INSTITUTE FOR DEFENSE ANALYSES

Red Team Data Collection and Analysis for the Cyber Assessment Program

Walter R. Dodson, III, Project Leader

Jason R. Schlup
Shawn C. Whetstone

July 2022

IDA Document NS D-33075

Log: H 2022-000267

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 V. Bram Lillard and consisted of Wendy-Angela S. Agata-Moss, 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, III, Project Leader
wdodson@ida.org • (703) 845-2424

V. Bram Lillard, Director, Operational Evaluation Division
vlillard@ida.org • (703) 845-2230

Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Document NS D-33075

Red Team Data Collection and Analysis for the Cyber Assessment Program

Walter R. Dodson, III, Project Leader

Jason R. Schlup
Shawn C. Whetstone

Executive Summary

The Director of Operational Test and Evaluation (DOT&E) performs cybersecurity and mission assurance assessments of Combatant Command and Service networks as part of DOT&E's Cyber Assessment Program (CAP). Analyses of data from these assessments help show how the cybersecurity posture changes across the Department of Defense from year to year. DOT&E has specified the data that CAP participants should collect during assessment events, including an action map that describes Cyber Red Team activities during the assessment. This briefing introduces action maps and summarizes analytic techniques IDA uses to support DOT&E's CAP data analysis.

In the first section, we define an action map and explain its requirements. Action map requirements from DOT&E's authoritative guidance for CAP assessments, the CAP Handbook, dictate how frequently Cyber Red Teams should create action maps and the data elements that Red Teams should capture in action maps. These 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. We emphasize the use of MITRE's ATT&CK knowledge base, which describes adversarial cyber techniques, to describe Red Team activities during CAP assessments. This approach is particularly noteworthy because this categorization will increase analysis fidelity, help analysts communicate results more clearly, and make it easier to integrate CAP with other efforts across the Department of Defense.

Next, we build on the action map requirements by creating an example action map based on a sample attack from MITRE's ATT&CK Evaluation program. The example uses a notional attack from the advanced persistent threat group APT29. We generate an action map for this notional attack using the ATT&CK knowledge base to comprehensively define Red Team activities in a manner that fulfills data requirements from the CAP Handbook. The action map provides a technical description of Red Team activity at each stage of the notional attack, such as the techniques used to capture user credentials and evade network defenses.

Then, we describe how IDA uses an action map to analyze the Department of Defense's cybersecurity posture. This analysis involves creating an attack thread, a concept

that links Red Team activities in a chain of actions from initial network ingress to either causing a cyber effect or being countered by network defenders. Our creation of the attack thread relies heavily on the categorization of Red Team activities according to the ATT&CK knowledge base and other factors, such as the types of adversarial tools used. We then statistically analyze attack threads to identify 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 data of this fidelity will be nontrivial. Additionally, new techniques and models are needed to analyze this quantity of data. We conclude that what is required is an advancement in data collection and analysis capabilities. DOT&E has explored and developed many of the required capabilities, such as automating the collection of Red Team activity, and we recommend they continue this development. Finally, DOT&E should also pursue the development of integration techniques to link the improved data collection with automatic action map generation and enhanced analysis capabilities.

Contents

Introduction 1
Action Map Creation 2
Action Map Analysis 11
Improved Data Collection 18

IDA

Red Team Data Collection and Analysis for the Cyber Assessment Program

Walter R. Dodson, III, Project Leader

Jason R. Schlup

Shawn C. Whetstone

CyberDT XSWG-14: July 13, 2022

Institute for Defense Analyses

730 East Glebe Road ●Alexandria, Virginia 22305

Red Team data inform analyses of cyber defensive performance across the Department of Defense

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

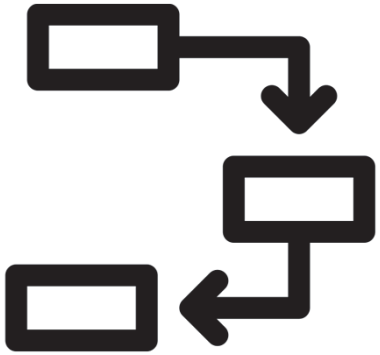
Varying missions and objectives

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 are useful for assessment outbriefs, Combatant Command reports, and Department-wide trend analyses

