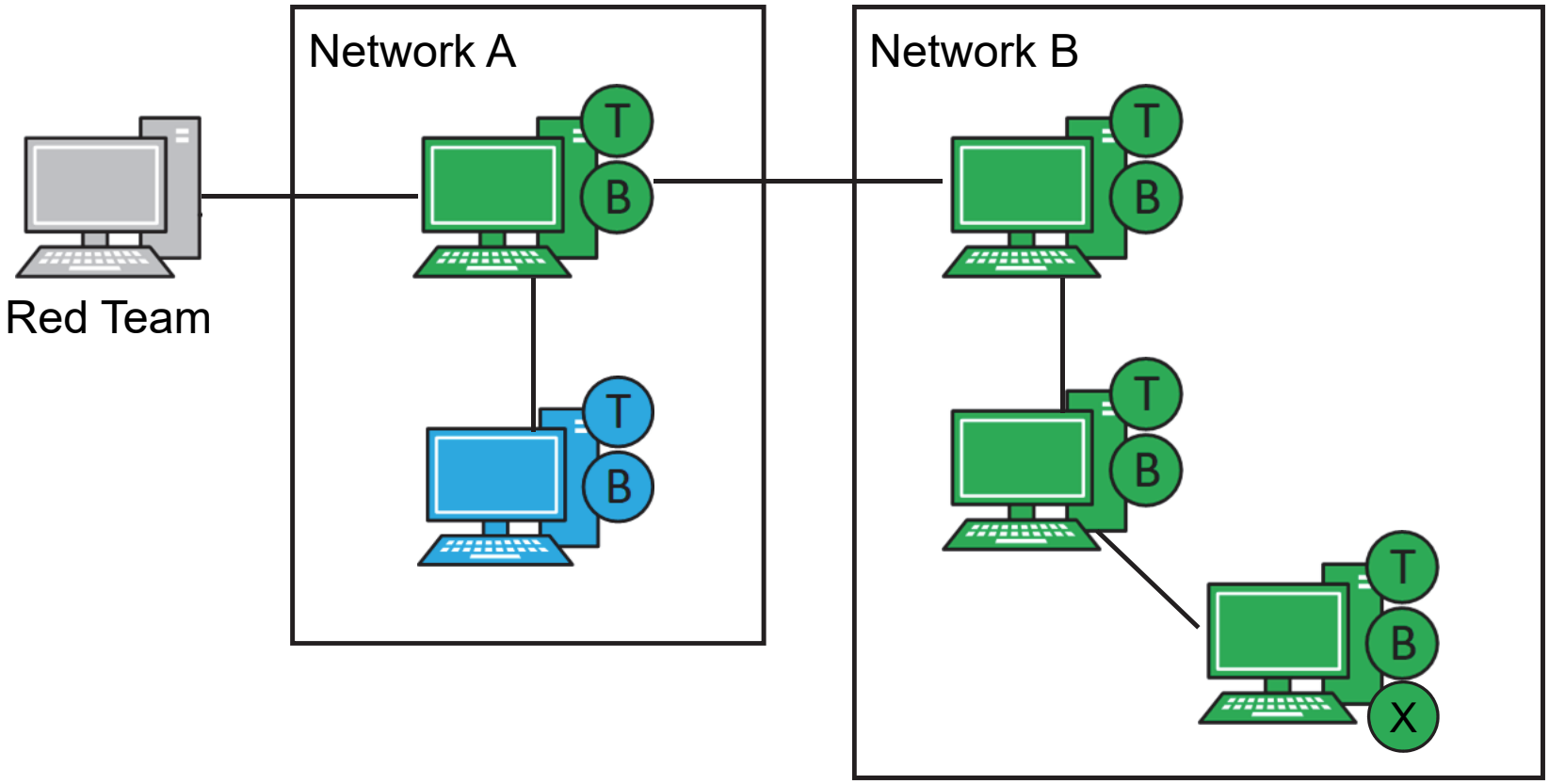
Red Teams use a “standard” symbol set to describe activities in action maps and simplify visualization of cyber campaign



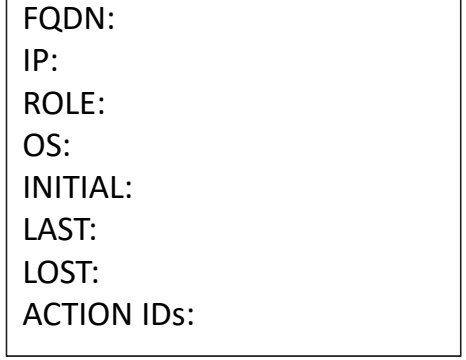




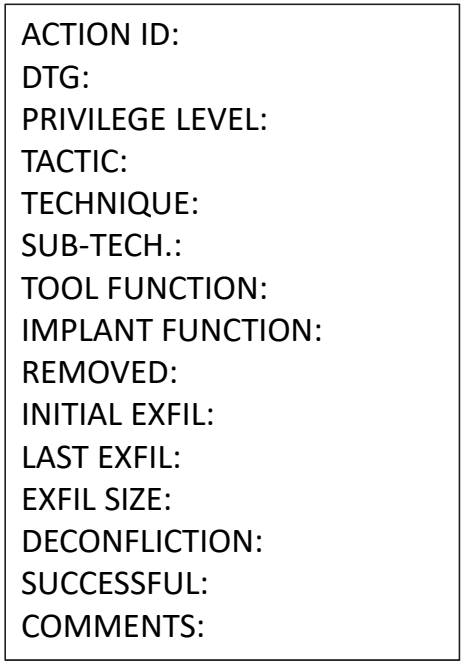
Uniform symbols and colors help visualize the current Red Team cyber campaign



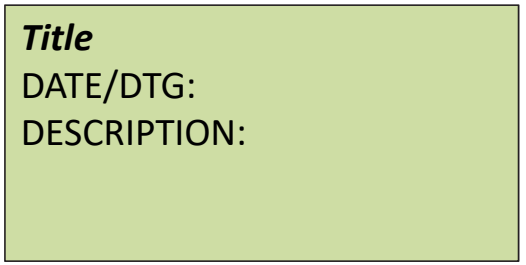
Beyond symbols and colors, an action map consists of three main data elements describing Red Team actions



System Description



Action Description



Note Field

DTG – Date-Time Group; FQDN – Fully Qualified Domain Name; ID – Identifier; IP – Internet Protocol; OS – Operating System

System descriptions provide technical and identifying details for every system Red Teams target

- Tracks unique identifiers of systems
  - If necessary, obfuscate FQDN/IP address
- Provides role of system for analytics
- Access dates provide timeline of Red Team network movements
- Action IDs help identify specific actions taken against systems toward Objectives and MRT-C

Example

FQDN: USER1.usmilbase.mil
IP: 12.13.14.15
ROLE: Workstation
OS: Win10
INITIAL: 1 JAN 2019
LAST: Current
LOST: N/A
ACTION IDs: 1

FQDN – Fully Qualified Domain Name; ID – Identifier; IP – Internet Protocol; MRT-C – Mission Relevant Terrain – Cyber; OS – Operating System

Notional data used on this slide.

Action descriptions provide details of each Red Team action, categorized using an action taxonomy

- Provides details of specific actions
- DTG provides timeline of Red Team actions and corresponding defender responses
- Privilege allows tracking of escalation and corresponding vulnerabilities
- Tactic, Technique, and Sub-technique from MITRE ATT&CK™
- Tool/functionality captures capability of tool, not specifics/signatures
- Comments field available for clarifications or additional details

Example

ACTION ID: 1
DTG: 011630 JAN 19
PRIVILEGE LEVEL: Domain Administrator
TACTIC: Initial Access
TECHNIQUE: Valid Accounts
SUB-TECH.: Domain Accounts
TOOL FUNCTION: RDP
DECONFLICTION: No
SUCCESSFUL: Yes
COMMENTS: Used known credentials to access this machine

DTG – Date-Time Group; ID – Identifier

Notional data used on this slide.

Note fields are general descriptions of widely used actions or notes and context of specific activities

- Overall descriptions
  - Initial credential source
  - Describing network movement
- Lumping similar actions together
  - Scanning
  - Wide-scale accesses
  - Installing tools in a similar manner
- More freeform, but should still include technical data and results of actions when possible

Example

Scanning
DATE: 01 JAN 19
DESCRIPTION: Scanned Domain A and Domain B from an outsider position.
- Scanned 12.13.14.0/24, 200 hosts up. 3 hosts with open port 80, 443. 5 hosts with open port 3389.
- Scanned 12.13.15.0/24. No hosts reachable.

Accesses
DATE: 02 JAN 19
DESCRIPTION: Accessed 50 workstations in Domain A using harvested creds. Accessed via remote file copy and starting service from 12.13.14.15. No additional actions taken on or from these 50 workstations.

Notional data used on this slide.

We will use an open-source attack example to visualize a sample action map

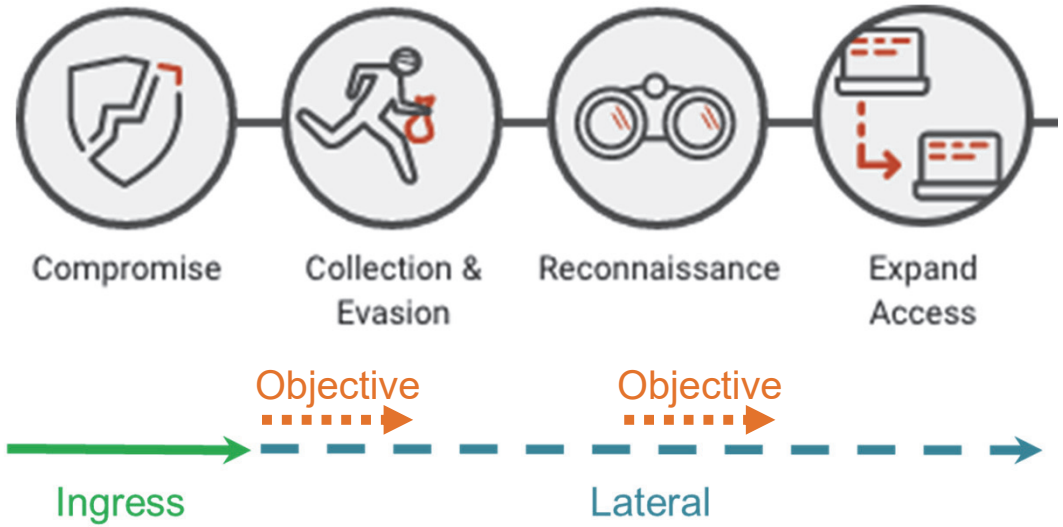
This presentation describes a notional APT29 (aka, Cozy Bear) campaign from the MITRE ATT&CK Evaluation program

This scenario begins with a **legitimate user clicking on a malicious payload** delivered via a “spray and pray” broad spearphishing.

