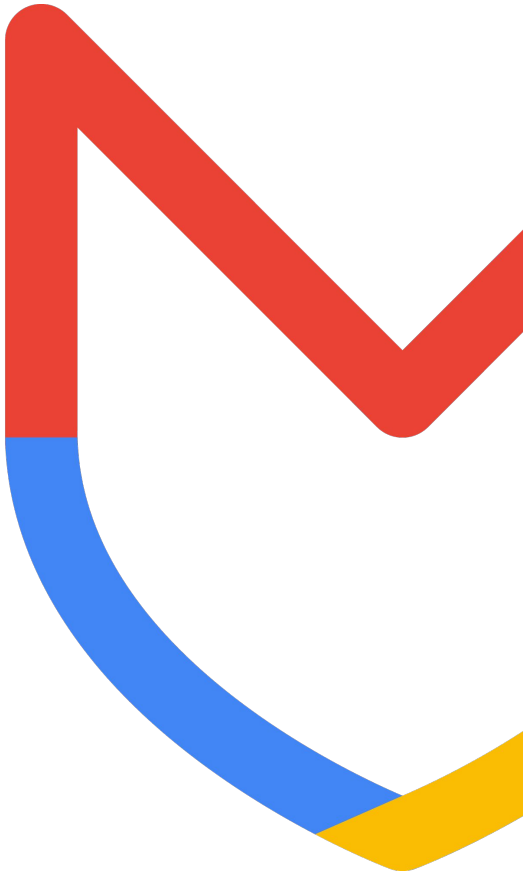
Deception in Depth for ICS

Guidance For Deception Deployment



2025

Brent Muir

Google Cloud

Security

Proprietary & Confidential

“Case studies and examples are drawn from our experiences and activities working for a variety of customers, and do not represent our work for any one customer or set of customers. In many cases, facts have been changed to obscure the identity of our customers and individuals associated with our customers.”



In our current state of cyber security, breaches are inevitable. Assume breach...”

Kevin Mandia, CEO, *Mandiant*

Assume Breach Mindset

01 Assume **Zero Days**

02 Assume **Credential Loss**

03 Assume **Social Engineering**

04 Assume **Controls Drifts**

Agenda

Problem statement

Demystifying Deception

Deception Strategies

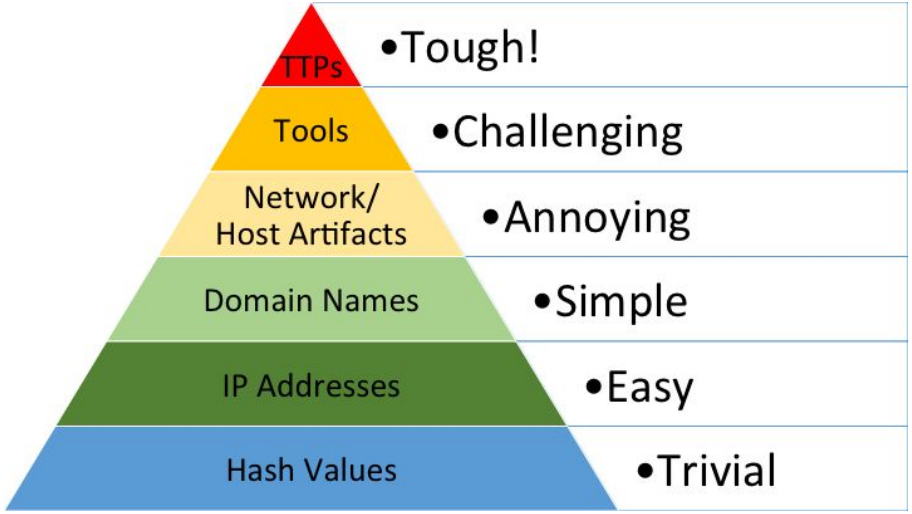
From Theory To Practice

Problem Statement

- SOCs are drowning in alerts
- APT groups are constantly evolving and becoming more clever at bypassing security controls.
- Threat hunting for TTPs is great, but time consuming

The Answer?