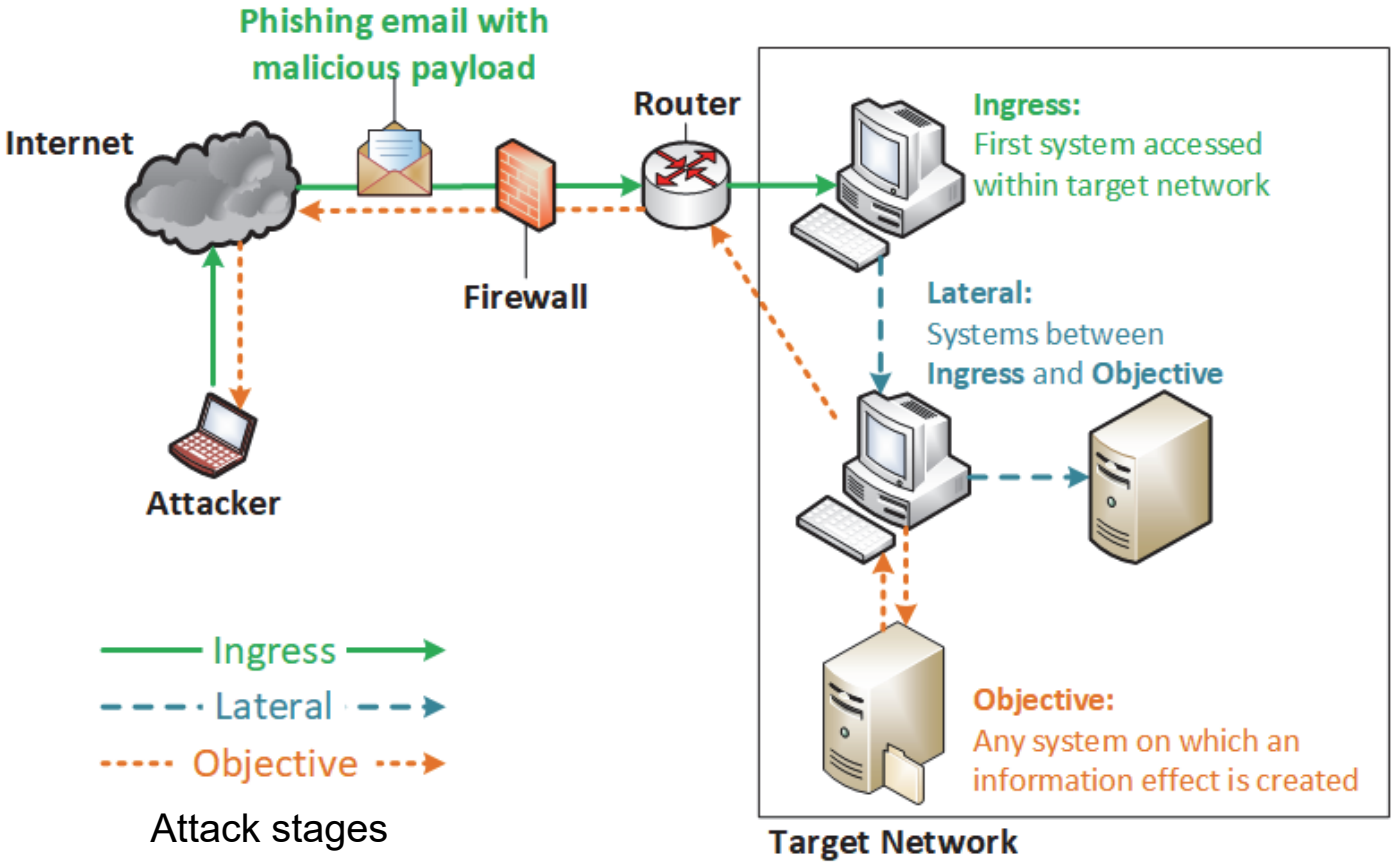
Action map defined as (see CAP Handbook[1]):

> "…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."

