DATAWorks 2025: Developing a Social Engineering/Physical Ingress Analysis Framework and Data Collection Standards for CAT Assessments

Saringi Agata-Moss

April 24, 2025

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

IDA has developed two products to collect and analyze data from Close Access Team (CAT) missions.

Social Spoofing Security Analysis Reference (S_3AR) Framework

- Categorizes social engineering and physical ingress techniques.
- Supports analyses of physical ingress assessments in a manner similar to the support the MITRE ATT&CK framework provides for on-network cyber activity.

CAT Data Standards

- Leverage S_3AR and a survey of CAT members about their mission operations.
- Incorporate information on mission operations received from 5 CATs.
- Include data collection sheets for CAT mission planning and preparation, daily actions, and systems accessed.

Presentation Roadmap

Introduction to Cyber Ingress and MITRE ATT&CK for On-Network Cyber Activity

- Overview of CAT's use to understand cyber ingress
- Overview of framework as used in APT29 cyberattack
- Use of data collection standards and framework to generate meaningful trends

S_3AR – A Framework for Understanding Physical Ingress and Social Engineering Activity

- Review of academic literature
- Survey of CAT members
- Introduction to IDA's framework: Social Spoofing Security Analysis Reference (S_3AR)

Development of CAT Data Standards

- Planning and preparation
- Daily actions
- Systems accessed
- Possible trends garnered from improved data

Presentation Roadmap

Introduction to Cyber Ingress and MITRE ATT&CK for On-Network Cyber Activity

- Overview of CAT's use to understand cyber ingress
- Overview of framework as used in APT29 cyberattack
- Use of data collection standards and framework to generate meaningful trends

S_3AR – A Framework for Understanding Physical Ingress and Social Engineering Activity

- Review of academic literature
- Survey of CAT members
- Introduction to IDA's framework: Social Spoofing Security Analysis Reference (S_3AR)

Development of CAT Data Standards

- Planning and preparation
- Daily actions
- Systems accessed
- Possible trends garnered from improved data

Close Access Team (CAT) assessments inform the red team's initial posture in a cyber exercise and highlight physical access vulnerabilities that could enable cyber compromise.

Cyber adversaries leverage both on-network and physical means to access systems – Close Access Teams (CATs) are an example of a physically enabled vector.

Adversary

Ingress: Initial access to target network.

- Phishing email
- **Physically enabled**
- Cross-domain solutions

Lateral: Pivot in target network, escalate privileges, and establish persistence.

Objective: Exfiltrate, manipulate, or deny mission-critical data.

CAT Assessments

Data Sources: OAR reports, outbriefs

Analysis Framework: N/A

On-Network Cyber Red Team Activity

Data Sources: Action maps, SIGACTs, OAR reports, etc.

Analysis Framework: MITRE ATT&CK framework

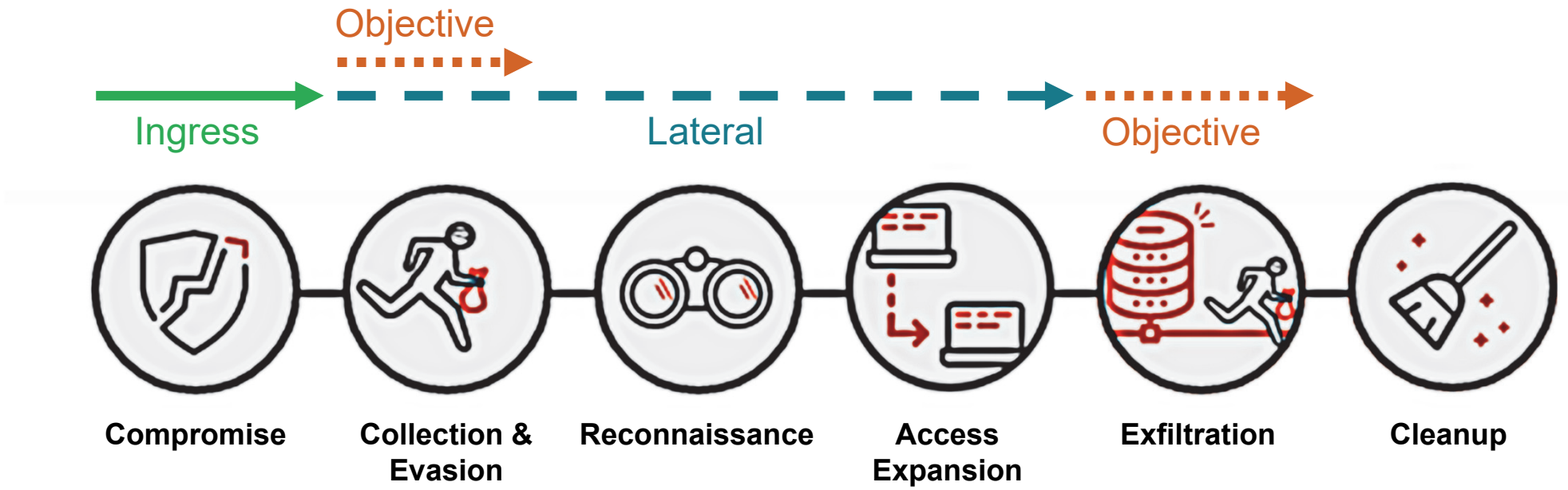
IDA leverages standardized data collection processes and an industry analysis framework standard, MITRE ATT&CK, for analyzing on-network cyber red team activity.

OAR – Observations, Analysis, and Recommendations; SIGACT – Significant Activity Report

IDA uses the MITRE ATT&CK framework to analyze red-team-generated action maps that represent on-network activity during an exercise.