APT – Advanced Persistent Threat

ATT&CK Evaluation data used on this slide.

This presentation describes a notional APT29 (aka, Cozy Bear) campaign from the MITRE ATT&CK Evaluation program

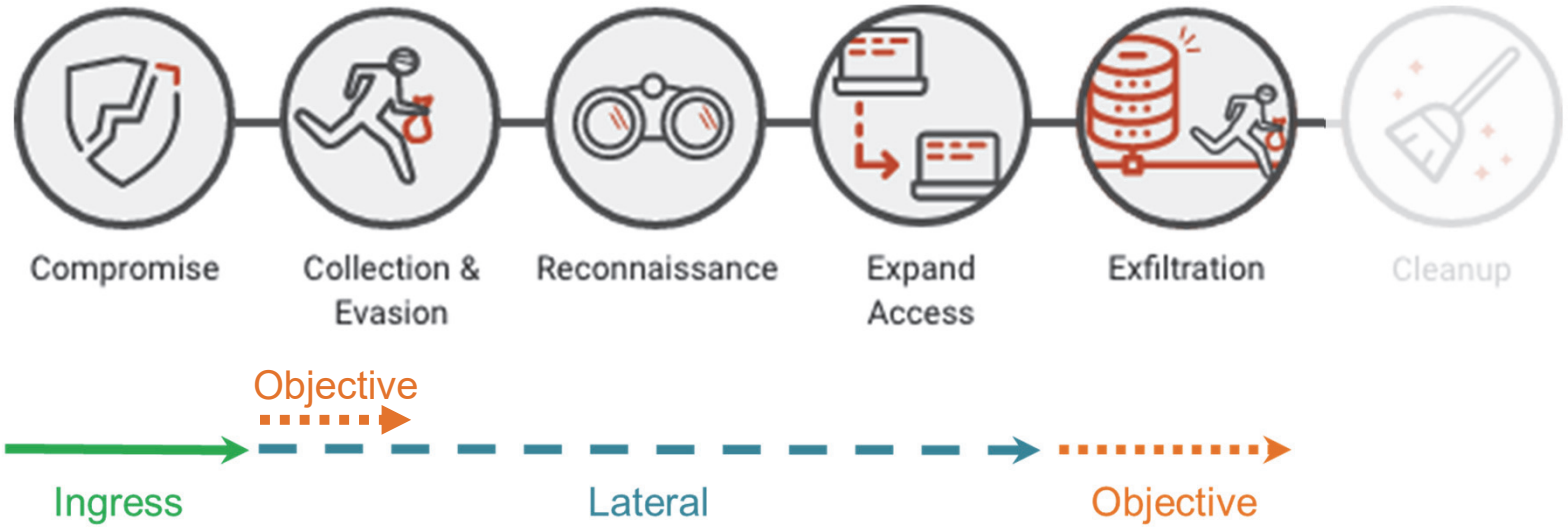


This scenario begins with a **legitimate user clicking on a malicious payload** delivered via a "spray and pray" broad spearphishing. The attacker immediately kicks off a **"smash-and-grab", rapid espionage mission, gathering and exfiltrating data**.

APT – Advanced Persistent Threat

ATT&CK Evaluation data used on this slide.

This presentation describes a notional APT29 (aka, Cozy Bear) campaign from the MITRE ATT&CK Evaluation program

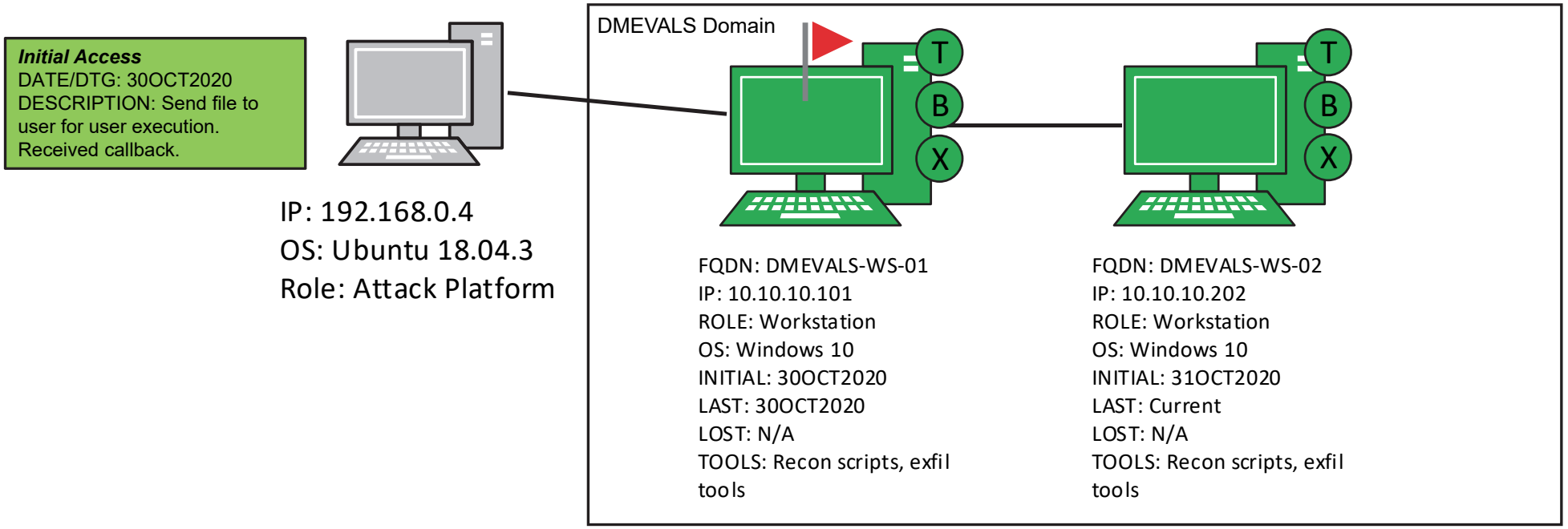


This scenario begins with a **legitimate user clicking on a malicious payload** delivered via a "spray and pray" broad spearphishing. The attacker immediately kicks off a **"smash-and-grab", rapid espionage mission, gathering and exfiltrating data**. After initial exfiltration, the attacker realizes the value of victim and **subsequently deploys a stealthier toolkit, changing TTPs and eventually moving laterally** through the rest of the environment for **continued data exfiltration**. The scenario ends with the execution of previously established persistence mechanisms.

APT – Advanced Persistent Threat; TTPs – Tactics, Techniques, and Procedures

ATT&CK Evaluation data used on this slide.

A typical action map may only include partial attack information and require analyst interpretation

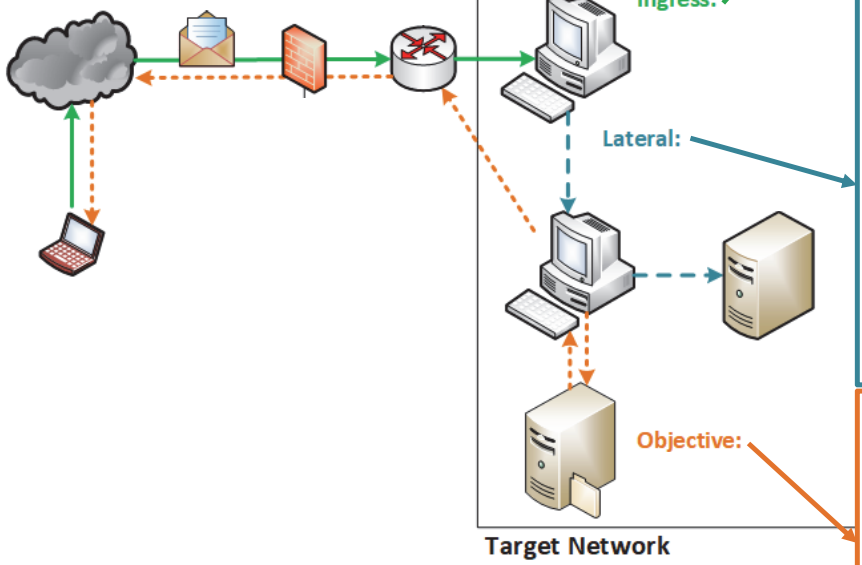


- Some data explicitly given (IP addresses, tool functionality)
- Provides some data, but will require additional info for more detailed analysis
- Interpret some data (e.g., node type, credential use)

DTG – Date-Time Group; FQDN – Fully Qualified Domain Name; IP – Internet Protocol; OS – Operating System

ATT&CK valuation data used on this slide.

Collect more data by thinking how you would reproduce the Red Team attack pathway



How did they get in?
- Credentials: Where did they come from? What tool or service did they use to pass credentials?
- Exploit: Phishing? What service? What exploit? Any special parameters needed?

How did they move laterally?
- Did they have to transfer a beacon?
  - What *is* a beacon? How does it communicate?
- What commands did they send to a beacon?
- Did they use defense evasion techniques?
- Did they use native OS commands or external tools?
- What level of access did they need for the tools to work?
- Did they use credentials? New ones or the same?

What happened on the objective node?
- Where did they find files (file shares, workstations, email, SharePoint/web portals)?
- Did they need credentials to access those sources?
- How much data and how was it transferred?
- How did availability effect occur? Disabled service?

OS – Operating System

Instead of broad descriptions of activities, we can record detailed technical information

First action: What is often recorded as “receive callback” actually contains five ATT&CK techniques and sub-techniques

Initial Access
DATE/DTG: 30OCT2020
DESCRIPTION: Send file to user for user execution. Received callback.

From MITRE ATT&CK Evaluation:

The scenario begins with an initial breach, where a legitimate user clicks (T1204 / T1204.002) an executable payload (screensaver executable) masquerading as a benign word document (T1036 / T1036.002). Once executed, the payload creates a C2 connection over port 1234 (T1065) using the RC4 cryptographic cipher. The attacker then uses the active C2 connection to spawn interactive cmd.exe (T1059 / T1059.003) and powershell.exe (T1086 / T1059.001).

