IDENTITY SECURITY AND PROTECTION

LORENZO INVERNIZZI

Modern Attacks

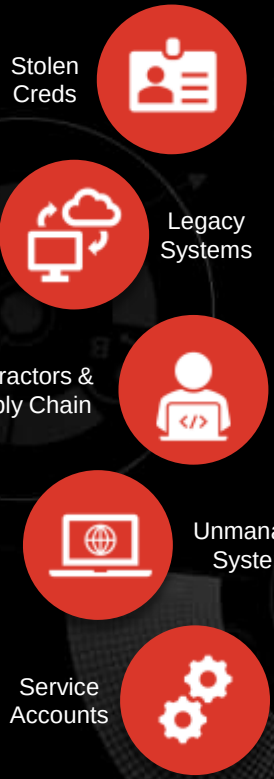
Ransomware, supply chain…

80% of data breaches have a connection to compromised privileged credentials

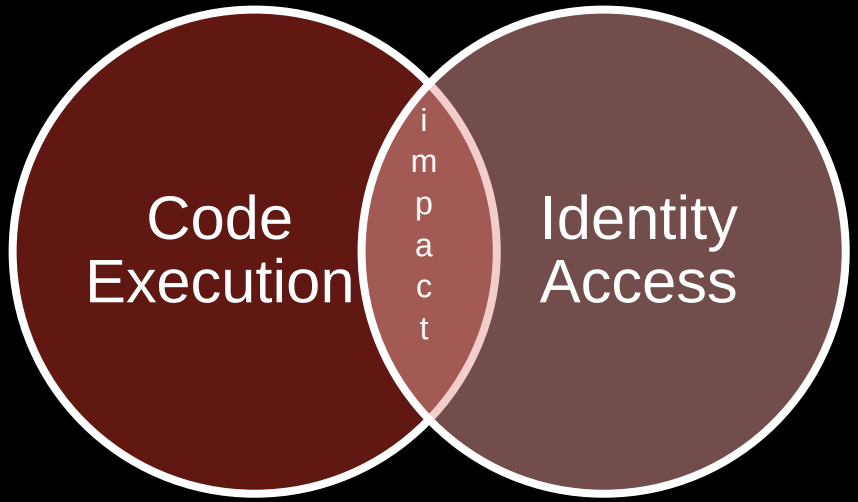
- Forrester Research

Breaches from stolen/compromised credentials took the **longest to detect (250 days!)**

- Cost of a Breach Report, 2021



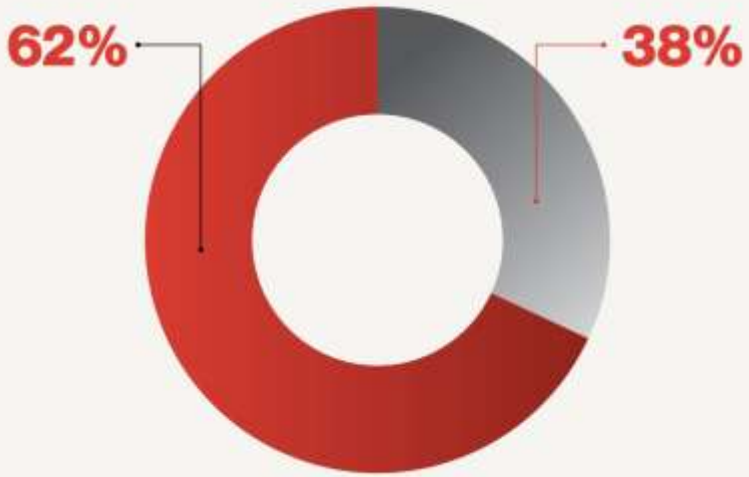
RANSOMWARE: TWO PART PROBLEM



- Ransomware is a two part problem
- Adversary needs to execute code on a single system (low impact)
- Adversary then needs to access and execute code on multiple systems (high impact)
- Solving just one part of the problem is not sufficient
- Why?