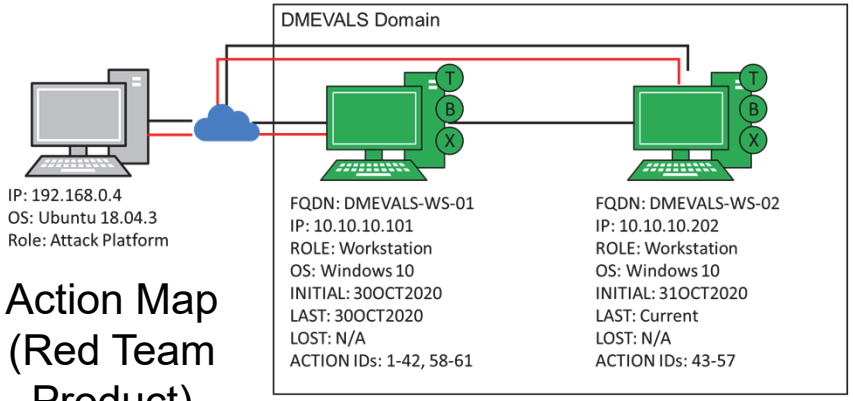
Example – APT29 (aka Cozy Bear)

Description: This scenario begins with a **legitimate user clicking on a malicious payload** delivered via a broad "spray and pray" spear-phishing attack. 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 user 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 attacker's execution of previously established persistence mechanisms.



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

IDA performs standardized analyses of red team products using the MITRE ATT&CK framework to develop attack spreadsheets and subsequent red team attack threads.



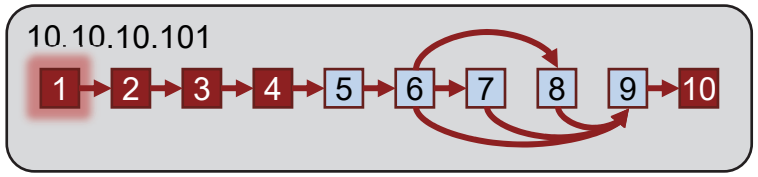
Action Map (Red Team Product)

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

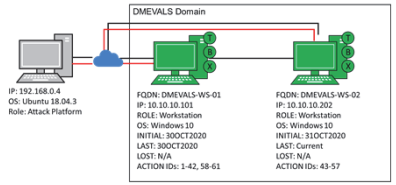
Note: notional data

Attack Thread (IDA Product)



Leveraging data standards and the ATT&CK framework allows IDA to generate key data products we use for cross-program reporting.

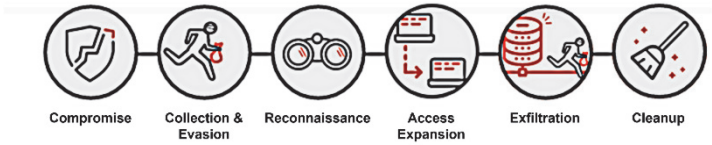
On-Network Data Standards



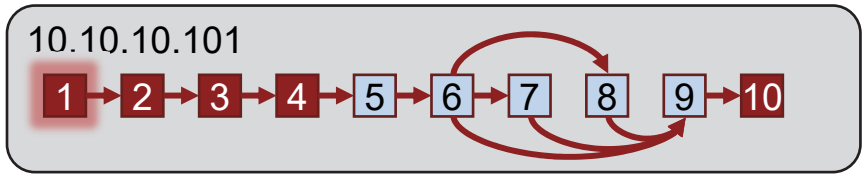
Action Map

Daily Situational Report

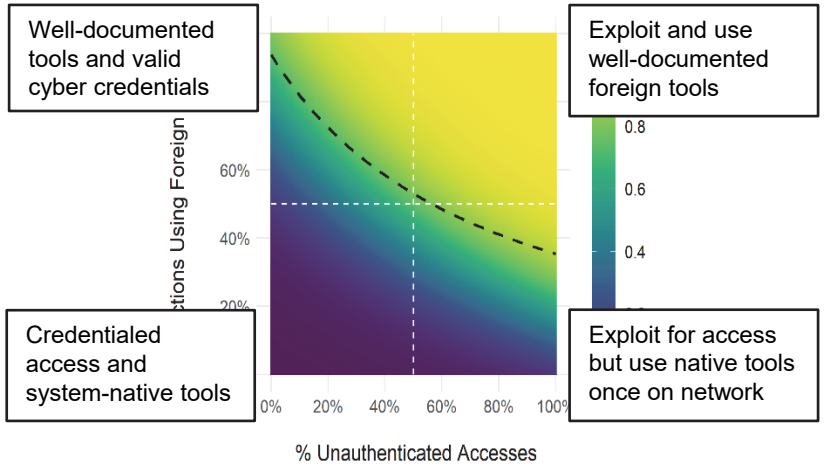
MITRE ATT&CK Framework



Generated Data



Attack Thread

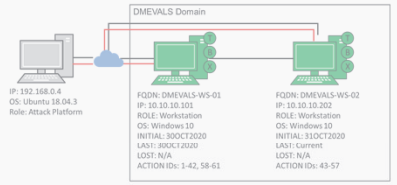


Probability of Detection Heat Map

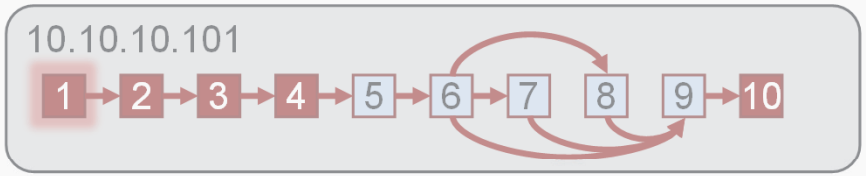
This slide uses notional data.