DECEPTION



http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html



Mislead, confuse, hide critical assets from, or expose covertly tainted assets to the adversary”

NIST Special Publication 800-160, Volume 2, Revision 1:

Developing Cyber-Resilient Systems

Demystifying Deception

01 Myth # 1 – Deception is hard

02 Myth # 2 – Deception is expensive

03 Myth # 3 – Deception doesn’t work

Benefits of Deception

01 Early Detection of Threats
02 Increased Situational Awareness
03 Reduce False Positives
04 Enhance Incident Response
05 Cost-Effective

The Five Pillars of Success for Deception

01 Technology

02 Cyber Defense Capabilities

03 Threat Intelligence

04 Adversarial Threat Modelling

05 Threat Hunting

Common Deception Tactics

Lures (EAC0005) – Deceptive systems and artifacts intended to serve as decoys, breadcrumbs, or bait to elicit a specific response from the adversary.

- Examples: Credential seeding in memory, cache files, and other data repositories.

Personas (EAC0012) – Create fictitious human user(s) through a combination of planted data and revealed behaviour patterns.

- Examples: Fake social media accounts, fake network accounts, fake email addresses, added into various databases and other systems.

Pocket Litter (EAC0011) – Data used to support the engagement narrative.

- Examples: System and network artifacts, to provide cover to support other deception tactics.

Common Deception Tactics Cont.

Artifact Diversity (EAC0022) – Present the adversary with a variety of network and system artifacts.

- Examples: Physical or virtual traditional honeypot devices, running diverse applications.

Network Diversity (EAC0007) – Use a diverse set of devices on the network to help establish the legitimacy of a deceptive network.

- Examples: Physical or virtual network honeypot devices, running various services to appear legitimate (e.g. PLC, RTU, etc.).

Application Diversity (EAC0006) – Present the adversary with a variety of installed applications and services.

- Examples: Honeypot application stack, running various services to appear legitimate (e.g. IIS, SQL, etc.).

Introduced Vulnerabilities (EAC0023) – Intentionally introduce vulnerabilities into the environment for the adversary to exploit.

- Examples: Obfuscated JavaScript that is run on website and repos, that if cloned, will send alert to SOC.

MITRE Engage Framework

Stage	Description
Plan	Identify and align an operation with a desired end-state
Collect	Gather adversary tools, observe tactics, and collect other raw intelligence about the adversary's activity
Detect	Establish or maintain awareness of adversary activity
Prevent	Stop all or part of the adversary's ability to conduct their operation as intended
Direct	Encourage or discourage the adversary from conducting their operation as intended
Disrupt	Impair the adversary's ability to conduct their operation as intended
Reassure	Add authenticity to deceptive components to convince an adversary that an environment is real
Motivate	Encourage the adversary to conduct part or all of their mission
Analyze	Retrospective review of information gained from an operation



https://engage.mitre.org/

Operationalising Deception

1. Adversarial threat modelling / threat profiling
   - *Which threat actors are targeting your organization?*
   - *Which assets are they most likely to target?*
   - *What is the attack path that could lead to the compromise / unauthorised access of the asset?*
2. Designing Deception
3. Deception Deployment
4. Deception Monitoring

From Theory to Practice

Example Deception Strategy – APT44: Plan

Overview of TA: APT44 is a cyber espionage motivated threat actor, targeting a range of industries, including Critical Infrastructure (CI), such as Energy and Utilities.

Detect and disrupt APT44 activities across the organization, prior to any adverse actions undertaken by the Threat Actor.