Adversary Tactics

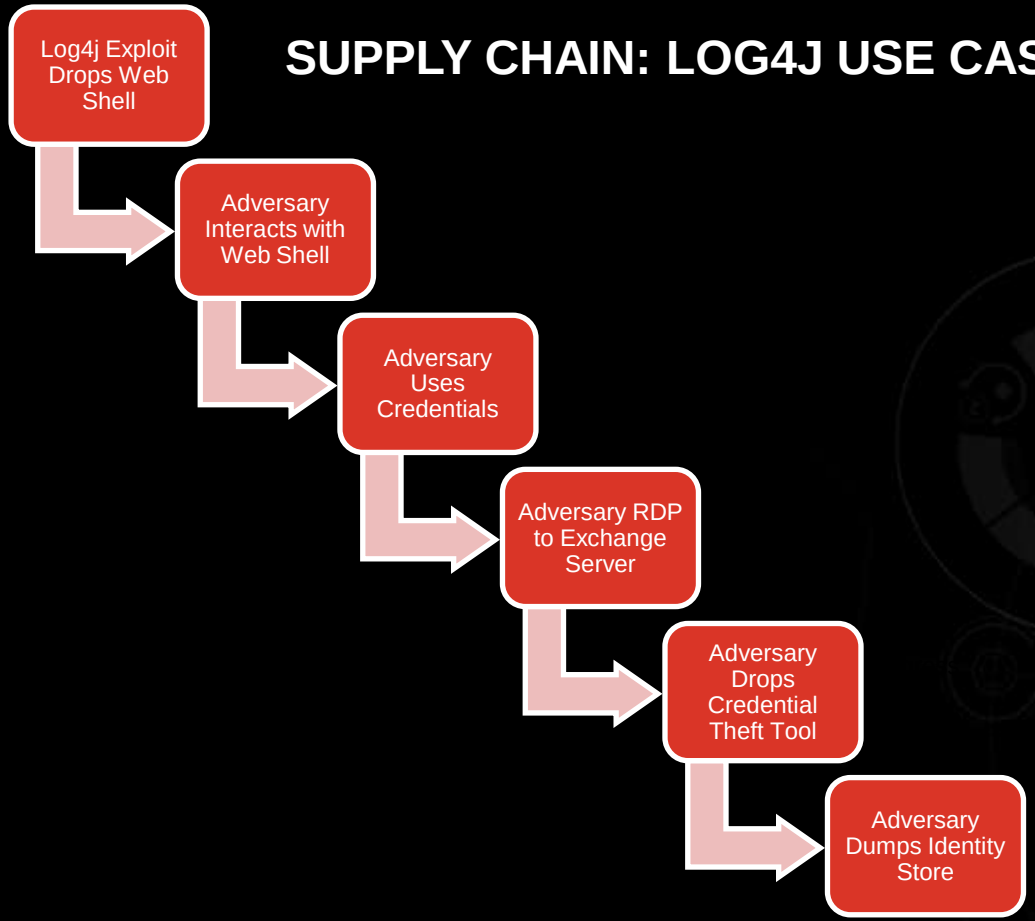
Detections indexed by the CrowdStrike Security Cloud in Q4 2021