Leveraging data standards and the ATT&CK framework allows IDA to generate key data products we use for cross-program reporting.

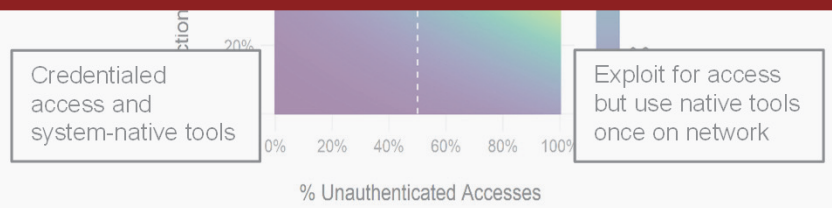
On-Network Data Standards



Generated Data



Set data standards and a TTP analysis framework for CAT operations are necessary for a streamlined, trend-based analysis of mission data.



Probability of Detection Heat Map

This slide uses notional data.

Presentation Roadmap

Introduction to Cyber Ingress and MITRE ATT&CK for On-Network Cyber Activity

- Overview of CAT's use to understand cyber ingress
- Overview of framework as used in APT29 cyberattack
- Use of data collection standards and framework to generate meaningful trends

S_3AR – A Framework for Understanding Physical Ingress and Social Engineering Activity

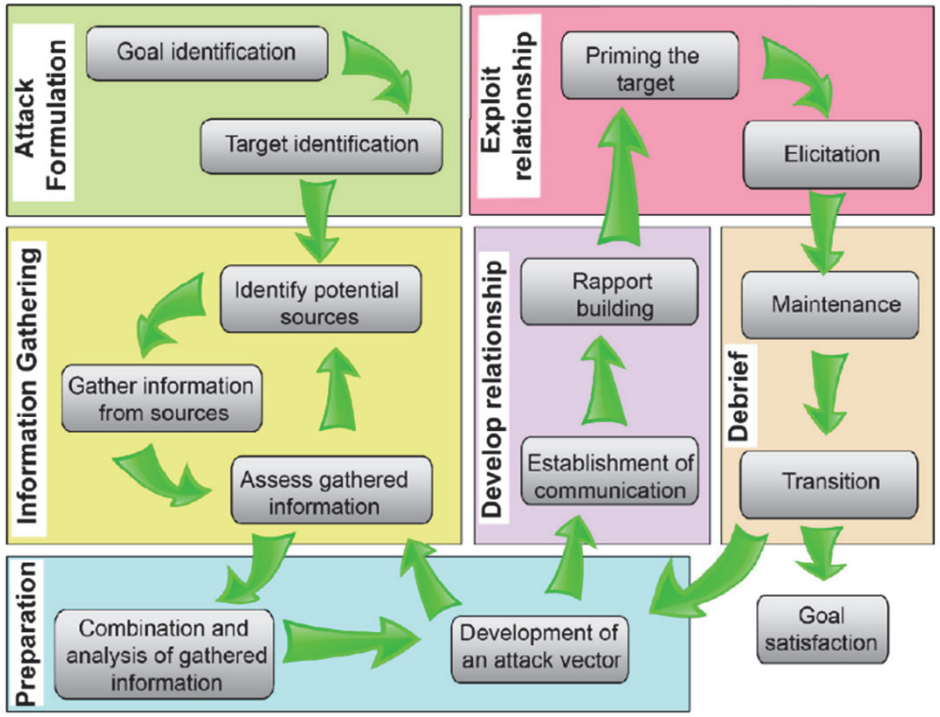
- Review of academic literature
- Survey of CAT members
- Introduction to IDA's framework: Social Spoofing Security Analysis Reference (S_3AR)

Development of CAT Data Standards

- Planning and preparation
- Daily actions
- Systems accessed
- Possible trends garnered from improved data

IDA designed a social engineering and physical ingress analysis framework to encapsulate the tactics, techniques, and procedures of Close Access Teams during their missions.

IDA turned to the academic literature on information processing and behavioral psychology and found a social engineering framework based on multiple social attack scenarios.



Mouton et al. Social Engineering Cycle

- Based on the behavioral psychology sub-area of deception.
- Defines the core steps of the flow of a social engineering attack and is derived from multiple scenarios.
- Does not reflect physical and logical ingress techniques, i.e., the "cyber" piece.
- Does not consider the compressed timeline of a CAT mission.

CAT – Close Access Team

Image from Francois Mouton, Louise Leenen, and H.S. Venter, "Social Engineering Attack Examples, Templates, and Scenarios," *Computers & Security* 59, no. 1 (2016): 186–209, https://doi.org/10.1016/j.cose.2016.03.004.

IDA generated version 1 of S_3AR by expanding the social engineering cycle (Mouton et al.) to encompass research on common non-destructive physical ingress practices and the TTPs used in CAT missions.

Academic Literature
Mouton et al. social engineering cycle

+

CAT Post-Mission Reporting
2014–present

→

Social Spoofing Security Analysis Reference (version 1)
[S_3AR]

Social Spoofing Security Analysis Reference (v1)

Tactics and Techniques — *Nodes*

Ingress

- **Research**
  - Preparation
  - Information Gathering
  - Attack Formulation
- **Ingress**
  - Physical Ingress
  - Electronic Ingress

→

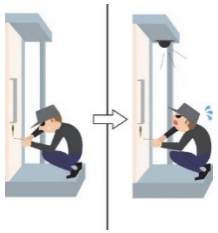
Lateral

- **Developing Rapport and Trust**
  - Develop Relationship
- **Exploiting Trust**
  - Exploit Relationship
  - Debrief

→

Objective

- **Utilizing Gathered Info**
  - Compromise or Attack



CAT – Close Access Team; TTPs – Tactics, Techniques, and Procedures

Francois Mouton, Louise Leenen, and H.S. Venter, "Social Engineering Attack Examples, Templates, and Scenarios," *Computers & Security* 59, no. 1 (2016): 186–209, https://doi.org/10.1016/j.cose.2016.03.004.