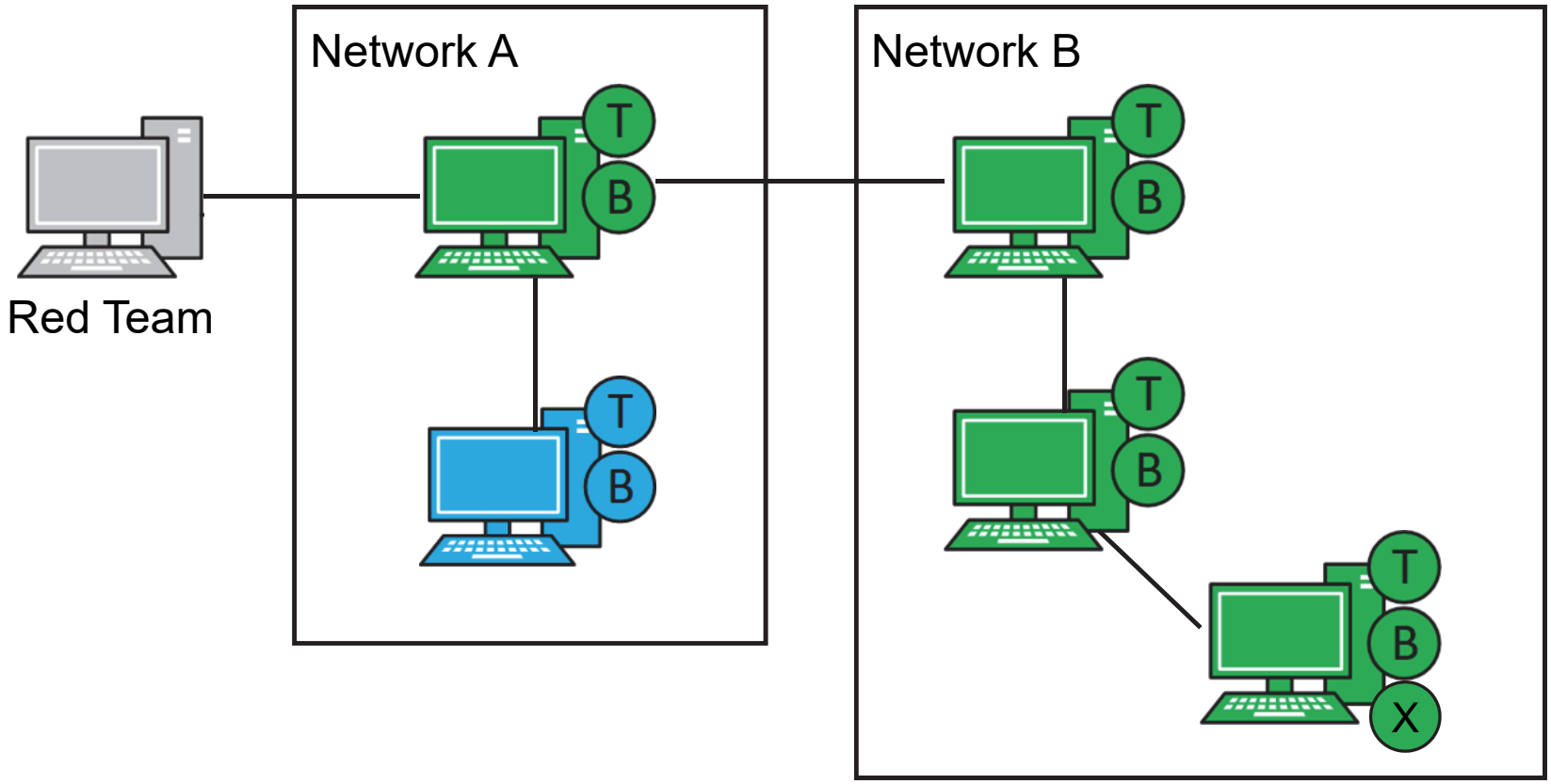
[1] DOT&E, "Cyber Assessment Program Handbook Version 4.1," May 2021.

CAP – Cyber Assessment Program

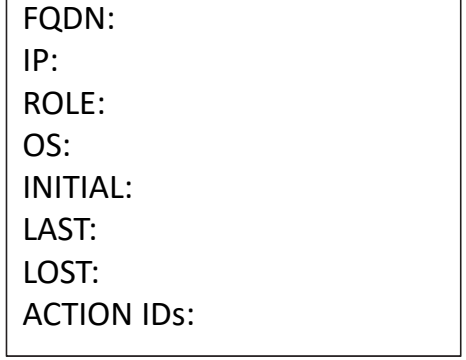
An action map provides a graphical depiction and the technical detail of Red Team activities and their attack thread



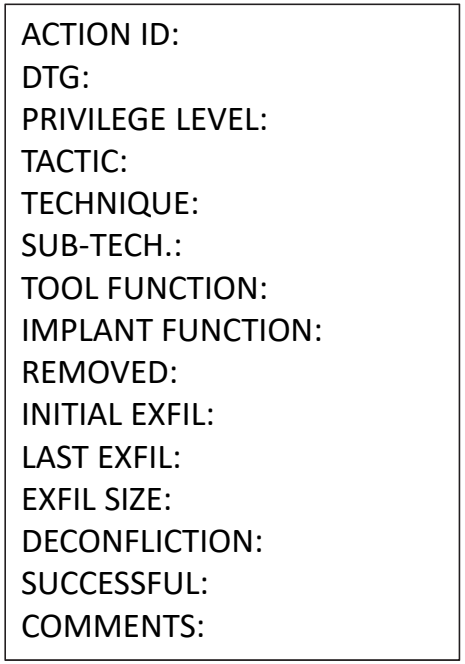
Uniform symbols and colors help visualize the current Red Team cyber campaign



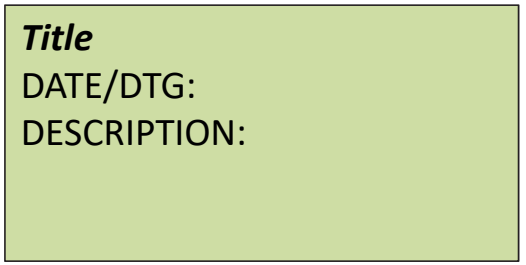
Beyond symbols and colors, an action map consists of three main data elements describing Red Team actions