APT44: aka Sandworm Team, DEV-0960 (Microsoft), Dark Basin (Citizen Lab), Frozenbarents (Google), Greyenergy (ESET), Hades (Kaspersky), Quedagh (F-Secure), Sandworm (ANSSI), Seashell Blizzard (Microsoft), Telebots (ESET), UAC-0082 (Ukrainian Government), Uac0113 (Recorded Future), Unk_cosmopatron (Proofpoint), Zebrocy (Kaspersky)

APT44 is a dynamic and operationally mature threat actor that has carried out the full-spectrum of espionage, influence and attack operations since as early as 2009. The group's long-standing center focus has been Ukraine, where it has carried out a campaign of disruptive and destructive attacks over the past decade using wiper malware, including during Russia's re-invasion in 2022. Beyond Ukraine, the group continues to sustain espionage operations that are global in scope and illustrative of the Russian military's far-reaching ambitions and interests in other regions.

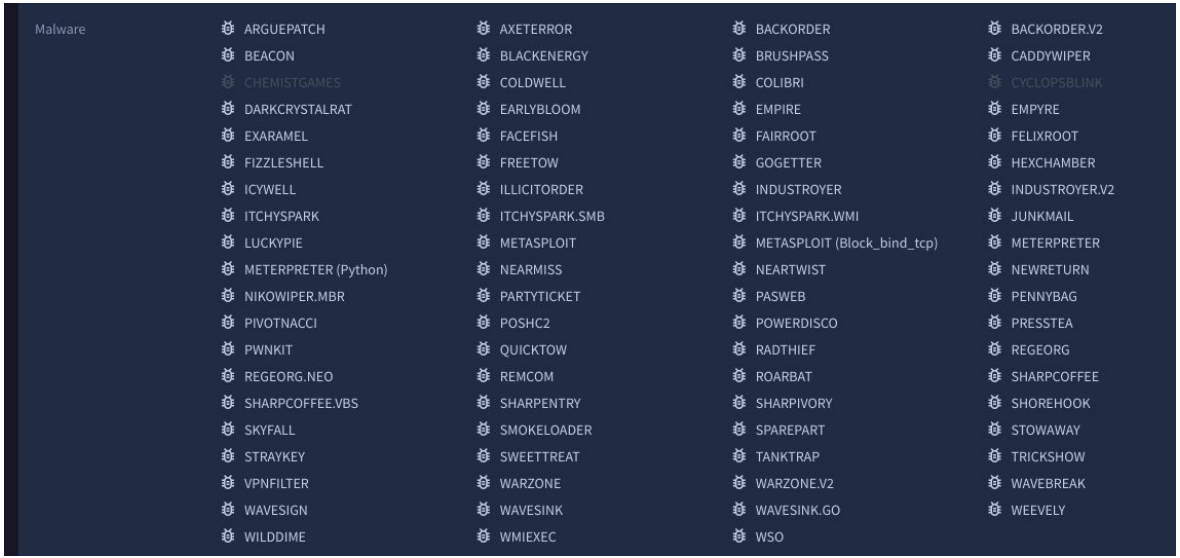
Example Deception Strategy – APT44: Collect

APT44 MITRE ATT&CK TTP mapping;



Example Deception Strategy – APT44: Collect

APT44 associated malware;



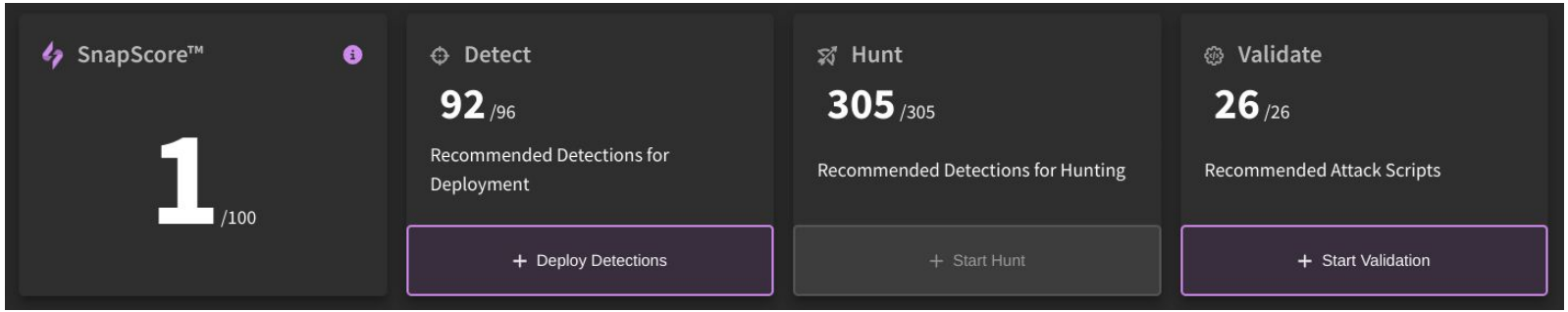
Example Deception Strategy – APT44: Collect