All images are from OpenVerse and are open source.

IDA generated version 1 of S_3AR by expanding the social engineering cycle (Mouton et al.) to encompass research on common non-destructive physical ingress practices and the TTPs used in CAT missions

Do the limitations of a CAT assessment (e.g., timeframe) allow for the "relationship building" the Mouton et al. model depicts?

Can we leverage CAT operational knowledge to better fit our model to DoD physical ingress missions (i.e., CATs)?

Academi

Mouton
engine

Spoofing
Analysis
(version 1)

Nodes

Tactics and Techniques

Ingress

Research

- Preparation
- Information Gathering
- Attack Formulation

Ingres

- Physical Ingress
- Electronic Ingress

- Exploit Relationship

Objective

Utilizing Gathered Info

- Compromise or Attack

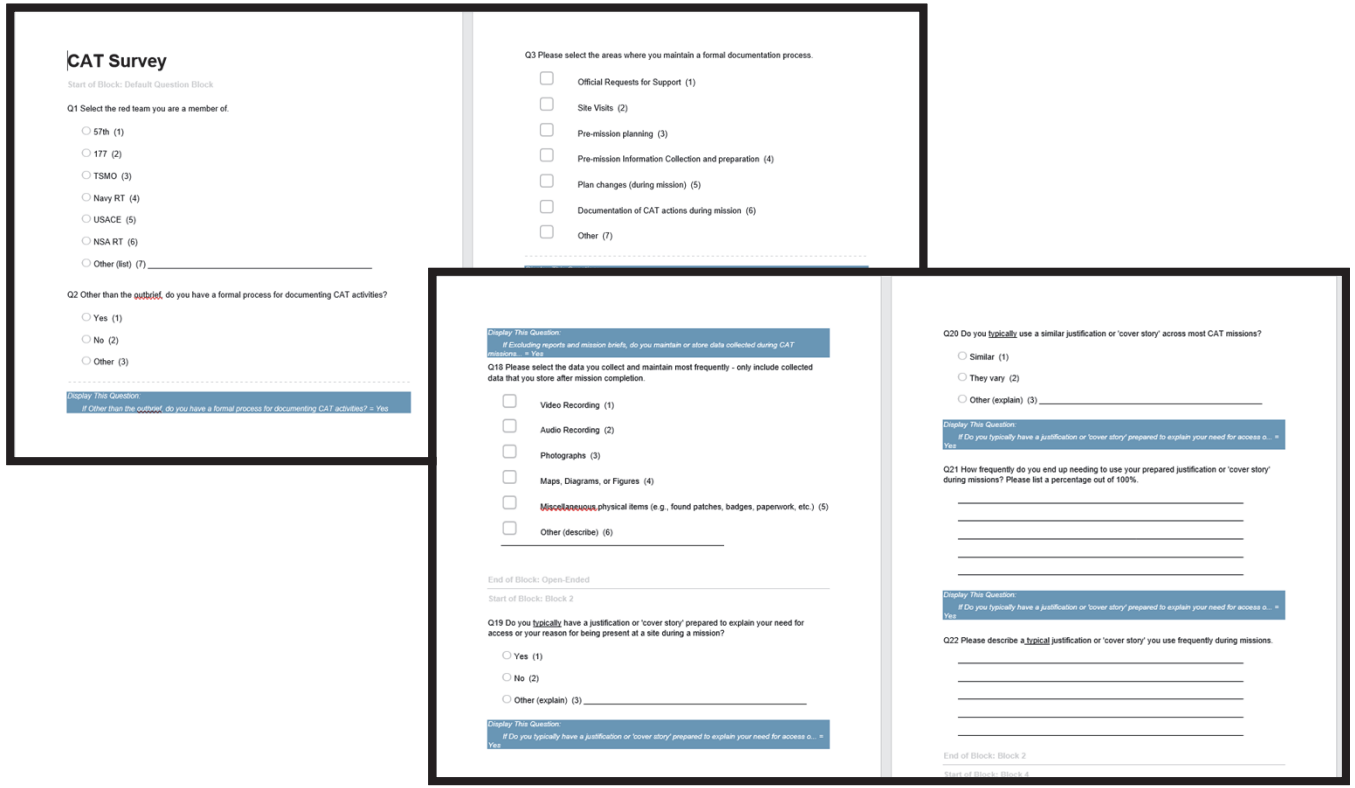
CAT – Close Access Team; TTPs – Tactics, Techniques, and Procedures

Francois Mouton, Louise Leenen, and H.S. Venter, "Social Engineering Attack Examples, Templates, and Scenarios," *Computers & Security* 59, no. 1 (2016): 186–209, https://doi.org/10.1016/j.cose.2016.03.004.

All images are from OpenVerse and are open source.

IDA surveyed five CATs about their mission planning and operations.

- IDA used general language to describe activities before and during a mission to avoid swaying responses.
- Survey had 27 questions total – a mix of multiple choice and open answer.
- Survey was well received by CAT operators and largely aligned with groupings for the TTPs we had already scoped for the pre-mission activity (planning) and objective nodes.
- Survey results substantially informed further development of the lateral node.