System Description



Action Description

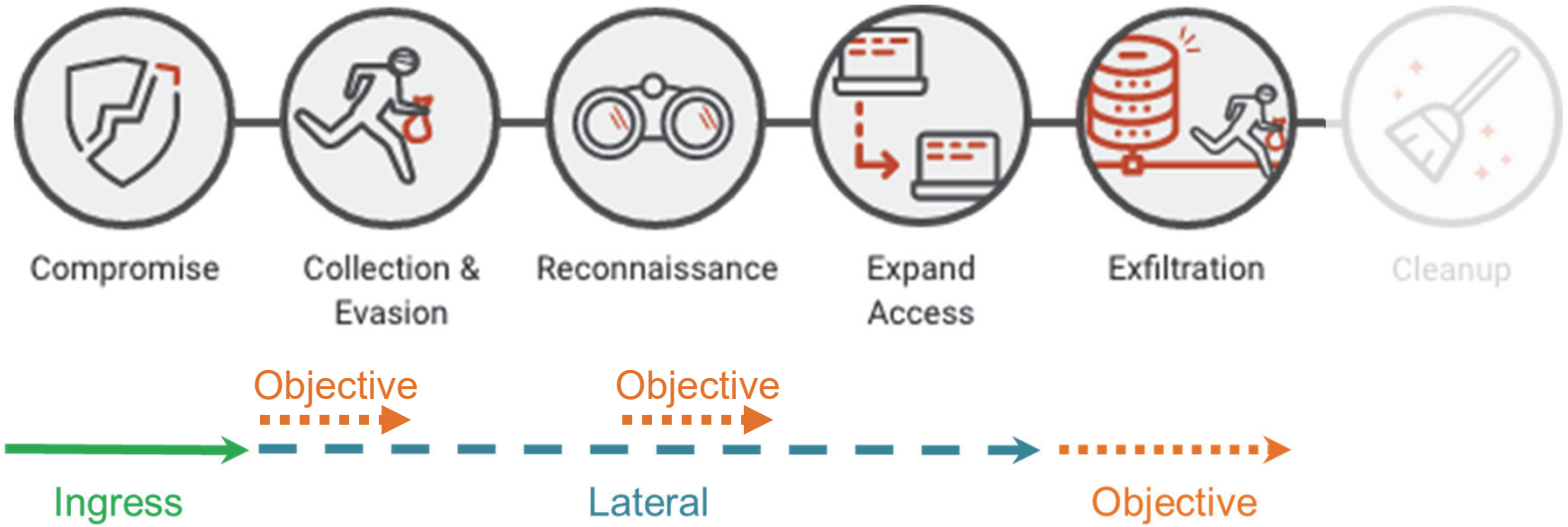


Note Field

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

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

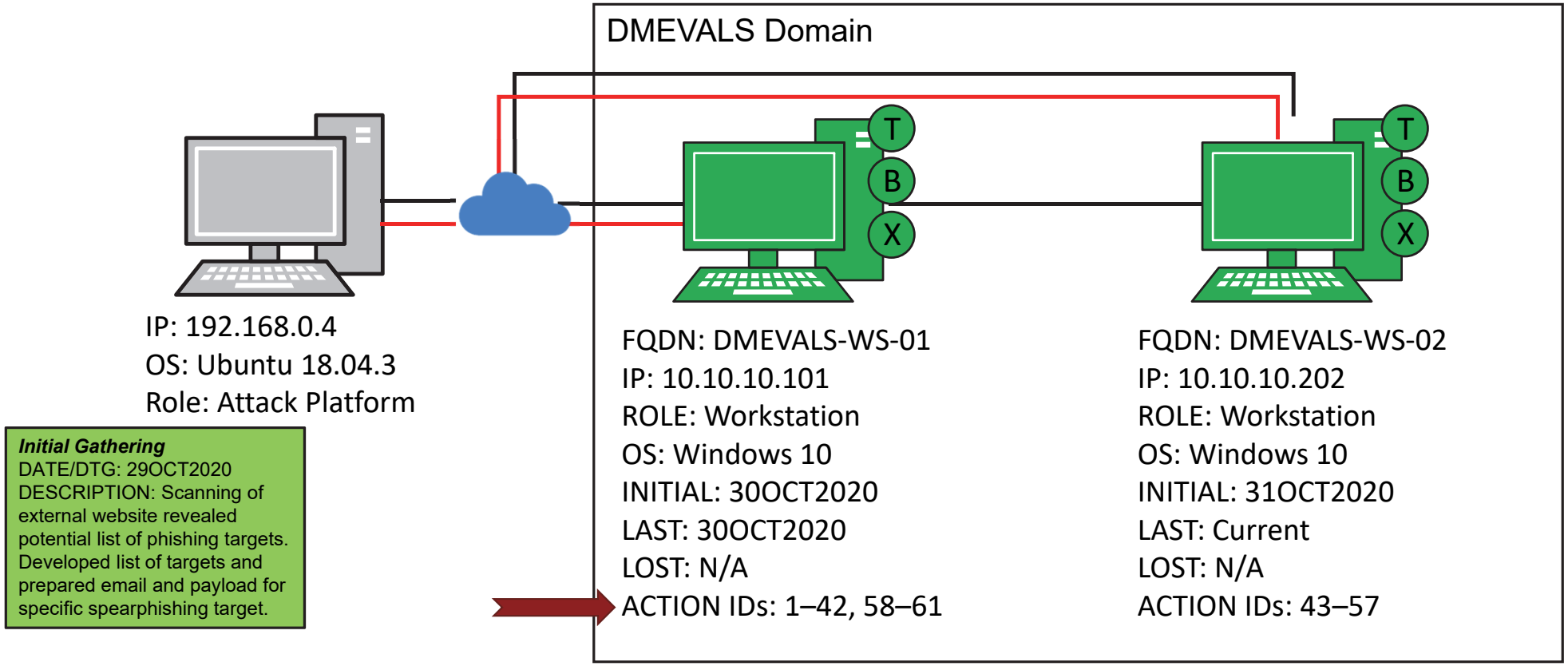


This scenario begins with a **legitimate user clicking on a malicious payload** delivered via a "spray and pray" broad spearphishing. The attacker immediately kicks off a **"smash-and-grab," rapid espionage mission, gathering and exfiltrating data**. After initial exfiltration, the attacker realizes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

The final action map contains system information and technical 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.