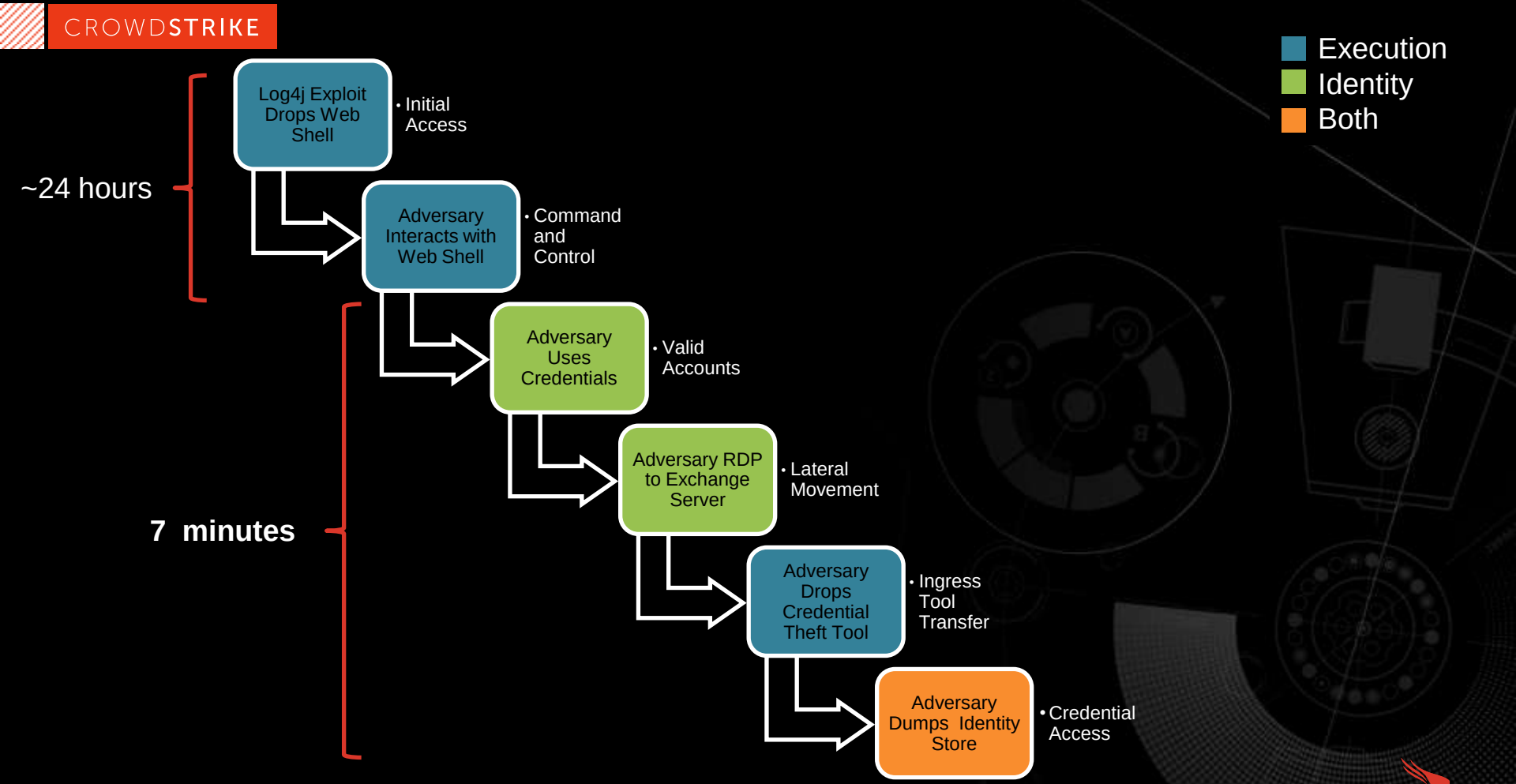


Adversaries continue to show that they have moved beyond malware.

Attackers are increasingly attempting to accomplish their objectives without writing malware to the endpoint. Rather, they have been observed using legitimate credentials and built-in tools — an approach known as "living off the land" (LOTL) — in a deliberate effort to evade detection by legacy antivirus products. Of all detections indexed by the CrowdStrike Security Cloud in the fourth quarter of 2021, 62% were malware-free.

SUPPLY CHAIN: LOG4J USE CASE



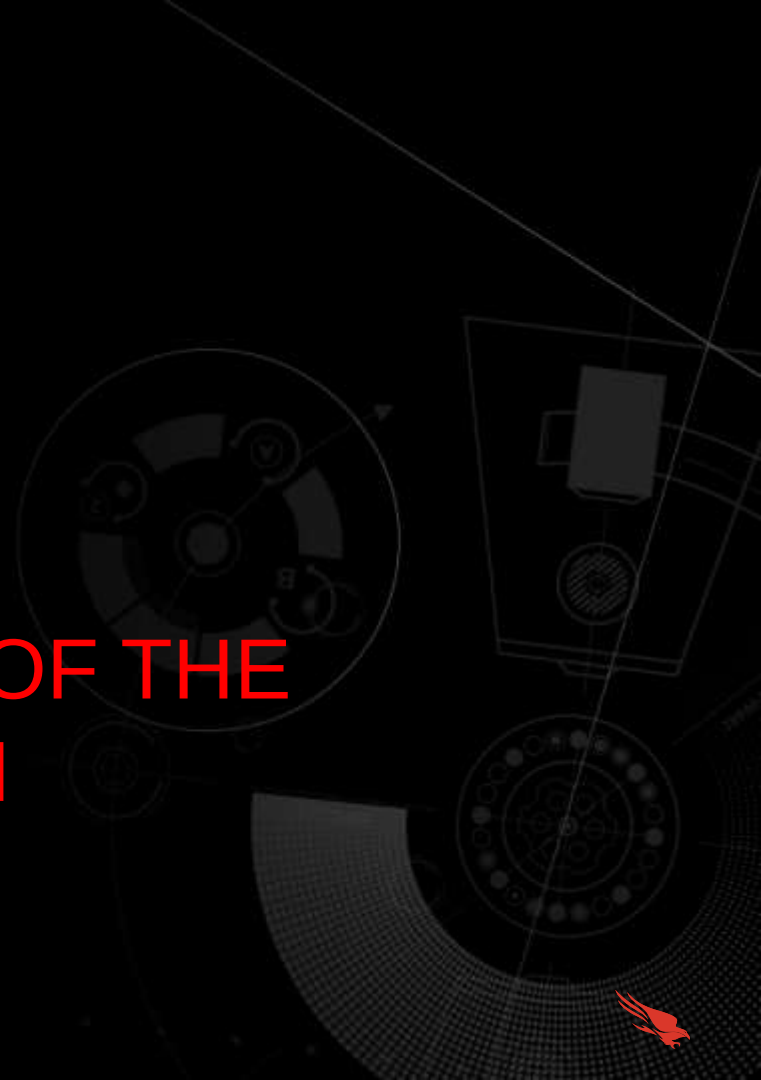

Execution
Identity
Both
~24 hours
7 minutes
Log4j Exploit Drops Web Shell
• Initial Access
Adversary Interacts with Web Shell
• Command and Control
Adversary Uses Credentials
• Valid Accounts
Adversary RDP to Exchange Server
• Lateral Movement
Adversary Drops Credential Theft Tool
• Ingress Tool Transfer
Adversary Dumps Identity Store
• Credential Access