Tactic: Execution
Technique: User Execution
Sub-tech.: Malicious File

Tactic: Defense Evasion
Technique: Masquerading
Sub-tech.: Right-to-Left Override

Tactic: Command and Control
Technique: Non-Standard Port
Sub-tech.: N/A

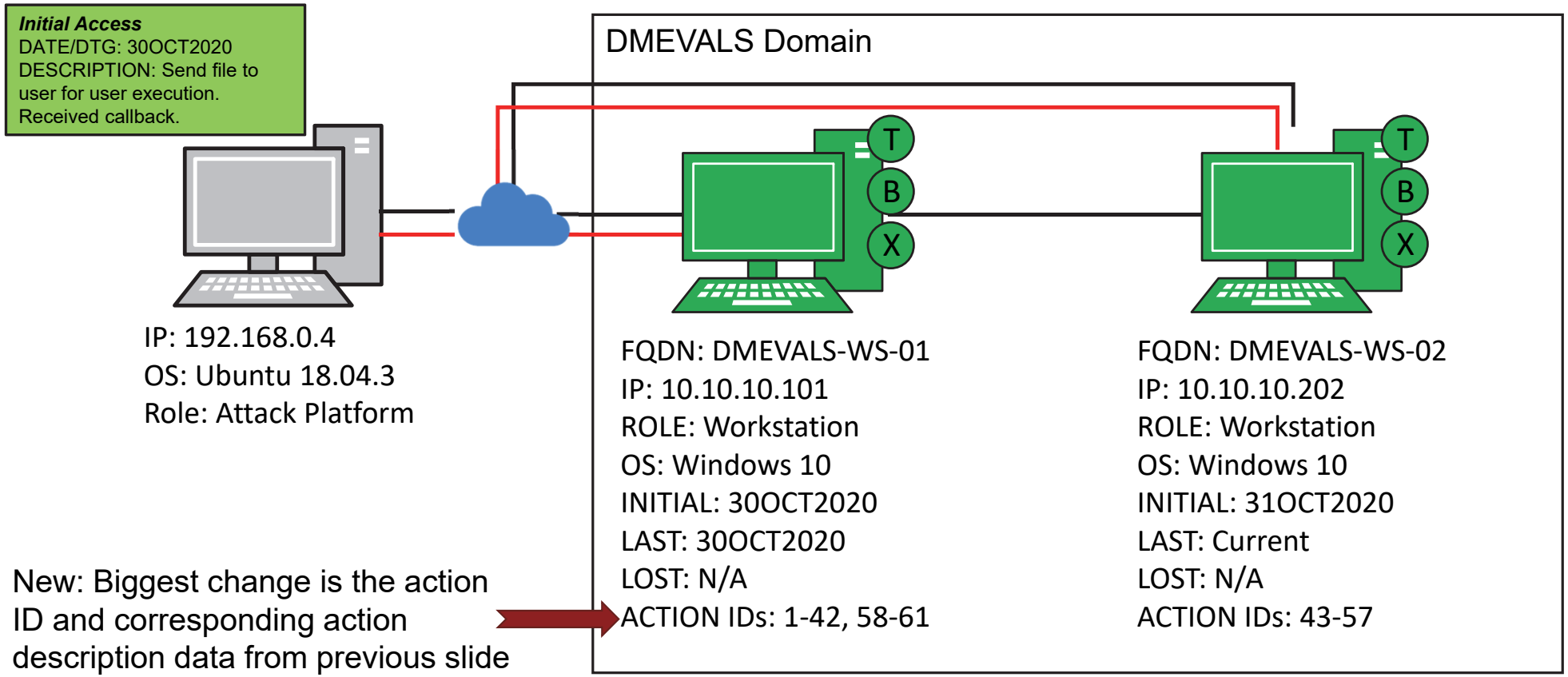
Tactic: Execution
Technique: Command and Scripting Interpreter
Sub-tech.: Windows Command Shell

Tactic: Execution
Technique: Command and Scripting Interpreter
Sub-tech.: PowerShell

C2 – Command and Control; DTG – Date-Time Group; RC4 – Rivest Cipher 4

ATT&CK Evaluation data used on this slide.

The final action map looks very similar to current action map deliverables, with separate action description data elements



DTG – Date-Time Group; FQDN – Fully Qualified Domain Name; ID – Identifier; IP – Internet Protocol; OS – Operating System

ATT&CK Evaluation data used on this slide.

The “received callback” can be described more completely using action description data elements and ATT&CK framework

We *can* collect this level of data for every Red Team activity…

Initial Gathering					
DATE/DTG: 29OCT2020 DESCRIPTION: Scanning of external website revealed potential list of phishing targets. Developed list of targets and prepared email and payload for specific spearphishing target.	ACTION ID: 1 DTG: 300800Z OCT2020 PRIVILEGE LEVEL: None TACTIC: Execution TECHNIQUE: User Execution SUBTECH: Malicious File TOOL: cod.3aka3.scr DECONFLICTION: No SUCCESSFUL: Yes COMMENTS: Screensaver executable	ACTION ID: 2 DTG: 300800Z OCT2020 PRIVILEGE LEVEL: None TACTIC: Defense Evasion TECHNIQUE: Masquerading SUBTECH: Right-to-Left Override TOOL: cod.3aka3.scr DECONFLICTION: No SUCCESSFUL: Yes COMMENTS: Executable masquerades as Word document	ACTION ID: 3 DTG: 300800Z OCT2020 PRIVILEGE LEVEL: User TACTIC: Command and Control TECHNIQUE: Non-Standard Port SUBTECH: N/A TOOL: cod.3aka3.scr DECONFLICTION: No SUCCESSFUL: Yes COMMENTS: Communicate over port 1234	ACTION ID: 4 DTG: 300801Z OCT2020 PRIVILEGE LEVEL: User TACTIC: Execution TECHNIQUE: Command and Scripting Interpreter SUBTECH: Windows Command Shell TOOL: cod.3aka3.scr DECONFLICTION: No SUCCESSFUL: Yes COMMENTS: Spawn interactive cmd.exe	ACTION ID: 5 DTG: 300801Z OCT2020 PRIVILEGE LEVEL: User TACTIC: Execution TECHNIQUE: Command and Scripting Interpreter SUBTECH: Powershell TOOL: cmd.exe DECONFLICTION: No SUCCESSFUL: Yes COMMENTS: Spawn interactive powershell.exe

. . .but this might be very time consuming.
The final section of this presentation proposes a method to collect this data.

DTG – Date-Time Group; ID – Identifier

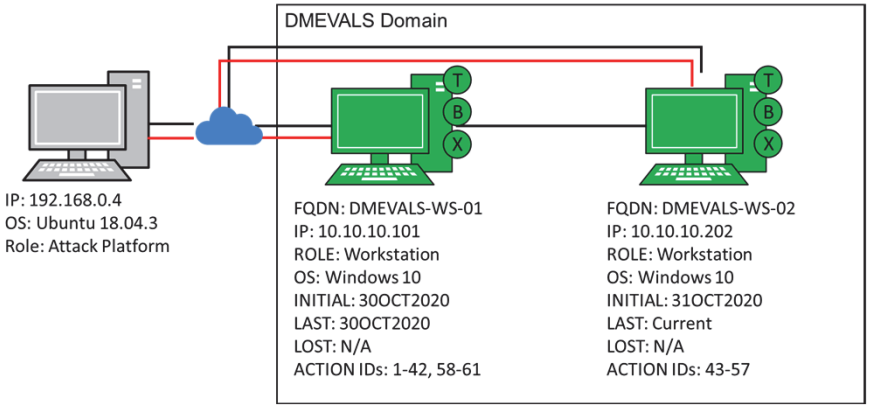
ATT&CK Evaluation data used on this slide.

IDA analysts then use action maps to evaluate defensive capability against Red Team attacks

The action map provides an easy-to-understand, but difficult-to-process, picture of an attack

Action Map
(Red Team product)

Attack Thread Spreadsheet
(IDA tool)

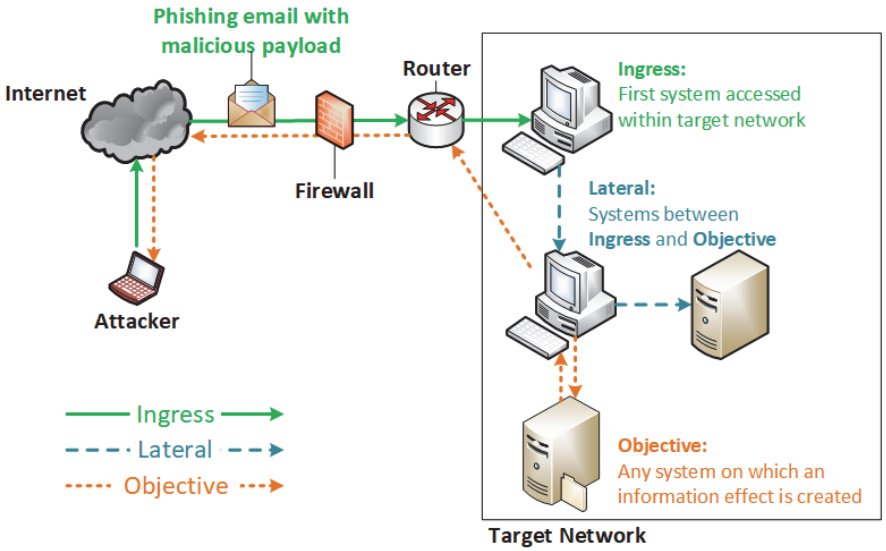


Activity No.	Antecedent(s)	Activity	Node	ATT&CK Tactic	ATT&CK Technique	ATT&CK Sub-Technique	Tool Type
1	N/A	Access	Ingress	Execution	User Execution	Malicious File	Foreign
2	1	Access	Ingress	Defense Evasion	Masquerading	Right-to-Left Override	Foreign
3	2	Access	Ingress	Command and Control	Non-Standard Port	N/A	Foreign
4	3	Access	Ingress	Execution	Command and Scripting Interpreter	Windows Command Shell	Foreign
5	4	Access	Ingress	Execution	Command and Scripting Interpreter	PowerShell	Native
6	5	Post-Access	Ingress	Discovery	File and Directory Discovery	N/A	Native
7	6	Post-Access	Ingress	Collection	Automated Collection	N/A	Native
8	6	Post-Access	Ingress	Collection	Data from Local System	N/A	Native
9	6, 7, 8	Post-Access	Ingress	Collection	Archive Collected Data	Archive via Utility	Native
10	9	Attack	Objective	Exfiltration	Exfiltration Over C2 Channel	N/A	Foreign
11	3	Post-Access	Ingress	Command and Control	Ingress Tool Transfer	N/A	Foreign
12	11	Post-Access	Ingress	Defense Evasion	Obfuscated Files or Information	Software Packing	Foreign
13	12	Post-Access	Ingress	Privilege Escalation	Event Triggered Execution	Component Object Model Hijacking	Native

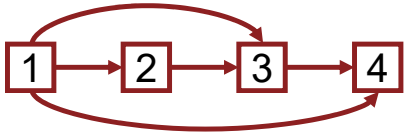
FQDN – Fully Qualified Domain Name; ID – Identifier; IP – Internet Protocol; OS – Operating System

ATT&CK Evaluation data used on this slide.