All actions can be described using the action description data elements

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

Initial Gathering	ACTION ID: 1	ACTION ID: 2	ACTION ID: 3	ACTION ID: 4	ACTION ID: 5
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.	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	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	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	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	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 these 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

Analysts convert the action map picture into a spreadsheet that links actions to 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

ATT&CK Evaluation data used on this slide.

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

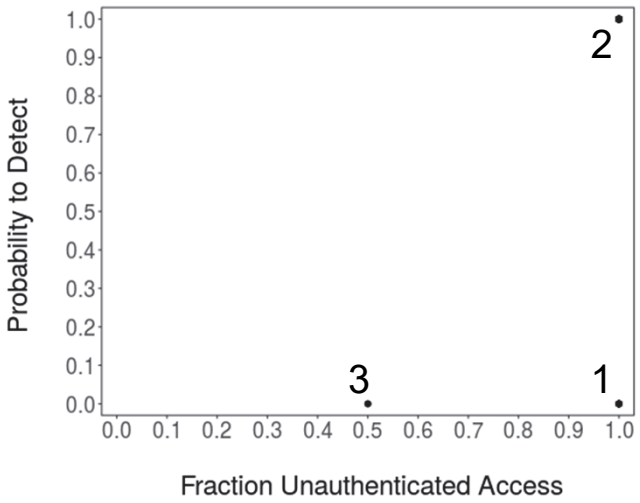
- APT29 Evaluation has three cyber effects: three exfiltration (confidentiality) activities
- Method: Find “attack” on an objective node, look at antecedent, then look at that action’s antecedent…
- Attack thread #1: 10 > 9 > {8,7} > 6 > 5 > 4 > 3 > 2 > 1
- The first attack thread has ten actions: five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

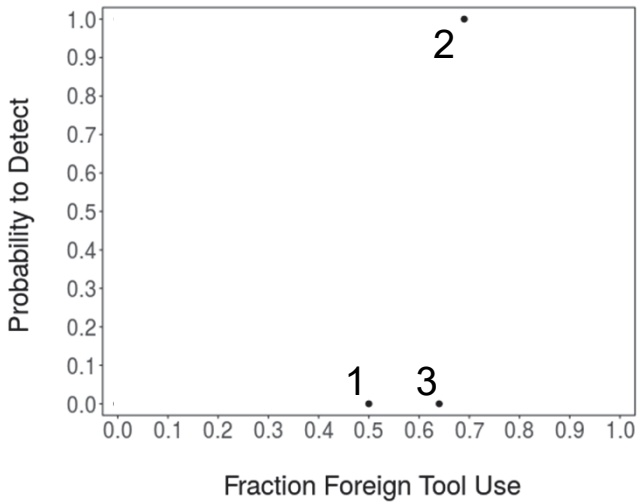
APT – Advanced Persistent Threat

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 the 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