WHAT

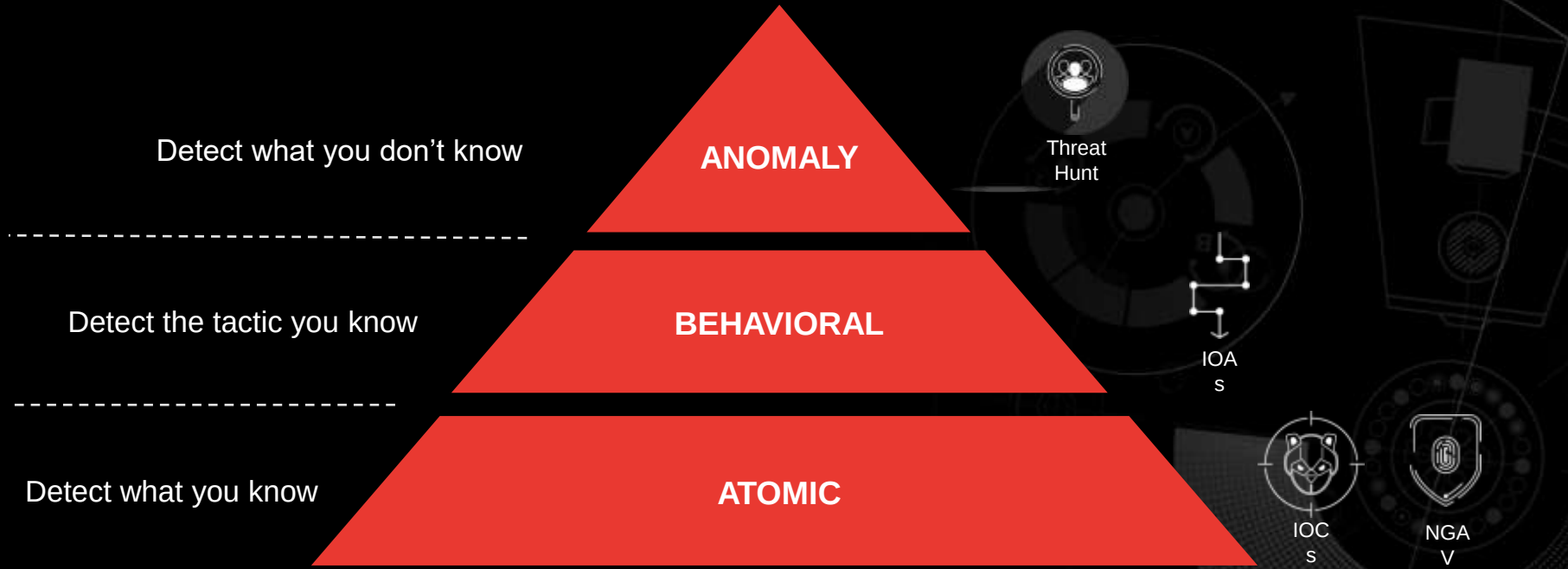
NEXT?

FOCUS ON 80% OF THE PROBLEM

To stop modern attacks



ORGANIZATIONAL MATURITY: DETECTION PROGRAM (ENDPOINT)



CROWDSTRIKE

ORGANIZATIONAL MATURITY: DETECTION PROGRAM (IDENTITY)

CROWDSTRIKE

ORGANIZATIONAL MATURITY: DETECTION PROGRAM (IDENTITY)