Dr. Sarah Shaffer
OED

CAT – Close Access Team; TTPs – Tactics, Techniques, and Procedures

IDA manually reviewed and coded all survey results and grouped like terms and phrases under the appropriate nodes.

Planning and Ingress

Information Gathering

- "Open source research (OSR) to identify specifics about the target…"
- "We typically use Google Maps to locate our targets first."
- "TA/customer meetings to discuss tactics and objectives."

Access Planning

- "We then started to photograph personnel with badges."
- "At the site-survey […] we identify ingress egress points."
- "Conduct physical site recon, identify persons of interest, patterns of life, and security processes."

Breaking and Entering

- "…entering outside of normal visiting hours…"
- "Late night B&E utilizing under the door tools and lock picks."
- "…under door tool…"

Falsified Credentials

- "…scan badges and shoulder surf for pins related to the badge…"
- "RFID skimmer were used in a back pack with a covert camera."

Lateral

Piggybacking

- "Social engineering for access to facility or target locations, piggybacking."
- "…and identifying if personnel are allowing 'piggybacking' into the target."

Impersonation

- "Higher headquarters has directed an assessment, test, survey, etc."
- "We are the Information Technology department and are taking inventory of equipment."

Objective

Implantation

- "Due to the mission objective being the implementation of technical access capability on a computer..."
- "[Implant] Lokeys, Teenseys, and Zap sticker."

Ms. Amy Guaman-Dumencela
OED

Dr. Sarah Shaffer
OED

We are further categorizing the lateral node tactics and techniques using preliminary results from the CAT member survey and the psychological principles of deception.

Academic Literature
Mouton et al. social engineering cycle

+

CAT Post-Mission Reporting
2014–present

+

Insight on CAT activity
CAT member survey

Psychology behind decision-making

→

Social Spoofing Security Analysis Reference (Version 2)
[S_3AR]

Social Spoofing Security Analysis Reference (v2) [Current]

Tactics and Techniques — *Nodes*

Ingress

- **Research**
  - Preparation
  - Information Gathering
  - Attack Formulation
- **Ingress**
  - Physical Ingress
  - Electronic Ingress

→

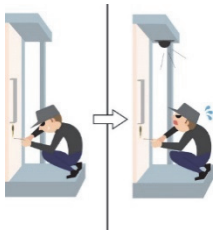
Lateral

- **Leveraging Personal Interactions / Intermediary Access Methods**
  - Opportunistic vs. intentional