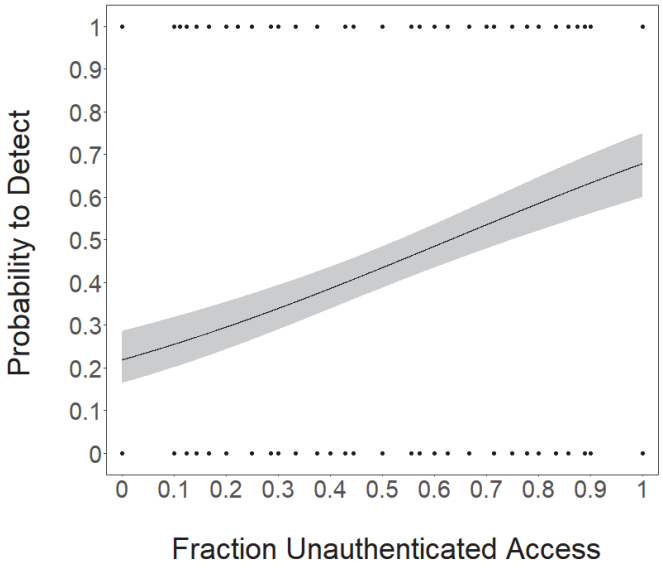


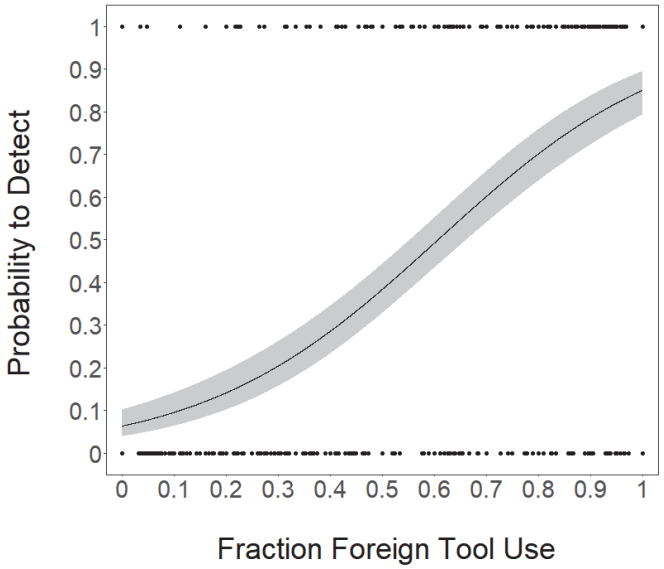


ATT&CK Evaluation data used on this slide.

Compiling data from this evaluation and other assessments generates a dataset 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
	.	.	.
	.	.	.
	.	.	.



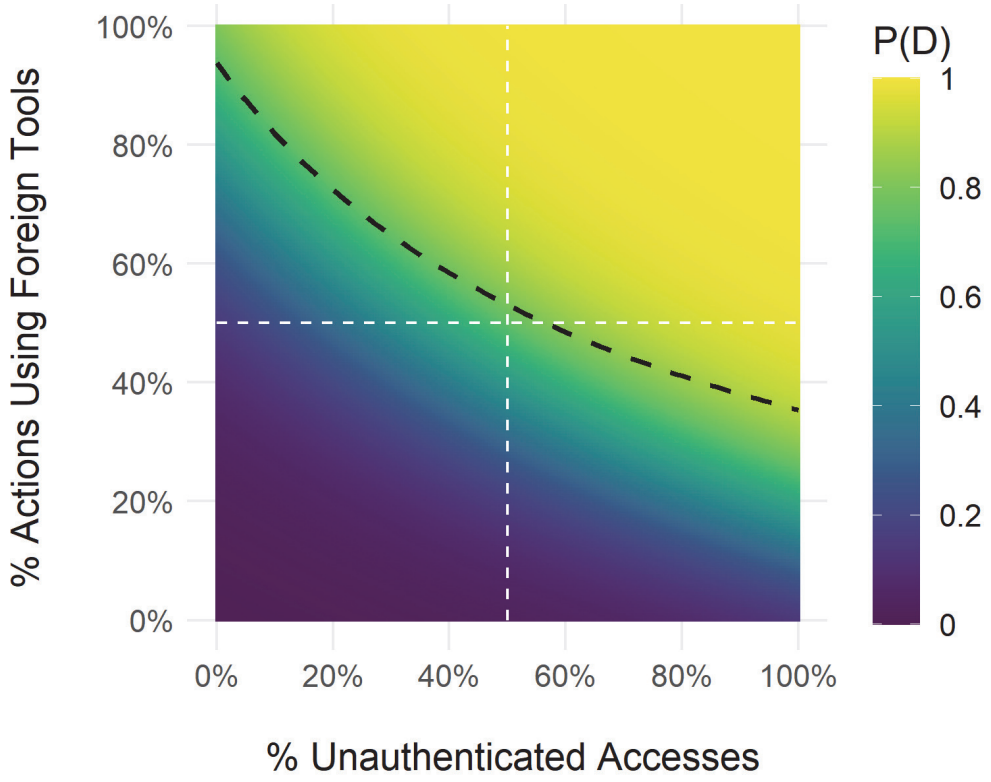


Notional data used on this slide.