A primary objective of creating and using action maps is developing an end-to-end picture of the “attack thread”



Action maps track Red Team activity from network ingress to cyber effects (Confidentiality, Integrity, Availability)



Each action taken can have one or more preceding or succeeding actions, which creates an “attack thread”

IDA's spreadsheet tool details all Red Team-reported action map activities and links actions into attack threads

Activity No.	Antecedent(s)	Activity	Node	ATT&CK Tactic	ATT&CK Technique	ATT&CK Sub-Technique	Tool Type
1	N/A	Access	Ingress	Execution	User Execution	Malicious File	Foreign
2	1	Access	Ingress	Defense Evasion	Masquerading	Right-to-Left Override	Foreign
3	2	Access	Ingress	Command and Control	Non-Standard Port	N/A	Foreign
4	3	Access	Ingress	Execution	Command and Scripting Interpreter	Windows Command Shell	Foreign
5	4	Access	Ingress	Execution	Command and Scripting Interpreter	PowerShell	Native
6	5	Post-Access	Ingress	Discovery	File and Directory Discovery	N/A	Native
7	6	Post-Access	Ingress	Collection	Automated Collection	N/A	Native
8	6	Post-Access	Ingress	Collection	Data from Local System	N/A	Native
9	6, 7, 8	Post-Access	Ingress	Collection	Archive Collected Data	Archive via Utility	Native
10	9	Attack	Objective	Exfiltration	Exfiltration Over C2 Channel	N/A	Foreign
11	3	Post-Access	Ingress	Command and Control	Ingress Tool Transfer	N/A	Foreign
12	11	Post-Access	Ingress	Defense Evasion	Obfuscated Files or Information	Software Packing	Foreign
13	12	Post-Access	Ingress	Privilege Escalation	Event Triggered Execution	Component Object Model Hijacking	Native

ATT&CK Evaluation data used on this slide.

IDA's spreadsheet tool details all Red Team-reported activities and links actions into attack threads

Activity No.	Antecedent(s)
1	N/A
2	1
3	2
4	3
5	4
6	5
7	6
8	6
9	6, 7, 8
10	9
11	3
12	11
13	12

Critical Information:

- Activity No.: Unique ID for each activity
- Antecedent: Activity No. that precedes current activity

ID – Identifier

ATT&CK Evaluation data used on this slide.

IDA's spreadsheet tool details all Red Team-reported activities and links actions into attack threads

Activity	Node
Access	Ingress
Access	Ingress
Access	Ingress
Access	Ingress
Access	Ingress
Post-Access	Ingress
Post-Access	Ingress
Post-Access	Ingress
Post-Access	Ingress
Attack	Objective
Post-Access	Ingress
Post-Access	Ingress
Post-Access	Ingress

Critical Information:

- Activity No.: Unique ID for each activity
- Antecedent: Activity No. that precedes current activity
- Activity: Pre-Ingress, Access, Post-Access, Attack
- Node: Ingress, Lateral, Objective

ID – Identifier

ATT&CK Evaluation data used on this slide.

IDA's spreadsheet tool details all Red Team-reported activities and links actions into attack threads

ATT&CK Tactic	ATT&CK Technique	ATT&CK Sub-Technique
Execution	User Execution	Malicious File
Defense Evasion	Masquerading	Right-to-Left Override
Command and Control	Non-Standard Port	N/A
Execution	Command and Scripting Interpreter	Windows Command Shell
Execution	Command and Scripting Interpreter	PowerShell
Discovery	File and Directory Discovery	N/A
Collection	Automated Collection	N/A
Collection	Data from Local System	N/A
Collection	Archive Collected Data	Archive via Utility
Exfiltration	Exfiltration Over C2 Channel	N/A
Command and Control	Ingress Tool Transfer	N/A
Defense Evasion	Obfuscated Files or Information	Software Packing
Privilege Escalation	Event Triggered Execution	Component Object Model Hijacking

Critical Information:

- Activity No.: Unique ID for each activity
- Antecedent: Activity No. that precedes current activity
- Activity: Pre-Ingress, Access, Post-Access, Attack
- Node: Ingress, Lateral, Objective
- ATT&CK Tactic
- ATT&CK Technique
- ATT&CK Sub-Technique

ID – Identifier

ATT&CK Evaluation data used on this slide.

IDA's spreadsheet tool details all Red Team-reported activities and links actions into attack threads

ATT&CK Sub-Technique	Tool Type
Malicious File	Foreign
Right-to-Left Override	Foreign
N/A	Foreign
Windows Command Shell	Foreign
PowerShell	Native
N/A	Native
N/A	Native
N/A	Native
Archive via Utility	Native
N/A	Foreign
N/A	Foreign
Software Packing	Foreign
Component Object Model Hijacking	Native

ID – Identifier

Critical Information:

- Activity No.: Unique ID for each activity
- Antecedent: Activity No. that precedes current activity
- Activity: Pre-Ingress, Access, Post-Access, Attack
- Node: Ingress, Lateral, Objective
- ATT&CK Tactic
- ATT&CK Technique
- ATT&CK Sub-Technique
- Tool Type: Native (present on target computer) or Foreign (brought by Red Team)

ATT&CK Evaluation data used on this slide.

We collect other data points for future analysis techniques and methods

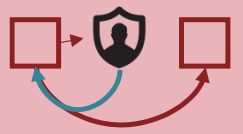
Detailed attack pathway analysis

Action timing

Network starting posture

Domain starting posture

Target identifier



Defensive antecedents

System trends across DODIN

Device

System/OS

Service

Red Team outcome

DODIN – Department of Defense Information Networks

Once data is in an organized and standardized format, create attack threads for analyses

Define an attack thread by starting at the end – what actions led to a cyber effect or a successful defense?

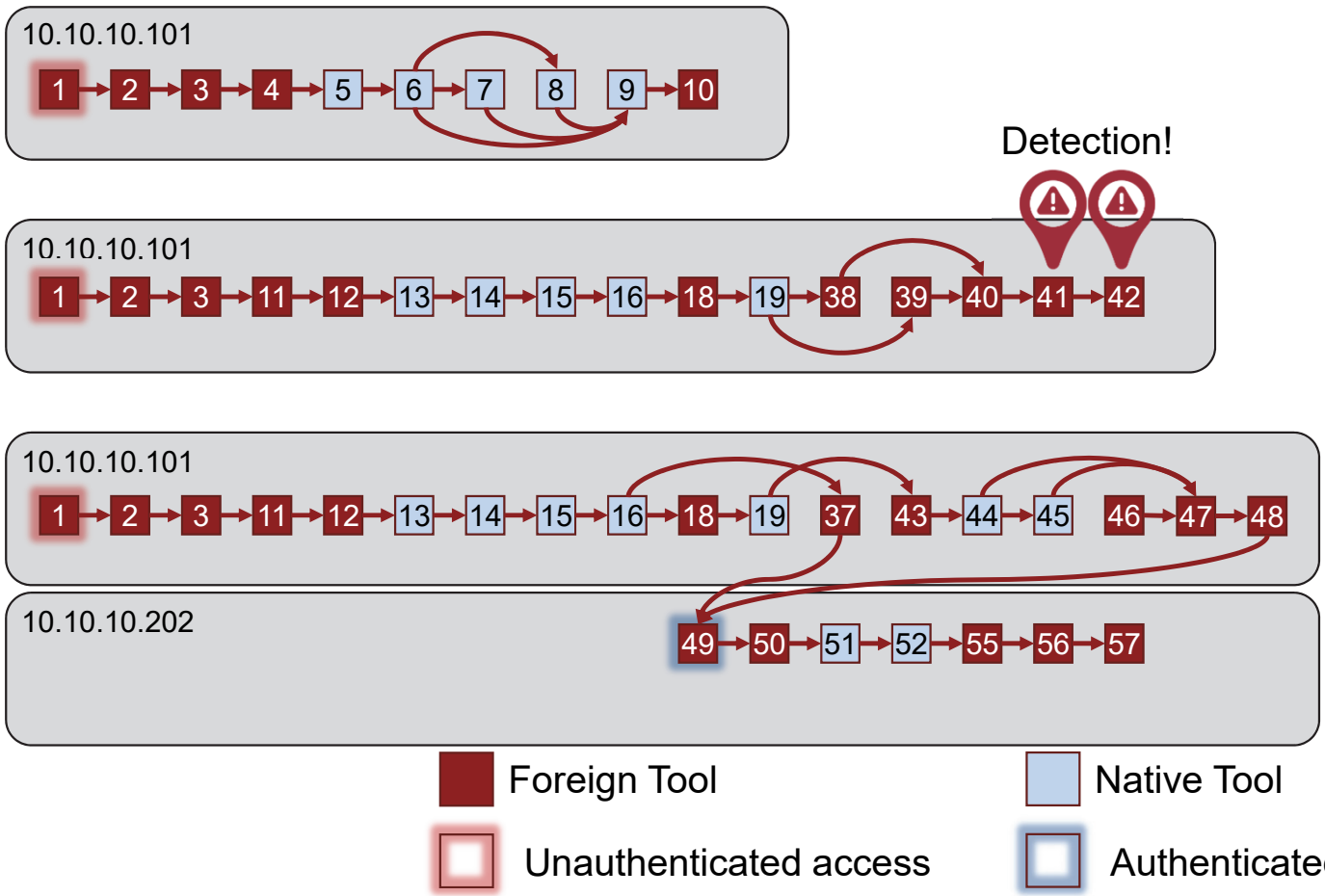
Activity No.	Antecedent(s)	Activity	Node	ATT&CK Tactic	ATT&CK Technique	ATT&CK Sub-Technique	Tool Type
1	N/A	Access	Ingress	Execution	User Execution	Malicious File	Foreign
2	1	Access	Ingress	Defense Evasion	Masquerading	Right-to-Left Override	Foreign
3	2	Access	Ingress	Command and Control	Non-Standard Port	N/A	Foreign
4	3	Access	Ingress	Execution	Command and Scripting Interpreter	Windows Command Shell	Foreign
5	4	Access	Ingress	Execution	Command and Scripting Interpreter	PowerShell	Native
6	5	Post-Access	Ingress	Discovery	File and Directory Discovery	N/A	Native
7	6	Post-Access	Ingress	Collection	Automated Collection	N/A	Native
8	6	Post-Access	Ingress	Collection	Data from Local System	N/A	Native
9	6, 7, 8	Post-Access	Ingress	Collection	Archive Collected Data	Archive via Utility	Native
10	9	Attack	Objective	Exfiltration	Exfiltration Over C2 Channel	N/A	Foreign