APT44 associated tooling;



Example Deception Strategy – APT44: Detect

- Obtain list of APT44 IOCs available from TI partners (e.g. GTI / Mandiant Advantage) to be added to detection use-cases.
- Conduct detection-mapping of APT44 TTPs, add additional to to be added to EDR detection use-cases.
- Additional detection use-case logic - e.g. APT44 | SnapAttack



Example Deception Strategy – APT44: Prevent

APT44 TTP Examples (not complete list);

ATT&CK Technique	Prevention Mechanism/s (not a complete list)
Spear Phishing (T1566 / ICS - T0865)	· URL rewriting · URL sandboxing · IOC blocking (email gateway and web proxy) · Abused file extension blocking (email gateway)
Command and Scripting Interpreter (T1059)	· Application allow listing, including scripting engines, and high-risk binaries
Remote Services (T1021 / ICS - T0886)	· Privileged Account Management (PAM) · Password Policies

***NOTE**: Confirmation of current security controls across the proposed deployment environments is required, from Business/System owners, confirmed via SOC team on detection/monitoring.*

Example Deception Strategy – APT44: Direct

Deception Strategy (Engage Technique)	Deception Seeding	Expected Outcome
Personas (EAC0012); fake email addresses and social media presence.	Create a LinkedIn profile for an “employee” within the company, who would have access to privileged credentials (e.g. IT engineer). Ensure fake employee profile has connections to trusted company employees within the organization, to provide a level of validity to the profile.	Create detection rules if anyone else sends a connection request to the profile. Create detection rules for associated email address for the “employee”.

Example Deception Strategy – APT44: Disrupt

Deception Strategy (Engage Technique)	Deception Seeding	Expected Outcome
Lures (EAC0005); Canary documents containing fake network IP addresses, fake host names, etc.	Add canary documents into Content Management System (CMS), online intranet repositories, etc.	Create detection rule for any attempted access of canary document, as well as traffic to the fake network/host names.

Example Deception Strategy – APT44: Reassure

Deception Strategy (Engage Technique)	Deception Seeding	Expected Outcome
Lures (EAC0005) / Personas (EAC0012); Create AD account (disabled).	Inject AD credentials into memory, SVN repositories, RDP, SSH, and canary documents seeded across the organization's intranet and Content Management System (CMS).	Create detection rules for any action attempted against AD account.
Pocket Litter (EAC0011); fake emails inside Persona mailbox, fake documents on honeypot systems.	Ensure the related honeypot systems and accounts (e.g. email) are seeded with innocuous documents/emails, to convince a Threat Actor that they have compromised legitimate accounts/systems.	Threat actor will assume device, stored data, and user accounts are valid, triggering alerts once accessed.