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

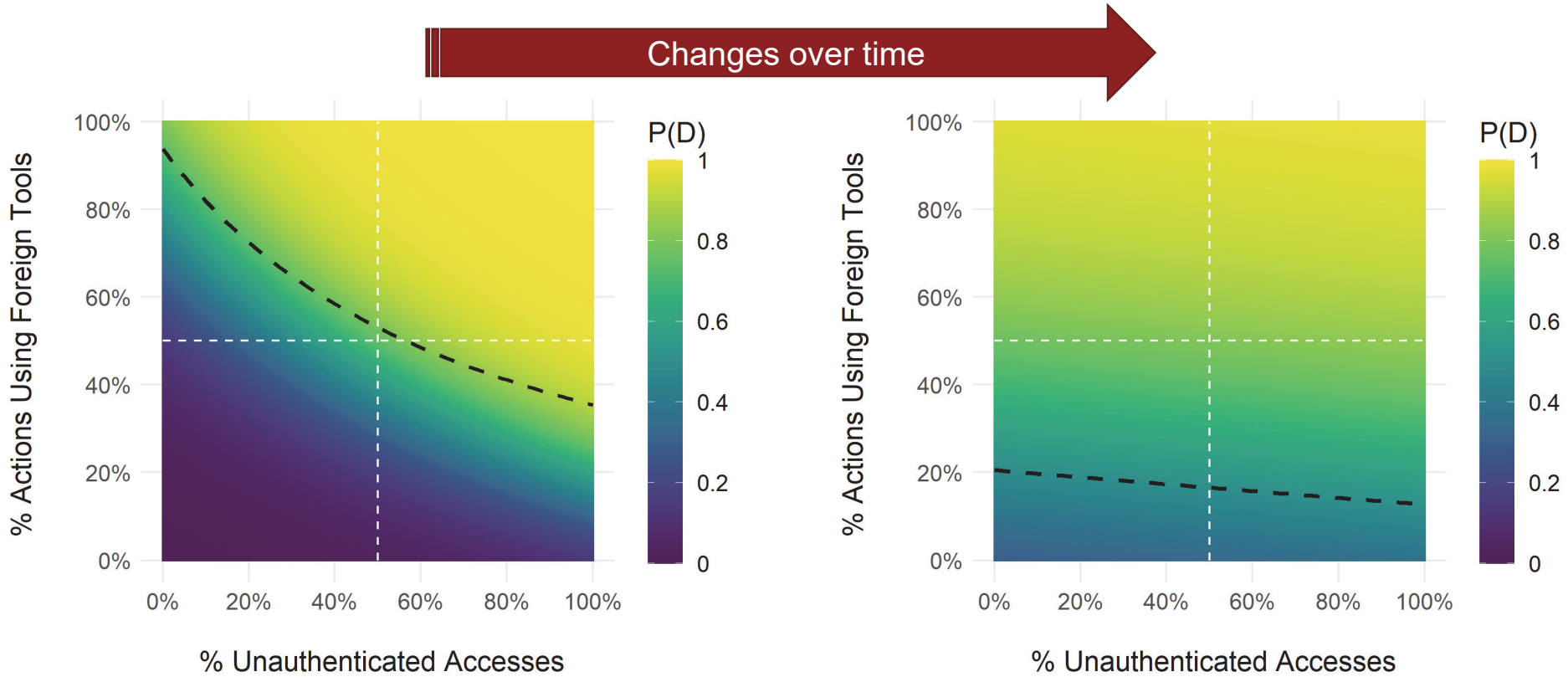
Attack #	Fraction Unauthent. Access	Fraction Foreign Tool Use	Detected?
1	1.00	0.50	0
2	1.00	0.69	1
3	0.50	0.64	0
4	0.00	0.82	0
5	0.44	0.08	0
6	0.63	0.14	0
7	0.00	0.29	0
8	1.00	0.33	1
9	0.00	0.40	0
10	0.80	0.62	1
	. . .	. . .	. . .

P(D) – Probability to Detect



Notional data used on this slide.