- APT29 Evaluation has three cyber effects: three exfiltration (confidentiality) activities
- Method: Find "attack" on an objective node, look at antecedent, then look at that action's antecedent …
- Attack thread: 10 > 9 > {8,7} > 6 > 5 > 4 > 3 > 2 > 1
- Ten actions, five using foreign tools, five using native tools

APT – Advanced Persistent Threat

ATT&CK Evaluation data used on this slide.

Visualizing the attack threads highlights the variety of methods, length, and complexity of each attack

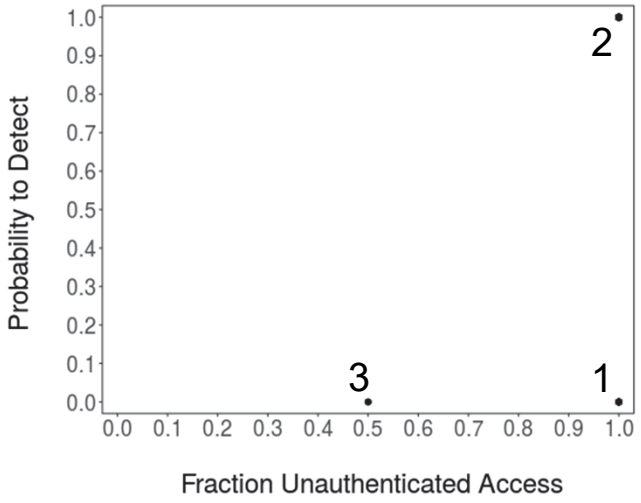


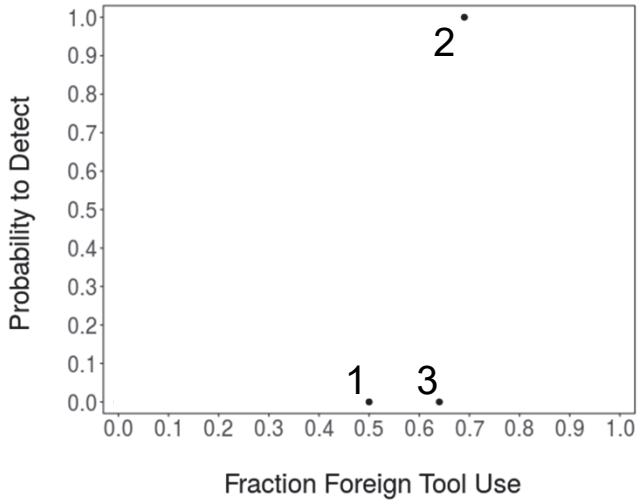
- Attack #1:
  - Ten actions, file exfil.
  - Five foreign tool, five native tool
  - One unauthenticated access
- Attack #2:
  - Sixteen actions, screenshot exfil.
  - Eleven foreign tool, five native tool
  - One unauthenticated access
  - "Assume" two detections, no defense
- Attack #3:
  - Twenty-five actions, file exfil.
  - Sixteen foreign tool, nine native tool
  - One unauthenticated access, one authenticated access

ATT&CK Evaluation data used on this slide.

Consider a binary logistic regression for detection probabilities based on the fraction of foreign tools used and fraction of authenticated accesses

Attack #	Fraction Unauthent. Access	Fraction Foreign Tool Use	Detected?
1	1.00	0.50	0
2	1.00	0.69	1
3	0.50	0.64	0

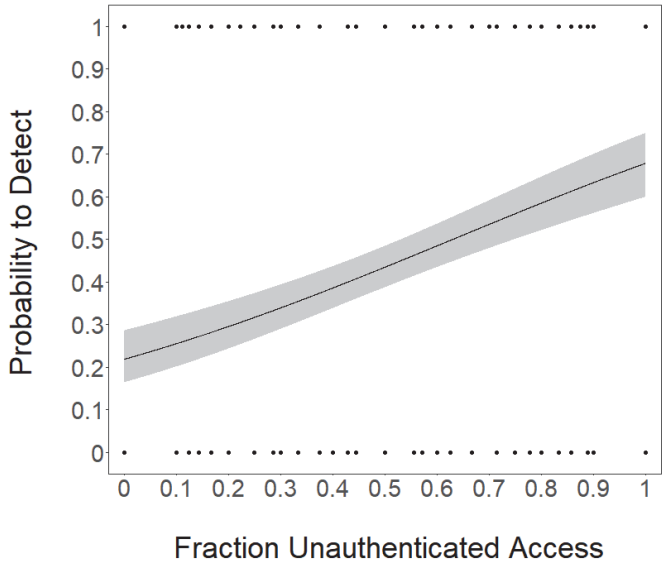


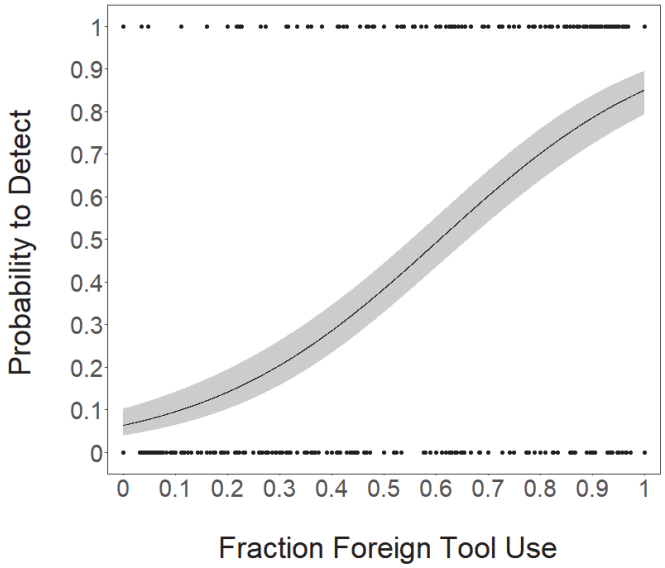


ATT&CK Evaluation data used on this slide.

Compiling data from this evaluation and other assessments generates dataset that we can analyze

Attack #	Fraction Unauthent. Access	Fraction Foreign Tool Use	Detected?
1	1.00	0.50	0
2	1.00	0.69	1
3	0.50	0.64	0
4	0.00	0.82	0
5	0.44	0.08	0
6	0.63	0.14	0
7	0.00	0.29	0
8	1.00	0.33	1
9	0.00	0.40	0
10	0.80	0.62	1
	. . .	. . .	. . .



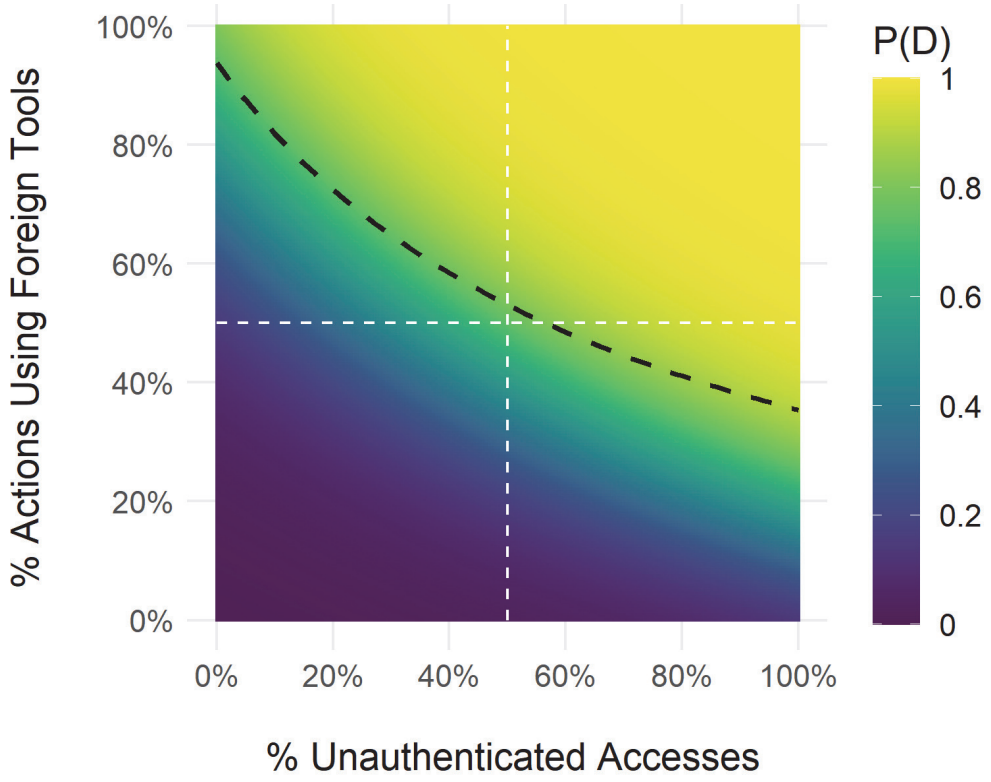


Notional data used on this slide.