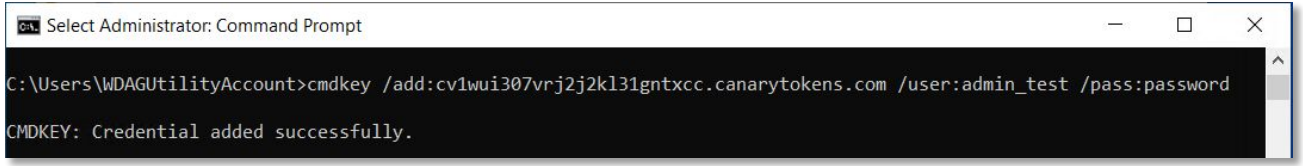
Example seeding the environment; In-Memory Credentials

- Using the ***New-HoneyHash.ps1*** PowerShell script (from the **Empire** project), or the ***cmdkey*** command will inject fake credentials into memory in Windows.
- Once an adversary dumps credentials from memory (e.g. LSASS, Mimikatz, etc.) these credentials will be present.
- Any attempt to use these credentials will trigger an alert.

1. Setup a fake account on AD, give it an interesting name (e.g. **admin123**)
2. Disable the account.
3. Setup monitoring of the account through your SIEM (any attempt to use/access the account should trigger a high-severity alert).
4. Inject the fake credentials into memory (e.g. ***New-HoneyHash,*** or ***cmdkey***)

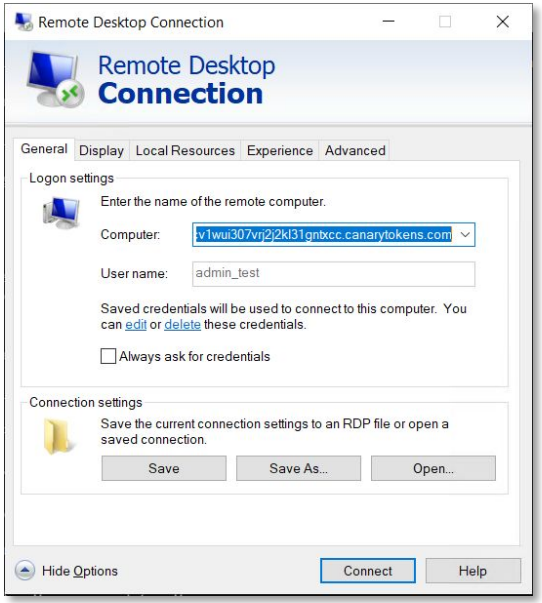
Example seeding the environment; Cached RDP Credentials

1. Use the **cmdkey** command to add the canary DNS hostname and fake credentials into memory, example below;



2. Create an **RDP connection file** including the canary DNS host name, choose “Save As…”;

3. Rename the RDP connection file, to give it an interesting name (E.g. OrgDC1) and store the RDP connection file in a directory where it is unlikely to be triggered accidently (e.g. **C:\Users\admin123\Desktop**).



Example Deception Strategy – APT44: Motivate

Deception Strategy (Engage Technique)	Deception Seeding	Expected Outcome
Lures (EAC0005); Canary database entries.	Create a fake network topology documents for honeypot ICS environment entries. Create fake spreadsheet with credentials to honeypot ICS environment.	Any access to the files will trigger an alert to the SOC (via File Integrity Monitoring).
Network Diversity (EAC0007); Honeypot VLAN.	Create a separate VLAN, used to convince/trick an adversary into believing that they are inside the ICS environment.	Threat Actor will be convinced of legitimacy of the systems/network that they have compromised.
Application Diversity (EAC0006) / Artifact Diversity (EAC0022); Honeypot systems/applications (on honeypot VLAN).	Create honeypot systems within the honeypot VLAN, e.g. PLC, RTU, HMI systems, application servers, databases, etc.	When APT44, or other Threat Actor, triggers a deception technique, there is an option to force the adversary onto the honeypot VLAN, in order to further analyse their TTPs.

Example Deception Strategy – APT44: Analyze

At the conclusion of a campaign that triggers any of the above deception techniques, review the relevant incident;

1. Map the campaign to the deception techniques;
   - *Did the adversary follow the intended path?*
2. Identify whether the deception strategy was successful;
   - *Did the adversary trigger the lure?*
   - *Did the detection alert trigger?*
3. Identify any potential deception improvements or additional placements of deception techniques.