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

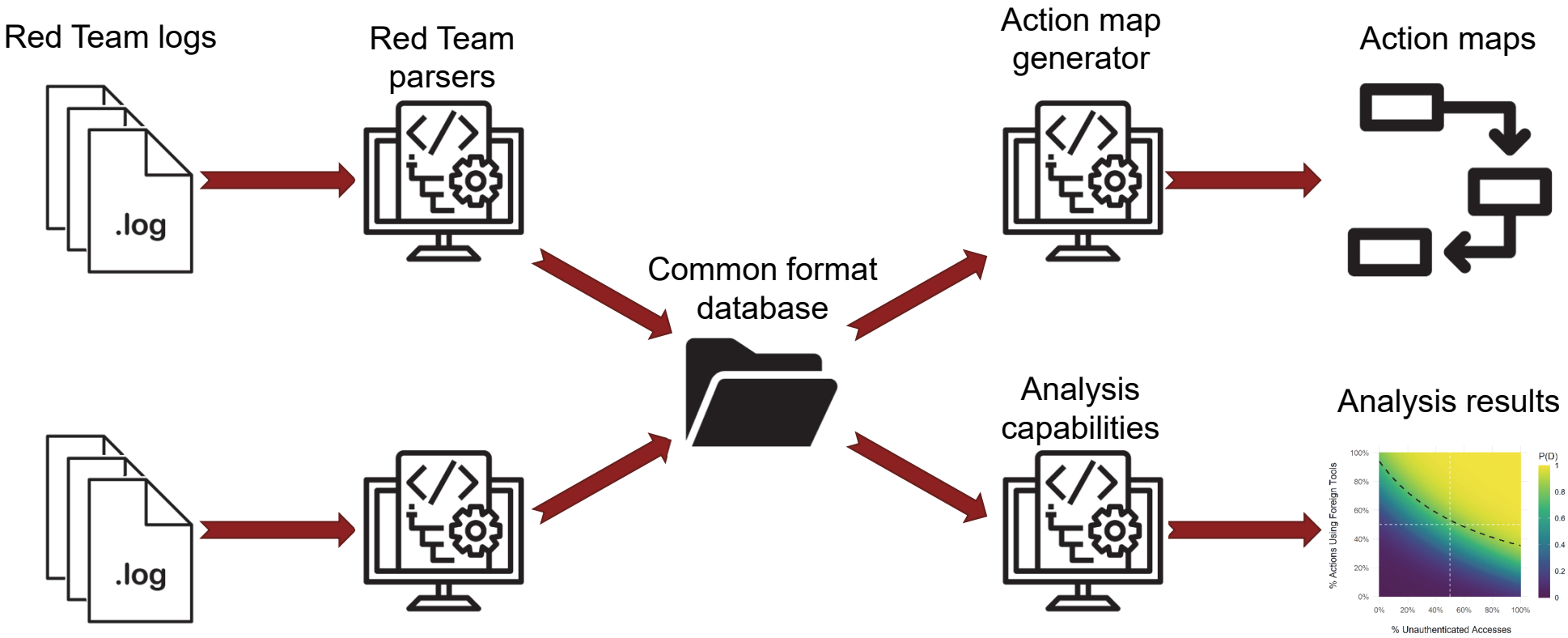


P(D) – Probability to Detect

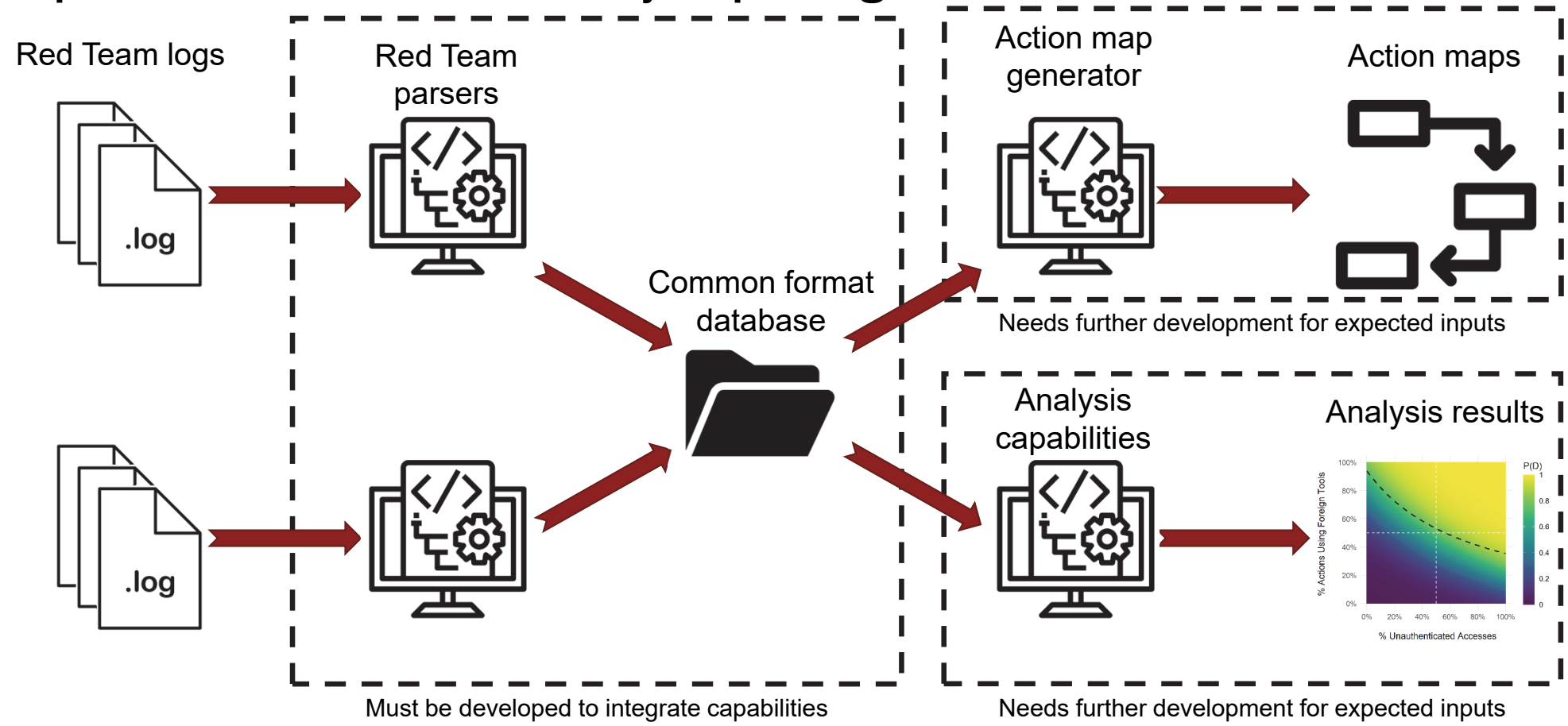
Notional data used on this slide.

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

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



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

Image references

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	
01-07-2022	Final	START DATE	END DATE July 2022

4. TITLE AND SUBTITLE
Red Team Data Collection and Analysis for the Cyber Assessment Program

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)	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 730 East Glebe Road Alexandria, Virginia 22305	NS D-33075 H 2022-000267

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 Washington, DC 20301	DOT&E	

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; 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. This briefing begins 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 action map analysis techniques, 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, by 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
Cybersecurity Assessment Program (CAP); Cyber Security; Cyber Assessment; Reproducible Research

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	c. THIS PAGE		
Unclassified	Unclassified	Unclassified	SAR	33

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