Compiling data from this evaluation and other assessments generates dataset that we can analyze

Attack #	Fraction Unauthent. Access	Fraction Foreign Tool Use	Detected?
1	1.00	0.50	0
2	1.00	0.69	1
3	0.50	0.64	0
4	0.00	0.82	0
5	0.44	0.08	0
6	0.63	0.14	0
7	0.00	0.29	0
8	1.00	0.33	1
9	0.00	0.40	0
10	0.80	0.62	1
	. . .	. . .	. . .

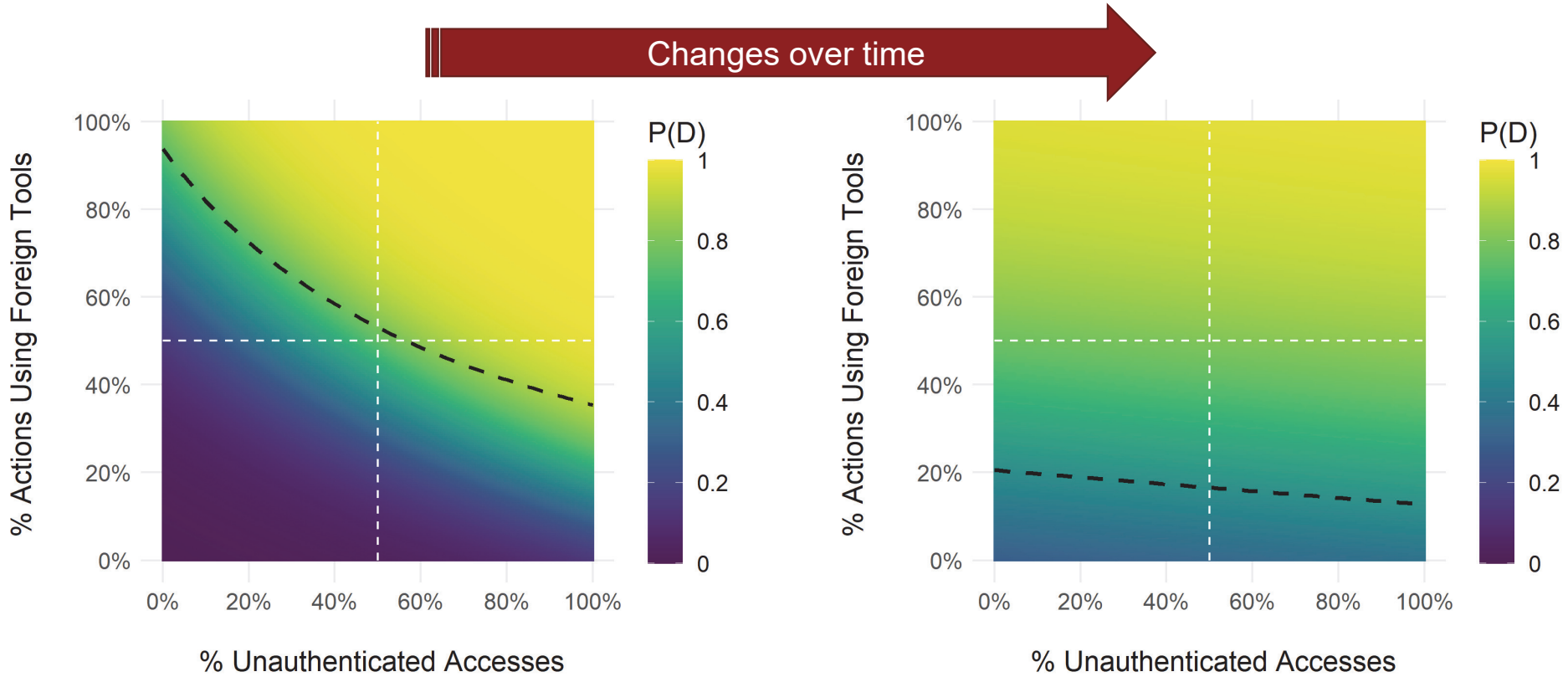
P(D) – Probability to Detect



Notional data used on this slide.

These analyses allow us to investigate trends across Commands and years

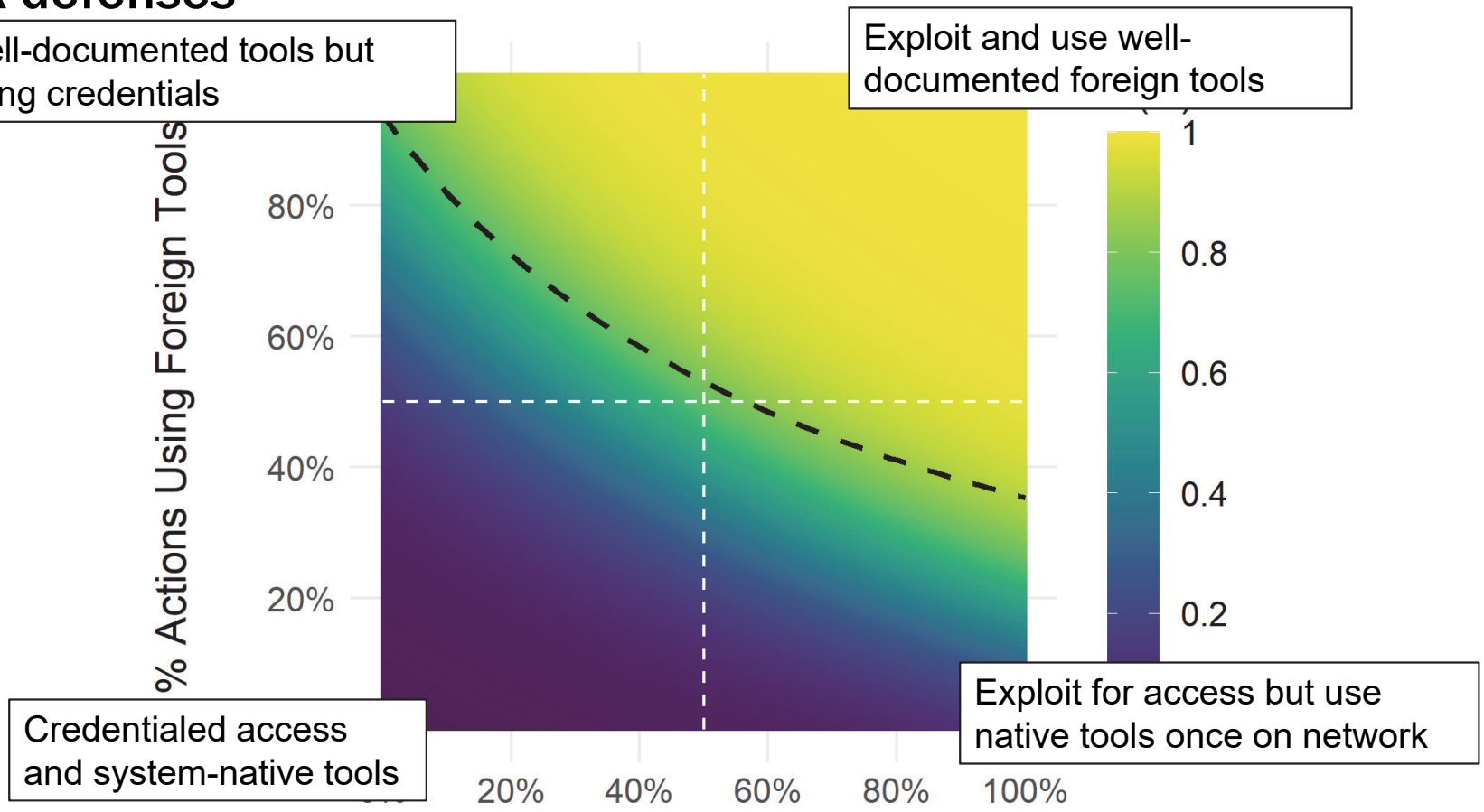
The logistic regressions can show how defensive capabilities across many organizations change over time



P(D) – Probability to Detect

Notional data used on this slide.

The logistic regression factors also help identify unique areas with strong or weak defenses

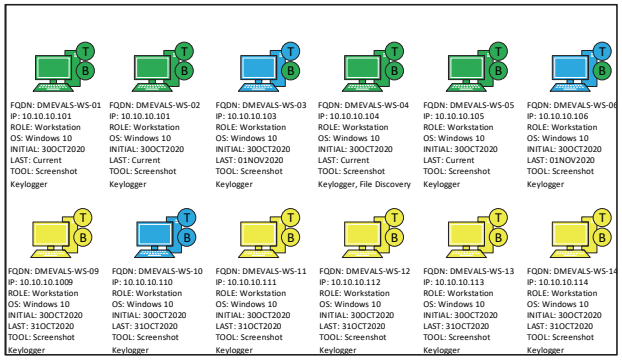


Notional data used on this slide.

Action map data collection and analysis can be challenging, so let us find solutions

The current action map format and data collection method puts strain on Red Teams each day

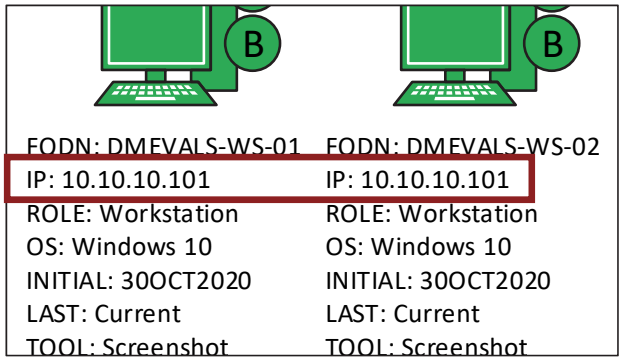
Time intensive



Lack of detail

FQDN: DMEVALS-FS-01	FQDN: DMEVALS-FS-02
IP: 10.10.10.51	IP: 10.10.10.52
ROLE: Workstation	ROLE: Workstation
OS: Windows 10	OS: Windows 10
INITIAL: 30OCT2020	INITIAL: 30OCT2020
LAST: Current	LAST: Current
TOOL: Screenshot	TOOL: Screenshot
File Discovery	File Discovery

Error prone



FQDN: DMEVALS-WS-01	FQDN: DMEVALS-WS-02
IP: 10.10.10.101	IP: 10.10.10.101
ROLE: Workstation	ROLE: Workstation
OS: Windows 10	OS: Windows 10
INITIAL: 30OCT2020	INITIAL: 30OCT2020
LAST: Current	LAST: Current
TOOL: Screenshot	TOOL: Screenshot

Initial Access
DATE/DTG: 30OCT2020
DESCRIPTION: Use credentials from HavelBeenPwned to access AF Network 1 and AF Network 2

Requires clarification

AF – Air Force; DTG – Date-Time Group; FQDN – Fully Qualified Domain Name; IP – Internet Protocol; OS – Operating System

Notional data used on this slide.