Create an addendum report, to be consumed alongside the incident report, highlighting the success/weaknesses of the deception tactics.

ICS Honeypot

ICS Honeypot Design Goals

1. Do no harm (no actual ICS/OT access or impact).
2. Do no harm (no actual ICS/OT access or impact).
3. The honeypot should be indistinguishable from an actual ICS device (from an attacker's perspective).
4. Once placed, it should require minimal support/maintenance (always-on, low-powered, ruggedized).
5. The honeypot should assist in identifying adversarial tooling, and TTPs.
6. The honeypot should keep the adversary busy, away from production OT.
7. Any interaction with the honeypot systems should be considered suspicious.

ICS Device Emulation / Honeypot

Benefits:

- Early detection of adversaries
- Adversarial monitoring
- Reduce cost via emulation

Tooling:

- OpenPLC
- FakeNet-NG
- Honeyd
- OpenCanary
- Interactive Protocol Listeners (e.g. pyModbus, opendnp3, bacpypes, etc.)
- Containers
- Virtual Machines

Common ICS Devices / Protocols to Emulate

Emulation of services/devices;

- HMI
- PLC
- RTU
- USB devices
- Databases (e.g. Oracle DB, Historian, SQL, etc.)

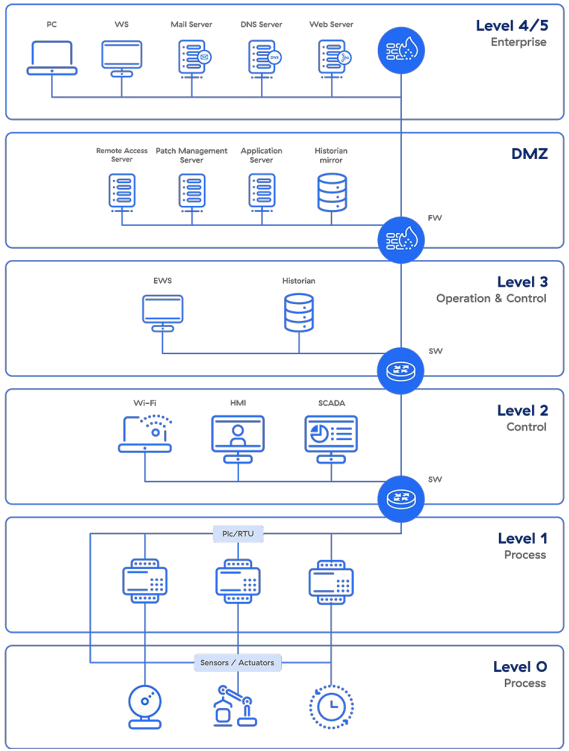
Emulation of ports/protocols;

- MODBUS
- DNP3
- BACnet
- Siemens S7
- FTP/SFTP
- ssh
- SAMBA
- RDP

Common ICS Protocols / Ports

Protocol Name	Ethernet Ports
Modbus TCP	TCP 502
Ethernet/IP	TCP 44818 / UDP 2222, 44818
DNP3	TCP 20000 / UDP 20000
ICCP	TCP 102
GE EGD	UDP 7937, 18426
Profinet	TCP 34962 – 34964, UDP 34962 – 34964
OPC Classic	TCP 1024 - 65535
OSIsoft PI	TCP 5450
Siemens S7	TCP 102
BACnet	UDP 47808

Purdue Placement for Honeypot Devices



	Device	Protocol	Listeners
Level 3.5	Jumphost/PAW	RDP/AD	
Level 3.5	VPN	IPSEC	
Level 3	Historian	Database	
Level 3	Jumphost	RDP	
Level 2	HMI	RDP	
Level 2	SCADA	ssh	
Level 1	PLC	DNP3	
Level 1	RTU	MODBUS	

Monitoring Interactions with ICS “Devices”

Network Traffic Visibility:

- Database queries
- VPN connections
- Other connection requests (e.g. ssh, RDP, etc.)
- PLC/RTU

Interactive Visibility:

- Jumphost login (authentication requests, etc.)
- SFTP actions (uploads/downloads, etc.)
- Jumphost actions (browsing, file access, file creation, process execution, device mounting, etc.)
- Command Line interactions (ssh, bash, cmd, etc.)