→

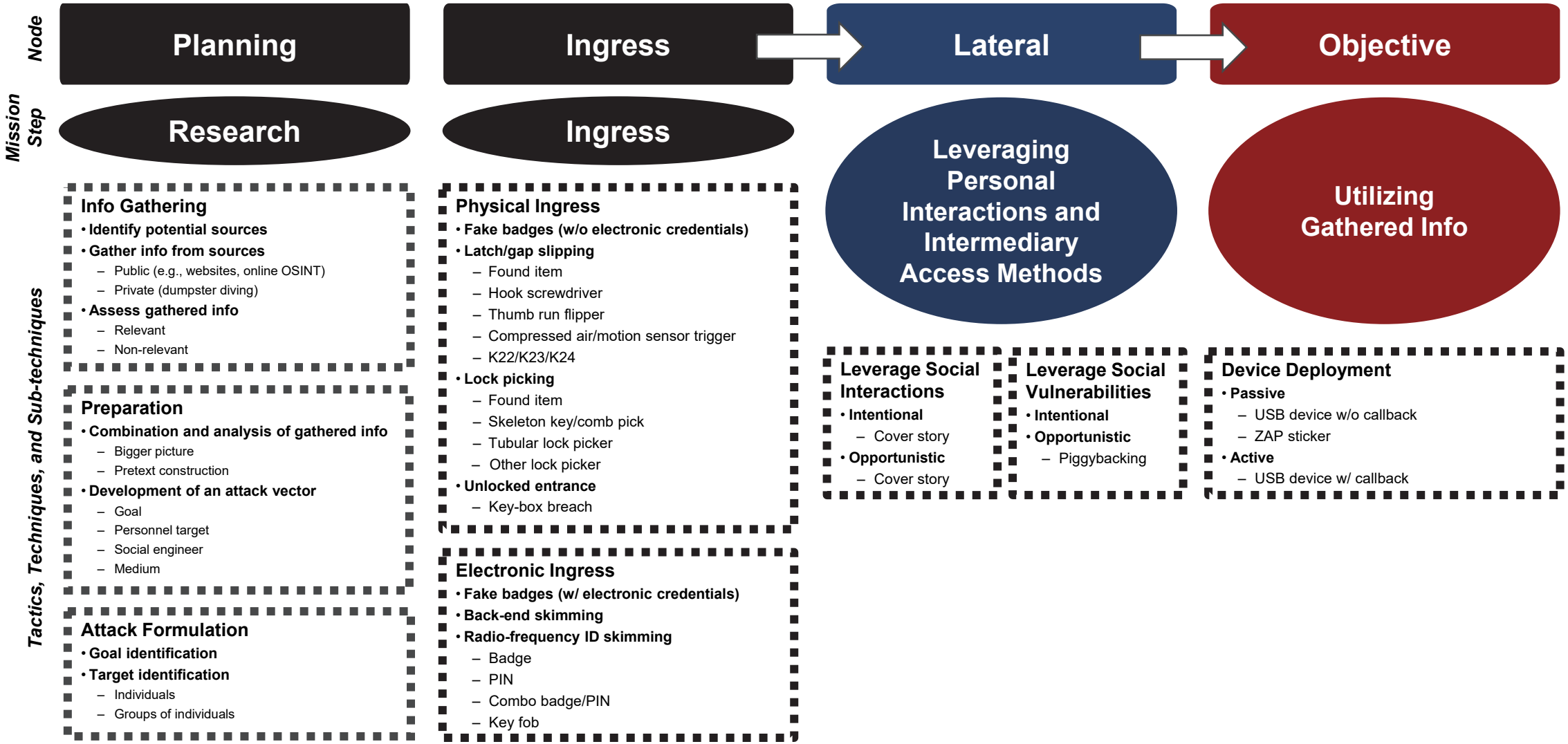
Objective

- **Utilizing Gathered Info**
  - Compromise or Attack



CAT – Close Access Team

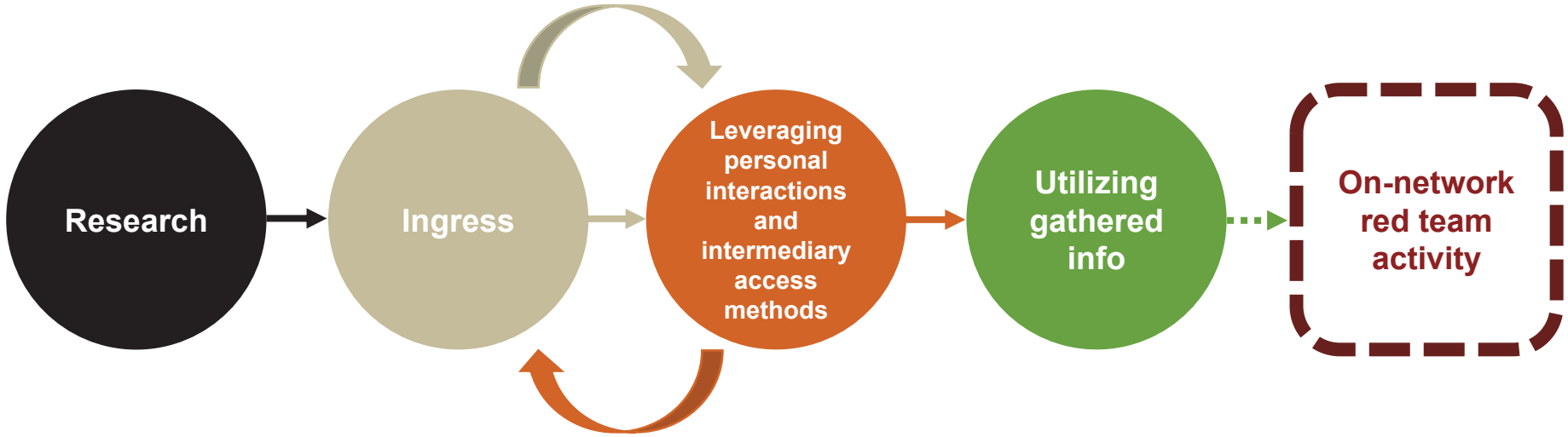
Social Spoofing Security Analysis Reference [S_3AR]



A similar breakdown of CAT member TTPs during physical ingress activity can be performed using the proposed social engineering/physical ingress attack framework.

Example – Attacker Ingress and Social Engineering on a Notional Company Headquarters

Description: In April 2013, **an attacker impersonating a company vice president** used a fake badge to enter the corporate headquarters of a France-based multinational company to obtain key financial information housed on company servers, which were located onsite in another vice president's office. **The attacker social-engineered the administrative assistant using perfect French** to gain 15 minutes of unescorted access to the office, where they implanted a remote access trojan (RAT) device. **After receiving the assistant's verbal consent to enter the target location**, the attacker used an RFID skimmer to pull badge and pin information from another company employee to legitimize their own doctored badge and gain access to the target location and system. **The RAT device was configured to contact a command and control server in Ukraine**. Using the RAT, the attacker took control of the system of interest. The attacker then successfully received callback to the device and used it to log keystrokes, browse and view the desktop, and exfiltrate financial documents.



CAT – Close Access Team; RFID – Radio-Frequency Identification; TTPs – Tactics, Techniques, and Procedures

Presentation Roadmap

Introduction to Cyber Ingress and MITRE ATT&CK for On-Network Cyber Activity

- Overview of CAT's use to understand cyber ingress
- Overview of framework as used in APT29 cyberattack
- Use of data collection standards and framework to generate meaningful trends

S_3AR – A Framework for Understanding Physical Ingress and Social Engineering Activity

- Review of academic literature
- Survey of CAT members
- Introduction to IDA's framework: Social Spoofing Security Analysis Reference (S_3AR)

Development of CAT Data Standards

- Planning and preparation
- Daily actions
- Systems accessed
- Possible trends garnered from improved data

Priorities for Data Collection

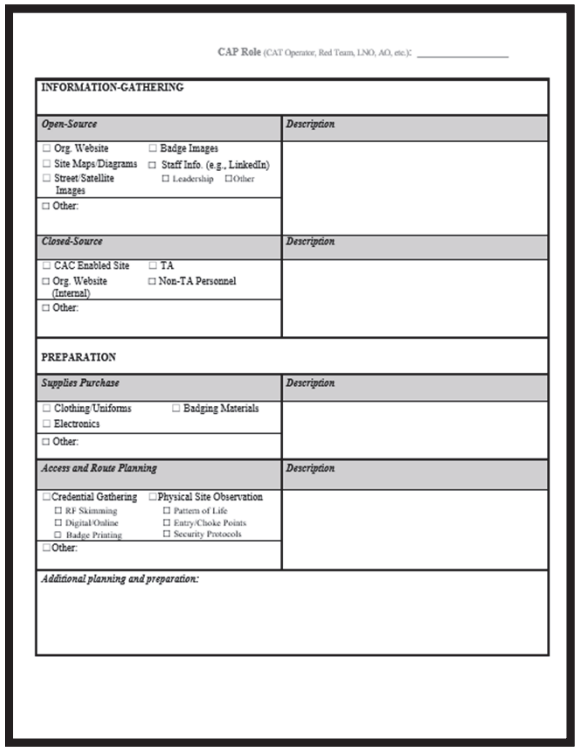
Avoid imposing additional burden on operators (e.g., time or effort).