Detect what you know

ATOMIC

Signature Detection

CROWDSTRIKE

HOLISTIC DETECTION PROGRAM

ID SIGNATURE DETECTION

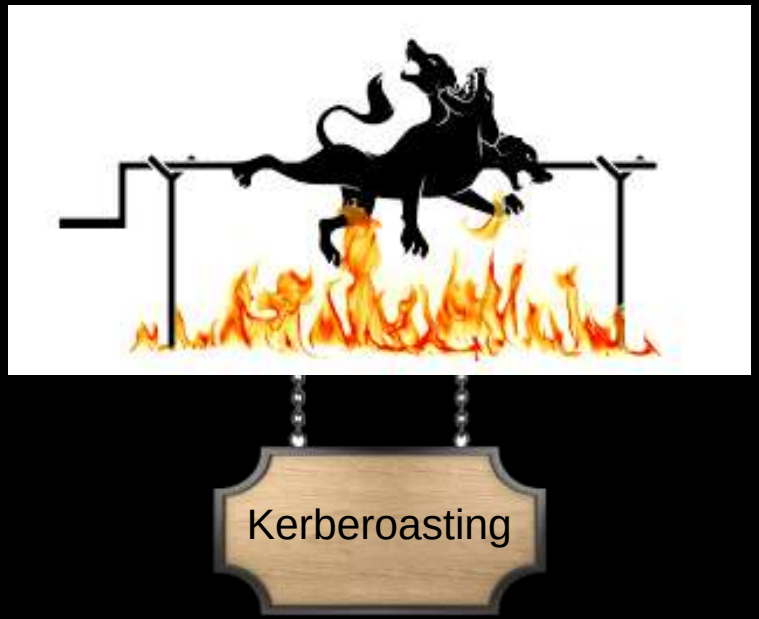
- Active Directory enumeration and analysis toolset
- Utilizes graph theory to show often unintended relationships in AD
- Three main components:
  - Data ingestor
  - Neo4j database
  - BloodHound client

CROWDSTRIKE

ORGANIZATIONAL MATURITY: DETECTION PROGRAM (IDENTITY)

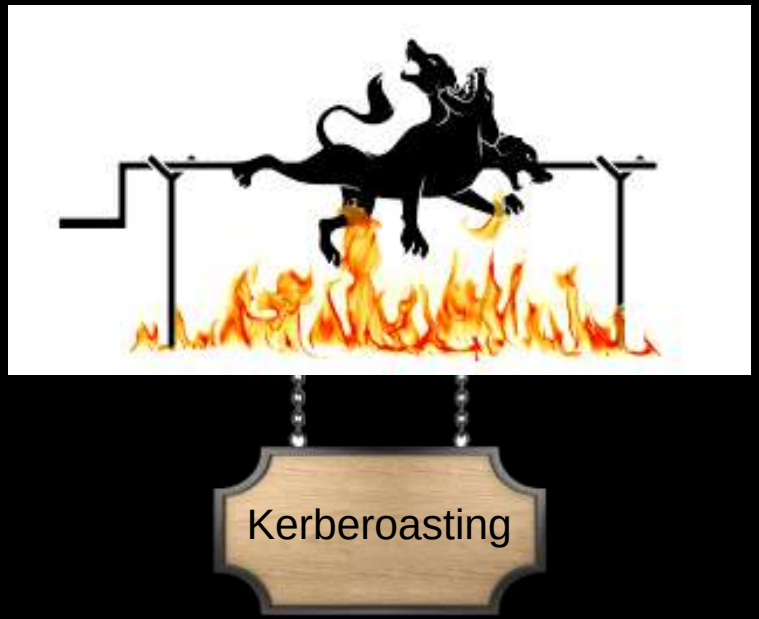
HOLISTIC DETECTION PROGRAM

ID BEHAVIORAL DETECTION



- Compromised account, attackers can request a valid service Kerberos ticket (accounts with SPN)
- Get the ticket offline and crack the pass.
- You can ask for hundreds.. AD never verifies if you use those service tickets (by design ☺)
- ..With that pass you can now move laterally without noise..