Detection Use-Cases

- Dependant on the SIEM (and SIEM logic) being used in your environment.
- Designed to provide contextual information about the adversary's actions (*what did they do, how did they do it, when did they do it,* etc.)

Example detection use-cases (pseudo logic);

- Historian database access
- Ladder logic updated to PLC device over MODBUS
- Firmware updated to RTU device via HMI
- New device (IP/MAC address) observed on LAN
- New USB device observed inside environment

Takeaways

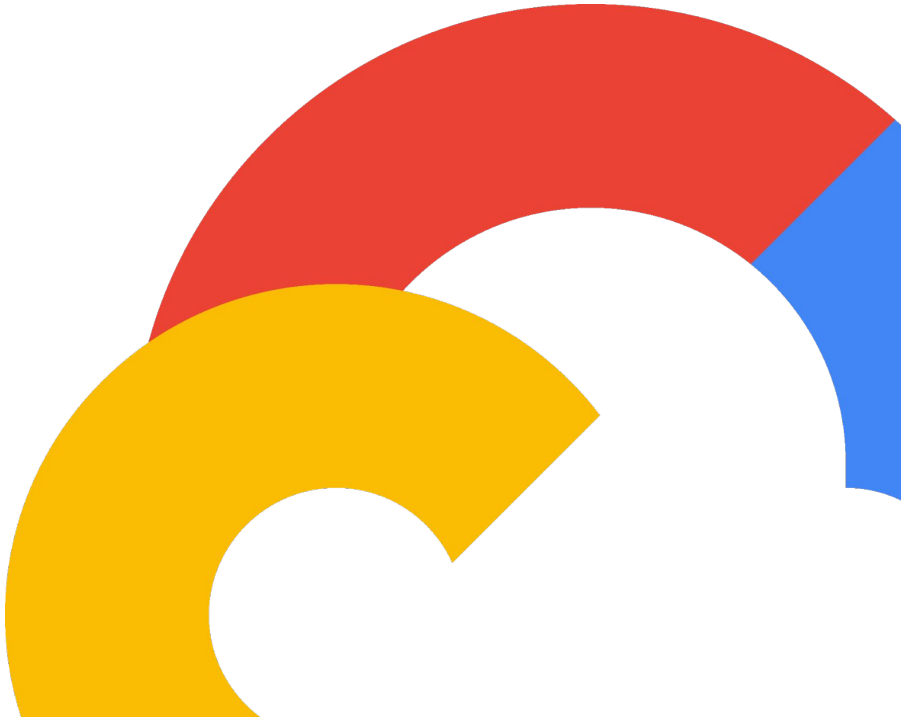
Key Takeaways

1. Know your adversaries
2. Know your environment
3. Deploy Deception!

Thank you

brentmuir@google.com

Google Cloud



Resources

- https://marcusedmondson.com/2022/02/21/dripping-a-little-honey-in-your-environment/
- https://github.com/EmpireProject/Empire/blob/master/data/module_source/management/New-HoneyHash.ps1
- https://canarytokens.org/generate
- https://blog.thinkst.com/2021/06/rdp-cmdkey-canary-and-thee_10.html
- https://twitter.com/markus_neis/status/1397472760859856897
- Setup of low interaction honeypot on a Raspberry Pi Zero W · GitHub - https://gist.github.com/cdeck3r/5151c53b282431158a59091c0e26f27d
- https://engage.mitre.org/
- http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
- https://github.com/dnp3/opendnp3
- https://pymodbus.readthedocs.io/en/latest/
- https://github.com/JoelBender/bacpypes