- Make surveys short and easy to complete (≤ 10 minutes/sheet).
- Act in a systematic fashion to collect informative data.
- Collect baseline data across all missions and scenarios.
- Ensure data cover fundamental mission elements in a variety of ways.
- Ensure data are informative even without operator clarification.
  - Make narratives and explanations optional, not required.

Be accurate.

- Operators should be able to complete surveys from memory (with high confidence).
- Data collection should not require extensive logging, note-taking, or documentation.
- Data collectors will be able to collect more detailed information with future iterations of these standards.

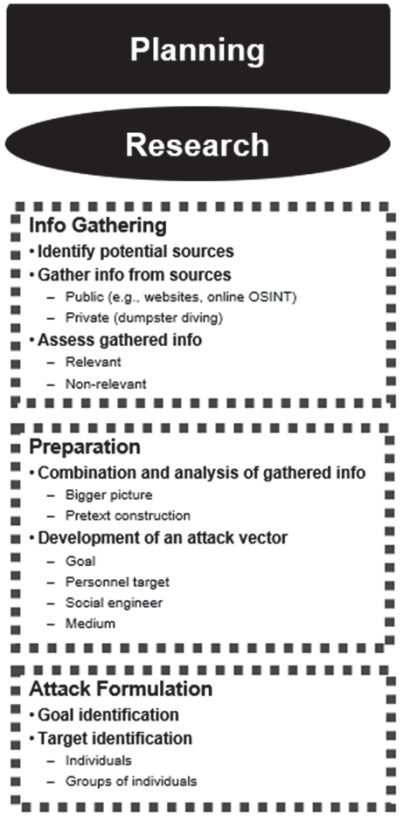
The Planning and Preparation DCS will be completed at the beginning of each location ingress attempt and as additional planning actions are performed.



CAP Role (CAT Operator, Red Team, LNO, AO, etc.): _____

INFORMATION-GATHERING	
Open-Source	*Description*
☐ Org. Website ☐ Badge Images ☐ Site Maps/Diagrams ☐ Staff Info. (e.g., LinkedIn) ☐ Street/Satellite Images ☐ Leadership ☐ Other ☐ Other:	
Closed-Source	*Description*
☐ CAC Enabled Site ☐ TA ☐ Org. Website (Internal) ☐ Non-TA Personnel ☐ Other:	
PREPARATION	
Supplies Purchase	*Description*
☐ Clothing/Uniforms ☐ Badging Materials ☐ Electronics ☐ Other:	
Access and Route Planning	*Description*
☐ Credential Gathering ☐ Physical Site Observation ☐ RF Skimming ☐ Pattern of Life ☐ Digital/Online ☐ Entry/Choke Points ☐ Badge Printing ☐ Security Protocols ☐ Other:	
Additional planning and preparation:	

Planning and Prep DCS

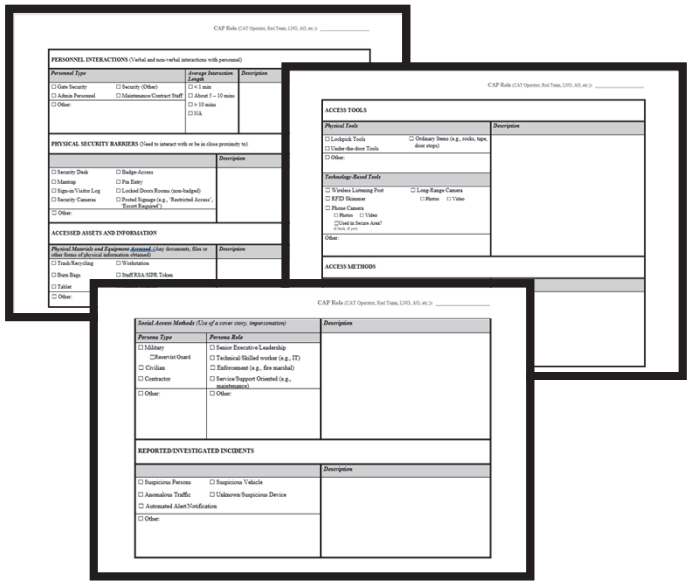


Ms. Amy Guaman-Dumencela
OED

Dr. Sarah Shaffer
OED

DCS – Data Collection Sheet

The Daily Actions DCS will be completed at least once daily but may be completed multiple times a day, as each specific location/target will require its own sheet.