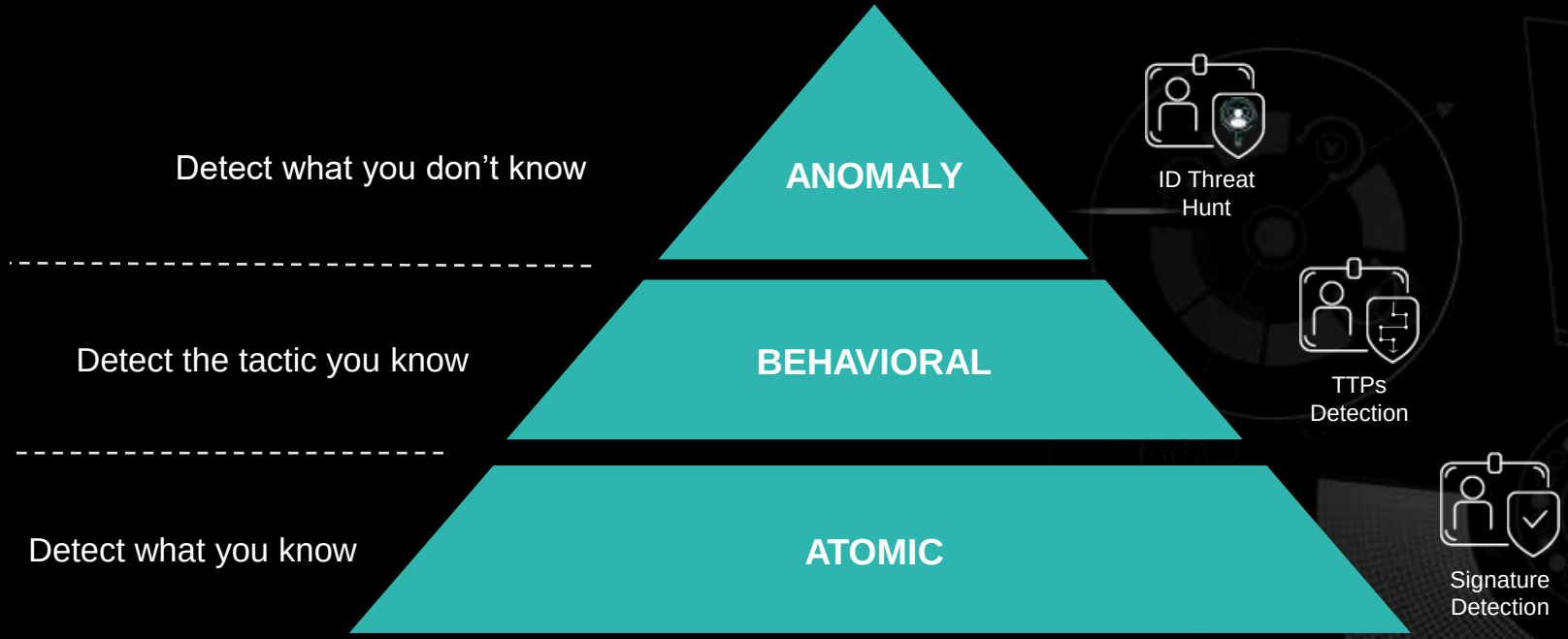
ID BEHAVIORAL DETECTION



- Compromised account, attackers can request a valid service Kerberos ticket (accounts with SPN)
- Get the ticket offline and crack the pass.
- You can ask for hundreds.. AD never verifies if you use those service tickets (by design ☺)
- ..With that pass you can now move laterally without noise..

- **Track the way SPN enumeration is done for verifying if it's legit or…. Not.**

ORGANIZATIONAL MATURITY: DETECTION PROGRAM (IDENTITY)



HOLISTIC DETECTION PROGRAM

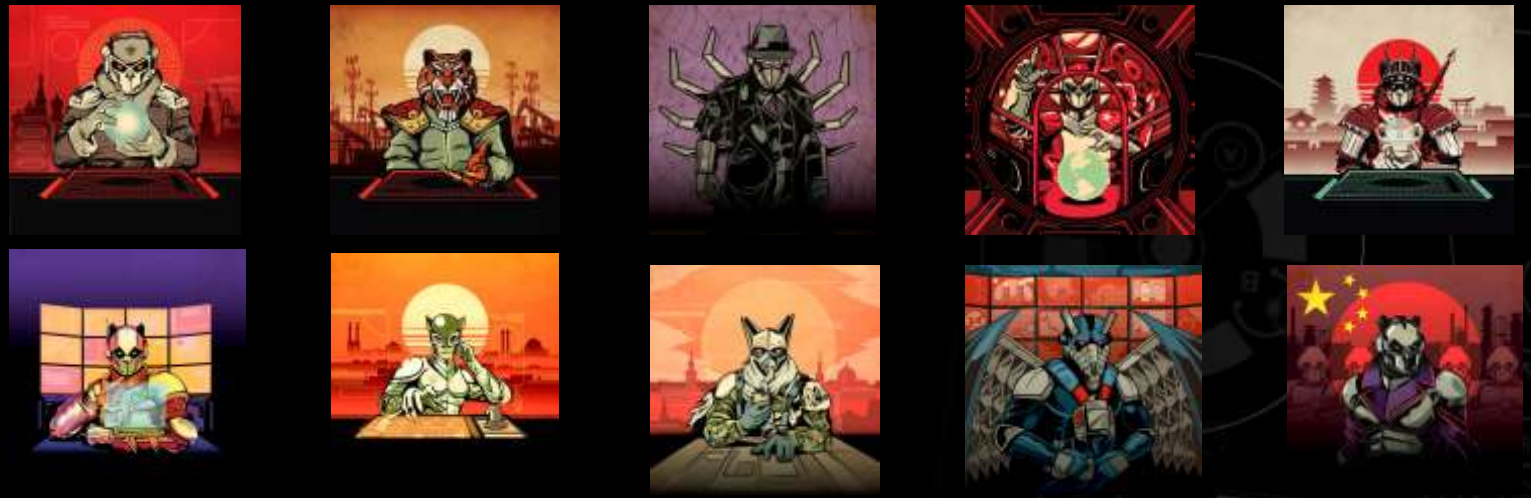
ID THREAT HUNTING

- Attackers can create “valid“ Kerberos “Golden Tickets” in couple of simple steps.
- Once they are created, there is no easy way of detecting them:
  - **TGTs with long lifetimes**
  - **Aberrant domain replication activity**
  - **Changes to privileges (I.E Debug priv)**
  - **…**