Red Teams often include their “primary” activities, but often omit amplifying information (e.g., the “how” and “why”)

Activity No.	Antecedent(s)	Activity	Node	ATT&CK Tactic	ATT&CK Technique	ATT&CK Sub-Technique
1	N/A	Access	Ingress	Execution	User Execution	Malicious File
2	1	Access	Ingress	Defense Evasion	Masquerading	Right-to-Left Override
3	2	Access	Ingress	Command and Control	Non-Standard Port	N/A

Primary action: What was the primary action Red Teams needed to advance attack?
- User execution of malicious file

Enabling actions: What did the Red Team do to have successful execution?
- Evade defenses via masquerading
- Establish C2 over non-standard port

Red Team’s goal isn’t to masquerade a file or use a non-standard port…these are a means to have successful user execution

C2 – Command and Control

Notional data used on this slide.

Defensive data collection is also challenging because we collect data indirectly

Detected Red Team activity notifications may come from:

- Red Team daily summaries
- JFHQ-DODIN Significant Activity portal
- Outbrief tech-on-tech
- Defender interviews/discussions

Some detections may not be reported (handled internally) or may not be noticed by defenders (automatic tools)

Defensive "playbook" and capability analysis

Defensive action timing

OPFOR antecedent

Defense phase

Detection technique

Responding agency

Responder tier

Response and recovery action

JFHQ-DODIN – Joint Force Headquarters-Department of Defense Information Network; OPFOR – Opposing Force

If we could collect details on all Red Team activities, we can investigate important and interesting questions

Refined Department-wide trends and annual changes of:

- Detection and response timelines
- Mitigation capabilities against specific adversarial actions
- Critical system properties
- Precursors to successful attacks

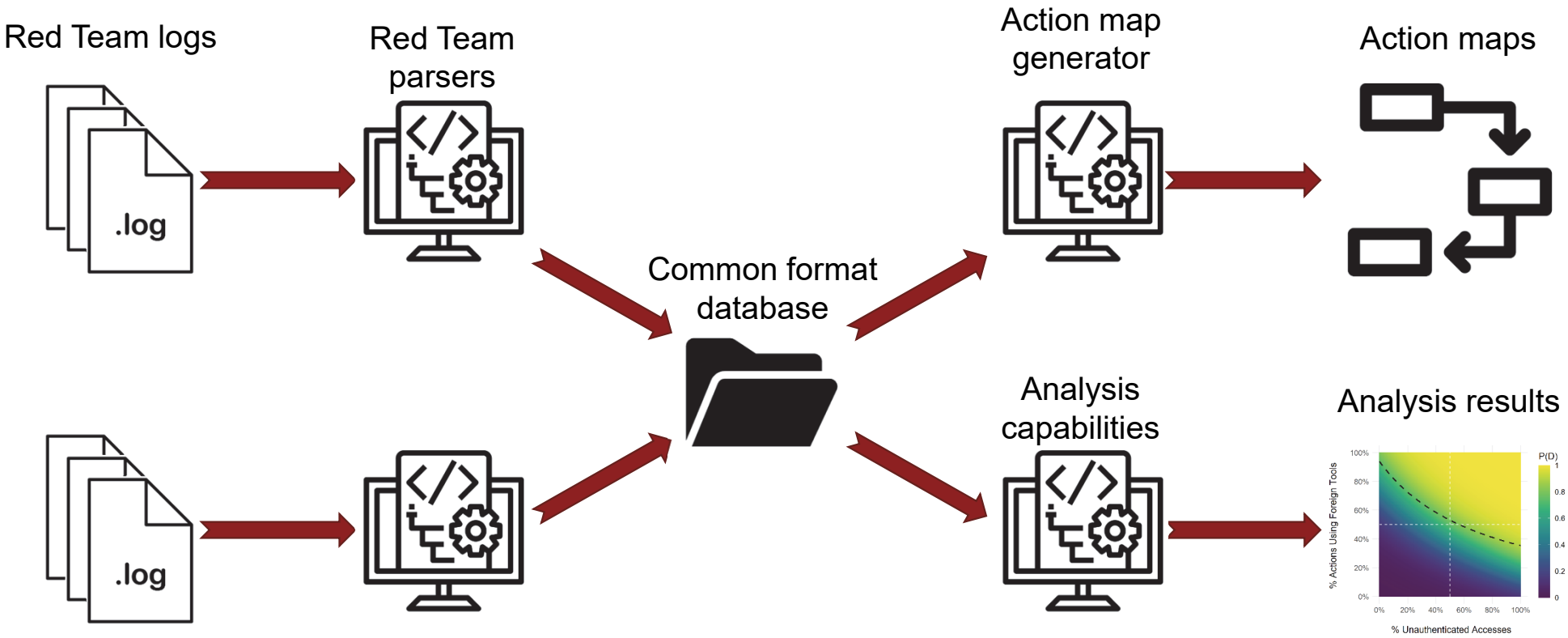
Problem Statement: Collecting the data required for increasingly detailed analyses is intractable using manual data collection methods

Goal: Develop automated and integrated Red Team data collection techniques and analysis methods

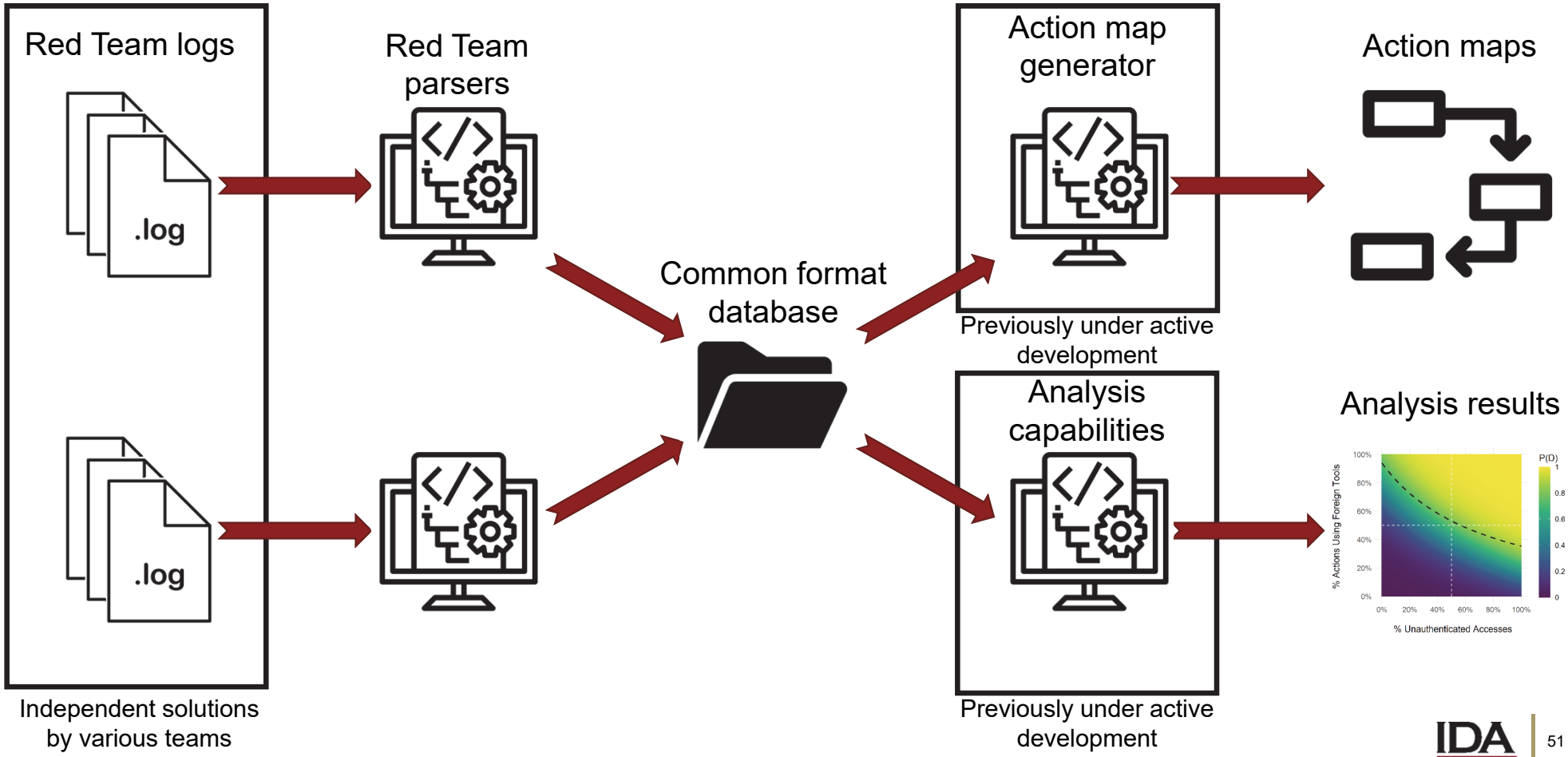
Automated data collection should:

- Describe all Red Team activities
  - Successful and failed
  - Timing information
- Support action map creation
- Be system- and attack platform-agnostic
- Reduce team data collection workload
- Enable advanced analysis techniques