Daily Actions DCS

Ingress

Ingress

Physical Ingress
- **Fake badges (w/o electronic credentials)**
- **Latch/gap slipping**
  - Found item
  - Hook screwdriver
  - Thumb tun flipper
  - Compressed air/motion sensor trigger
  - K22/K23/K24
- **Lock picking**
  - Found item
  - Skeleton key/comb pick
  - Tubular lock picker
  - Other lock picker
- **Unlocked entrance**
  - Key-box breach

Electronic Ingress
- **Fake badges (w/ electronic credentials)**
- **Back-end skimming**
- **Radio-frequency ID skimming**
  - Badge
  - PIN
  - Combo badge/PIN
  - Key fob

Lateral

Leveraging Personal Interactions and Intermediary Access Methods

Leverage Social Interactions
- **Intentional**
  - Cover story
- **Opportunistic**
  - Cover story

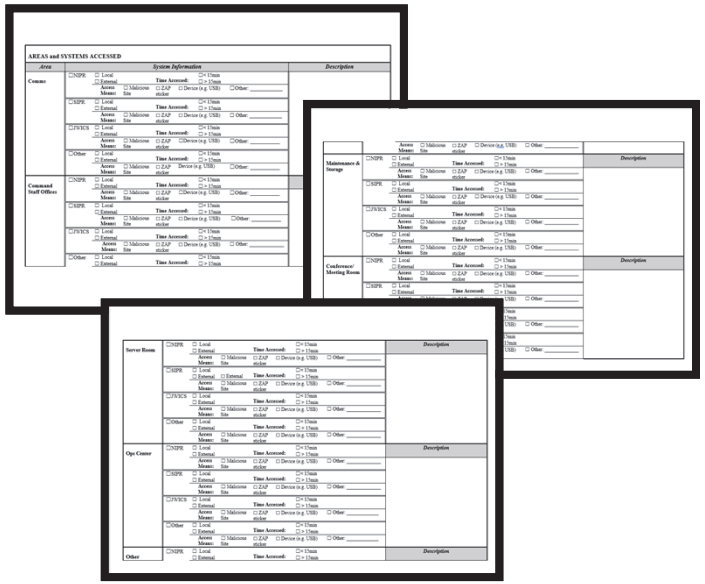
Leverage Social Vulnerabilities
- **Intentional**
- **Opportunistic**
  - Piggybacking

Ms. Amy Guaman-Dumencela
OED

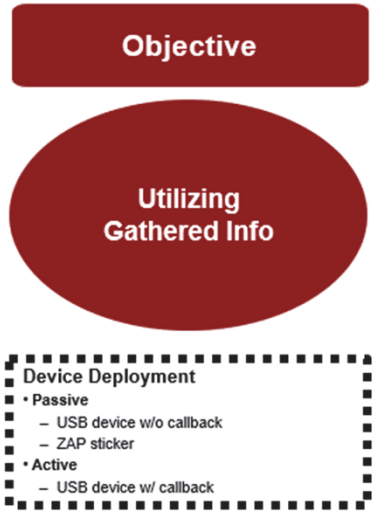
Dr. Sarah Shaffer
OED

DCS – Data Collection Sheet

The Systems Accessed DCS will be completed daily for each group system access for common building areas that CATs target.



Systems Accessed DCS



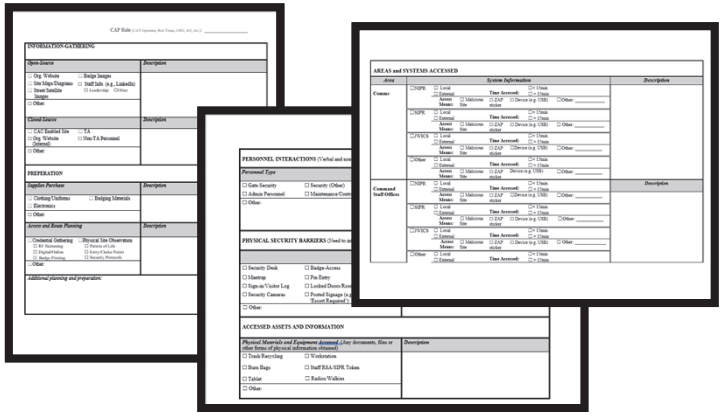
Ms. Amy Guaman-Dumencela
OED

Dr. Sarah Shaffer
OED

CAT – Close Access Team; DCS – Data Collection Sheet

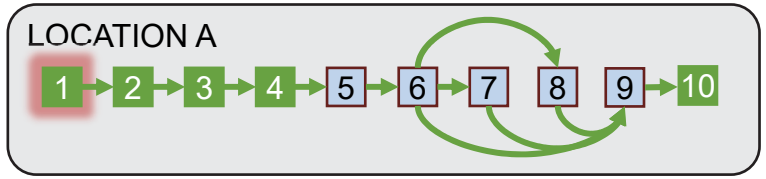
IDA has laid the groundwork for more granular and consistent data collection efforts.

Data Collection Sheets (Red Team Product)

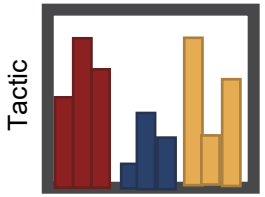


Attack Thread Spreadsheet (IDA Tool)

SE Framework TACTIC	SE Framework TECHNIQUE	SE Framework SUB-TECHNIQUE
Attack Formulation	Goal Identification	N/A
Attack Formulation	Target Identification	Individual
Attack Formulation	Target Identification	System
Information Gathering	Identify Potential sources	N/A
Information Gathering	Gather Information from sources	Public (Websites, Social Media etc



Attack Thread (IDA Product)



Possible Trend Analysis (IDA Product)

Completed Work

- Comprehensively reviewed the academic literature on social engineering and psychological deception to inform an analysis framework.
- Surveyed CAT members to confirm their common use of the tactics, techniques, and procedures described in prior CAT mission reports.
- Developed a physical ingress/social engineering framework informed by CAT member feedback, academic literature, and real CAT mission results.
- Created standardized data collection sheets that span mission planning, location ingress, post-ingress activities, and access to systems of interest.

CAT data standards and S_3AR will allow IDA to perform more granular analyses of CAT operations to provide more insightful feedback on physical ingress vulnerabilities in the Department of Defense.

CAT – Close Access Team; S_3AR – Social Spoofing Security Analysis Reference