ID THREAT HUNTING

- Attackers can create “valid“ Kerberos “Golden Tickets” in couple of simple steps.
- Once they are created, there is no easy way of detecting them:
  - **TGTs with long lifetimes**
  - **Aberrant domain replication activity**
  - **Changes to privileges (I.E Debug priv)**
  - **…**
- **At the end.. Connect the dots (Threat hunt)**

…by the way.. all these 179 actors..



…use it every day since 2014…

…now let's make ~~a plan..~~ a REALISTIC plan

WHAT WE NEED?

WHAT WE NEED?

IDENTITY THREAT DETECTION

- AD abuse evidences
- Risk analysis
- Account Monitoring
- **Behavior analysis**
- **.....**

CROWDSTRIKE

WHAT WE NEED?

IDENTITY THREAT DETECTION

- AD abuse evidences
- Risk analysis
- Account Monitoring
- **Behavior analysis**
- **.....**

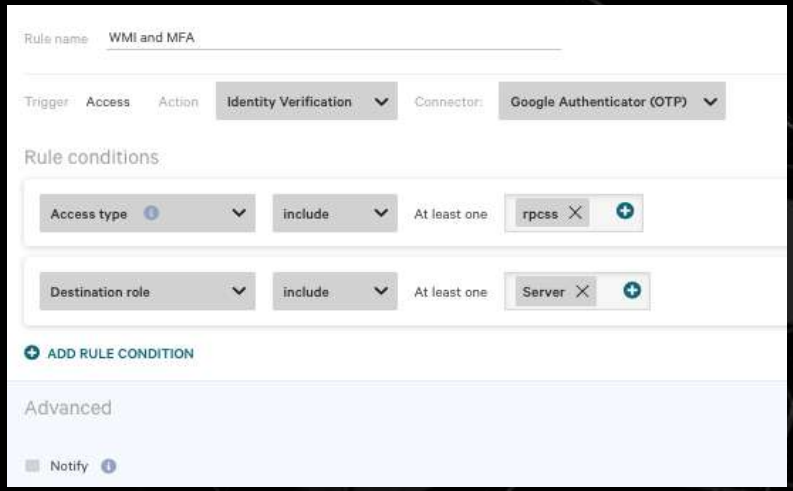
IDENTITY THREAT PROTECTION

- MFA conditional access

SIMPLE POLICIES AGAINST..

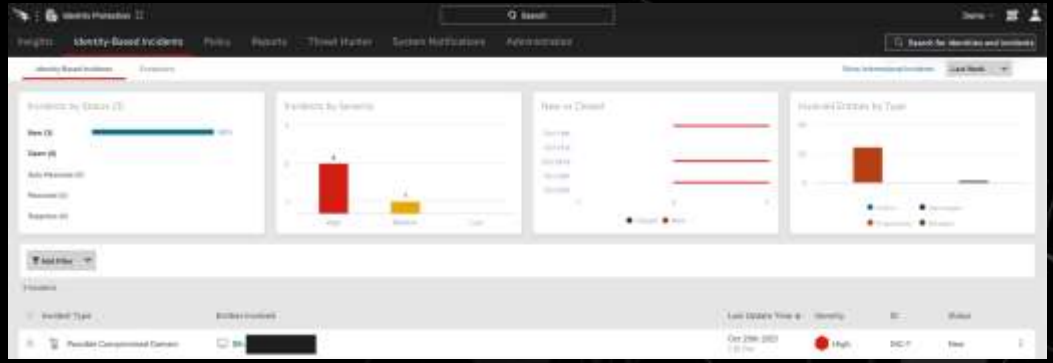
- Detect anomalous LDAP activity + BloodHound signatures

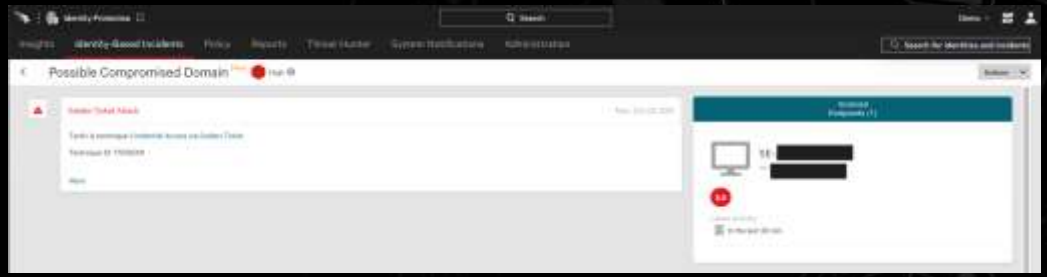
SIMPLE POLICIES AGAINST..