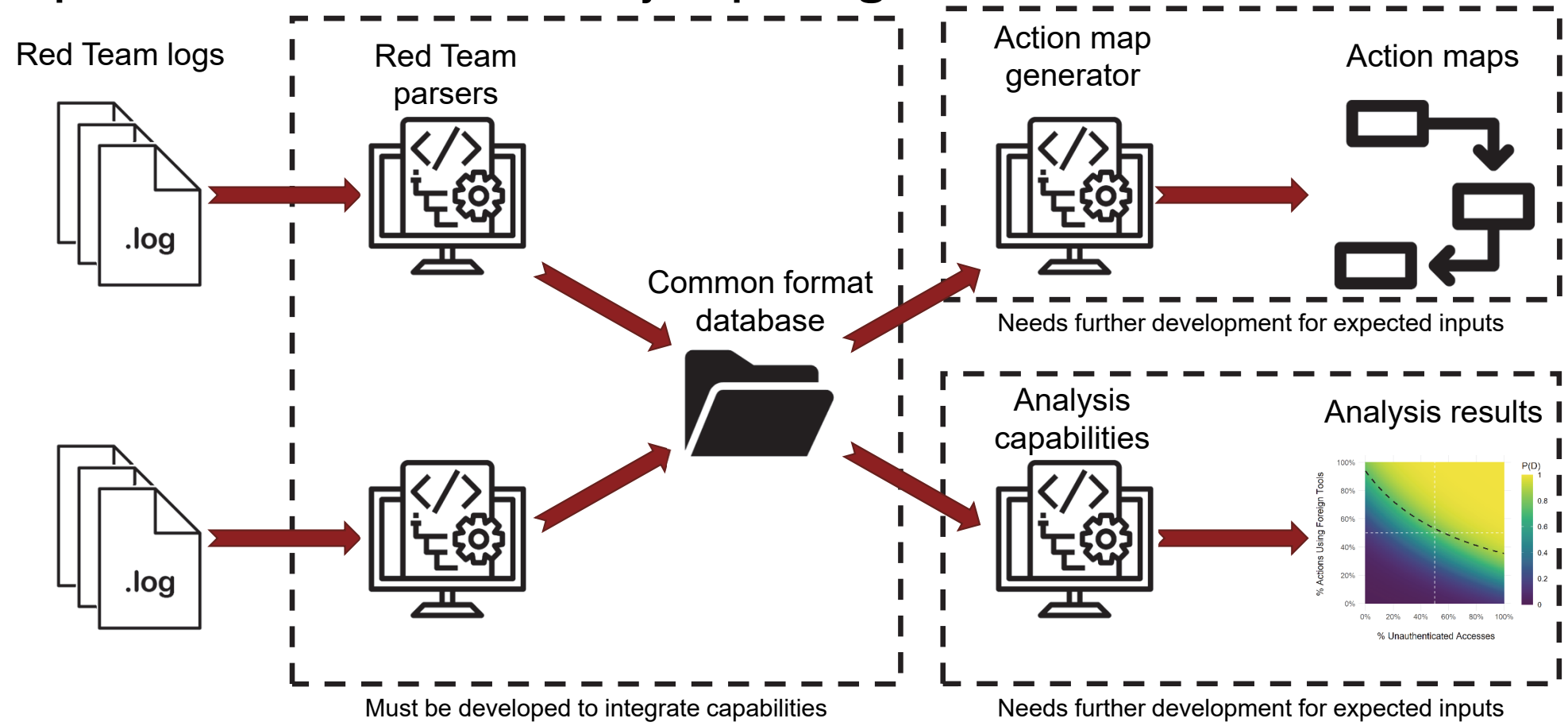
Proposed method: Finalize and integrate previously developed and new capabilities into a flexible analysis package



Proposed method: Finalize and integrate previously developed and new capabilities into a flexible analysis package



Proposed method: Finalize and integrate previously developed and new capabilities into a flexible analysis package

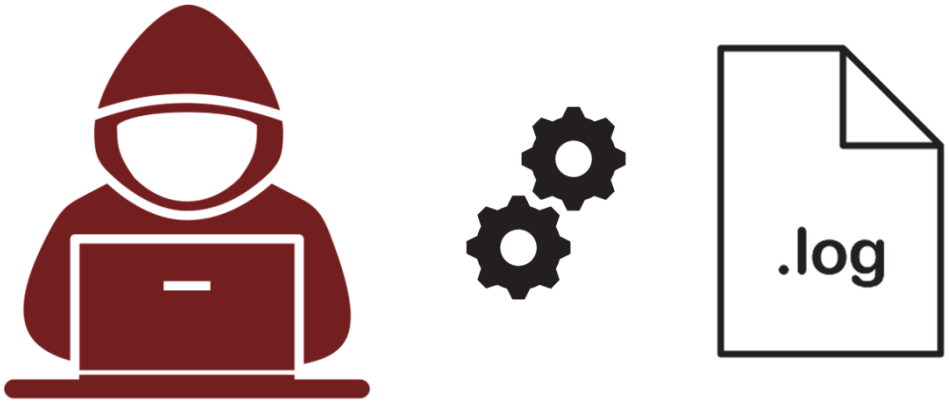


Outcomes: Reduced Red Team data collection workload, more complete data, and new analysis methods

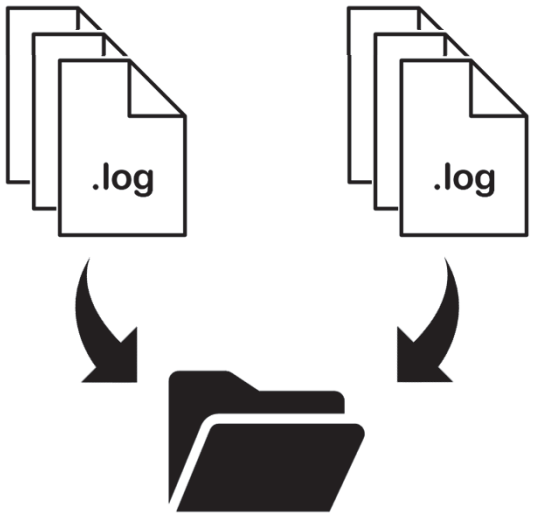
Previous DOT&E and Red Team efforts have supported these requirements:

- Automated Red Team log collection
- Automated action map creation
- Machine learning categorization of Red Team actions

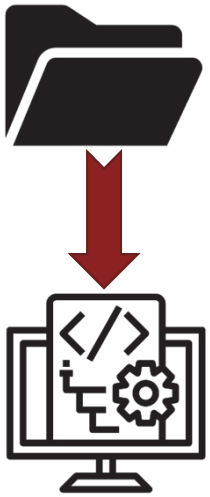
Capability will allow Red Teams to focus on Red Team responsibilities



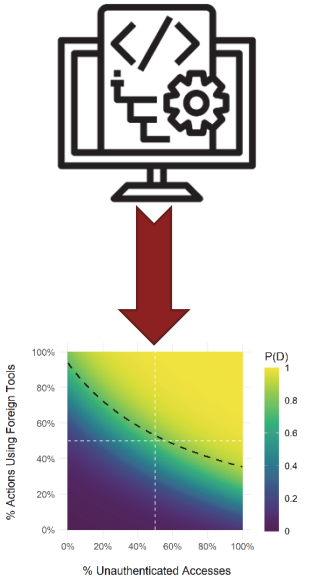
Next steps: Collaborate with the DOT&E CAP Community to develop solutions and increase our analysis fidelity



Began receiving Red Team data (2021-2022)



Discussed automation efforts (Dec. 2021)



CONOPS development (Jan. 2022)

CAP – Cyber Assessment Program; CONOPS – Concept of Operations

We can develop and implement these automation strategies to provide increasingly tailored recommendations to the Department of Defense

Image reference

https://attackevals.mitre-engenuity.org/APT29/

Clock by Astatine Lab from the Noun Project
Domain by Gregor Cresnar from the Noun Project
Networking by Alex Setyawan from the Noun Project
Person by Guilherme Furtado from the Noun Project
Graph by ICONCRAFT from the Noun Project
Admin by Gregor Cresnar from the Noun Project
Server by Tezar Tantular from the Noun Project
PC by Vectors Point from the Noun Project
Windows by buheicon from the Noun Project
Files by Icon Island from the Noun Project
Success by Caesar Rizky Kurniawan from the Noun Project
Team by Gregor Cresnar from the Noun Project
Warning by Adrien Coquet from the Noun Project
Ambulance by Vectors Market from the Noun Project
Find file by Supalerk Laipawat from the Noun Project
Click by Aneeque Ahmed from the Noun Project
Tactic by Iconbox from NounProject.com
Definition by Umer Younas from NounProject.com
Data by Joey Chen from NounProject.com
Conversation by Eucalyp from NounProject.com
Script by Phonlaphat Thongsriphong from NounProject.com
Analysis by Ninejipjip from NounProject.com
Process by Andrejs Kirma from NounProject.com
Log by Alfarizi from NounProject.com
Hacker by karina from NounProject.com

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
01-01-2022	**Draft** Final	**START DATE**	**END DATE** Jan 2022

4. TITLE AND SUBTITLE
Cyber Assessment Program Action Map Introduction

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
HQ0034-19-D-0001		
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**
BD-9-2377	2377	

6. AUTHOR(S)
Schlup, Jason, R.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Institute for Defense Analyses
730 East Glebe Road
Alexandria, Virginia 22305

8. PERFORMING ORGANIZATION REPORT NUMBER
D-32938-NS
H 2022-000007

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'S REPORT NUMBER
Director, Operational Test and Evaluation 1700 Defense Pentagon Room 1D548 Washington, DC 20301-1700	DOT&E	

12. DISTRIBUTION/AVAILABILITY STATEMENT
Public release approved. Distribution is unlimited.

13. SUPPLEMENTARY NOTES
Project Leader: Dodson, Walter R.

14. ABSTRACT
Analyzing data from DOD Cyber Red Teams is crucial to the DOT&E's Cyber Assessment Program (CAP) operational Mission Assurance and cyber operations assessments, which help assess and improve the Department of Defense's ability to defend warfighting capabilities and missions. As part of the program, Cyber Red Teams deliver a data product, called an action map, prior to and during an assessment. Over the past five years, IDA has helped DOT&E define standards for the expected action map content and form. We begin this training briefing by defining action maps and the required data elements each action map should include. Then, we use an example open source cyber attack description to show how Red Teams typically create an action map, and highlight some challenges associated with action map creation. Next, we introduce how IDA analyzes action maps, including how the action map data helps inform DOT&E reports. Finally, we focus on future efforts to improve the action map creation and analysis process, buy using automated data collection capabilities and analysis techniques. Automating the time-consuming and error-prone aspects of using action maps will improve available analysis techniques and the reproducibility of our research.

15. SUBJECT TERMS
Cyber Security; Cybersecurity Assessment Program (CAP); Cyber Assessment; Reproducible Research

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	SAR	65

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER
Walter R. Dodson	703-845-2424