- Force MFA when using RPC. “Roasted” credentials will fail this step..

SIMPLE POLICIES AGAINST..





- Detection via Ticket characteristics and usage…

CROWDSTRIKE

WHAT WE NEED?

IDENTITY THREAT DETECTION

- AD abuse evidences
- Risk analysis
- Account Monitoring
- **Behavior analysis**
- **……**

IDENTITY THREAT HUNTING

Contextual ID threat Identification •

OverWatch / Falcon Complete / Partner •

IDENTITY THREAT PROTECTION

- MFA conditional access

CROWDSTRIKE

WHAT WE NEED?

SEGREGATION BETWEEN SEC/PROD

Keep process & focus on each •

Speed on Incident response •

Contextual correlation on other Incidents •

IDENTITY THREAT DETECTION

- AD abuse evidences
- Risk analysis
- Account Monitoring
- **Behavior analysis**
- **……**

IDENTITY THREAT HUNTING

Contextual ID threat Identification •

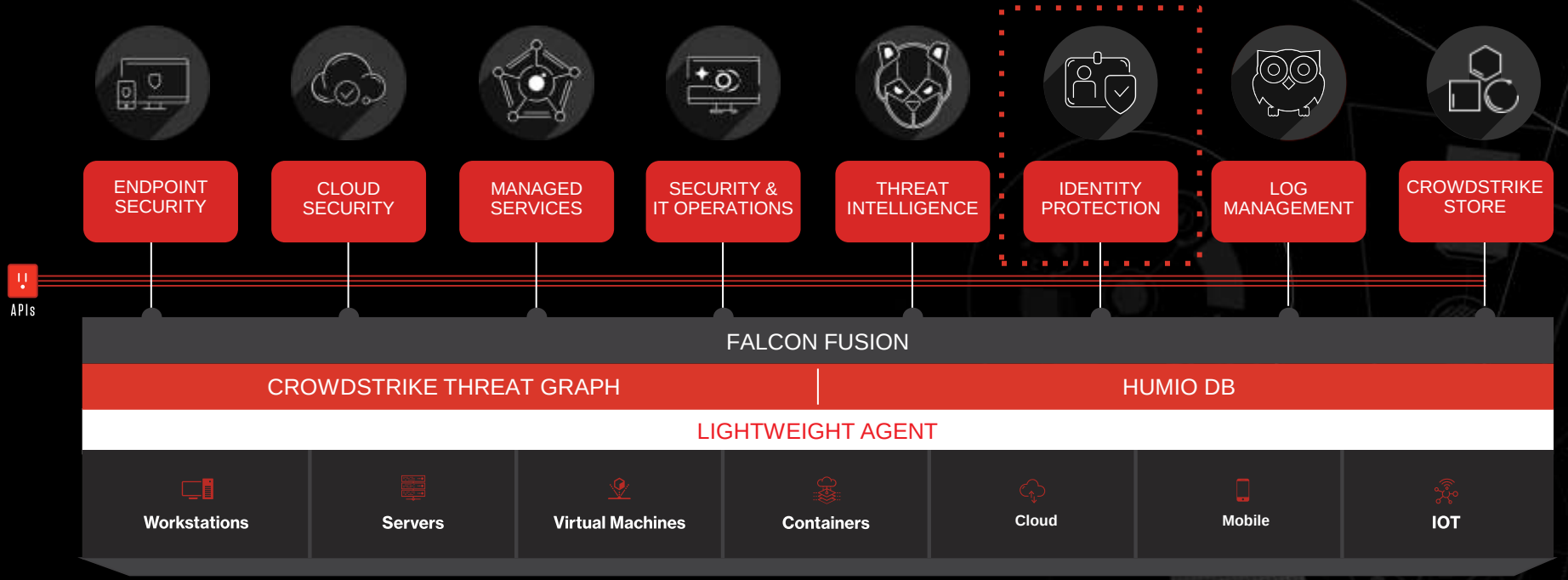
OverWatch / Falcon Complete / Partner •

IDENTITY THREAT PROTECTION

- MFA conditional access

CROWDSTRIKE

Falcon Platform: Defining the Security Cloud




CROWDSTRIKE