SPECTEROPS

Attackers Follow Security Principles Too

Elad Shamir


SPECTER BASH
OCTOBER 7 - 10, 2024
9:00am – 5:00pm Central Time
The Inverness Denver (Hilton)
200 Inverness Drive West • Englewood, Colorado 80112
COURSES:
Red Team Operations
Detection
Identity-Driven Offensive Tradecraft
Tradecraft Analysis
Azure Security Fundamentals
EXCLUSIVE IN-PERSON SWAG
CUTTING EDGE INSIGHTS
LEARN COMPREHENSIVE SKILLS IN HANDS-ON LABS
EVENTS WITH INDUSTRY PEERS
SPECTEROPS.IO/SPECTER-BASH
SPECTEROPS

ADVERSARY TACTICS

SPECTEROPS

Identity-Driven Offensive Tradecraft

Learn to identify and execute a wide range of elaborate attacks against both on-premises and cloud technologies using identity-based attacks.

New Course Coming October 2024!

- **Attack Path Discovery:** Learn to identify Clean Source Principle violations and uncover attack paths.
- **Exploit Identity Architectures:** Gain skills to navigate and exploit on-prem and hybrid identity systems for lateral movement and privilege escalation in complex environments.
- **Advanced Authentication and Authorization Attacks:** Develop expertise in intricate authentication and authorization mechanisms to conduct sophisticated attacks and achieve red team objectives.
- **Abuse Legitimate Configuration Management Systems:** Utilize legitimate configuration management solutions and processes to execute adversary tactics with precision and effectiveness.
- **Hands-on Labs:** Practice skills in a specially designed lab environment that simulates a real-world client environment incorporating a variety of technologies and Attack Paths, including cross-tenant and supply chain attacks.
- **Red vs. Blue Insight:** Learn defenders' perspective and detection logic, as well as OPSEC considerations to counter the detections and keep hacking.

CONFERENCE:
MARCH 31 – APRIL 1, 2025

TRAINING:
APRIL 2 – 5, 2025

TAKE ADVANTAGE OF SPECIAL EARLY BIRD PRICING NOW

- **Location: Convene** – 1201 Wilson Boulevard, Arlington, Virginia 22209
- **Call for Papers opening October 1, 2024**
- **FREE conference pass with paid training ticket**
- **Courses:** Red Team Operations, Identity-Driven Offensive Tradecraft, Tradecraft Analysis and Azure Security Fundamentals

SPECTEROPS.IO/SO-CON

Agenda

- Why attack paths are identity-driven?
- What makes an attack path?
- A framework for attack path discovery

What are Identity-Driven Attacks?

Introduction

- Every modern ecosystem has a mechanism, or a set of mechanisms, that govern access to resources
- These mechanisms must handle **authentication** and **authorization**
  - **Authentication:** Verifying the **identity** of the **principal**
  - **Authorization:** Determining whether the **principal** is permitted to perform an **action** on a **resource** in the **current state**

What are Identity-Driven Attacks?

Authentication

- Authentication can be performed locally by the system or delegated to a designated Identity Provider (IdP) or Identity and Access Management (IAM) solution
- These solutions can be on-premises, in the cloud, or even external to the environment (federated)
- Authentication can be performed using a single or multiple authentication factors (password, certificate, device, biometrics, etc.) and through authentication protocols (Kerberos, NTLM, SAML, OIDC, etc.)

What are Identity-Driven Attacks?

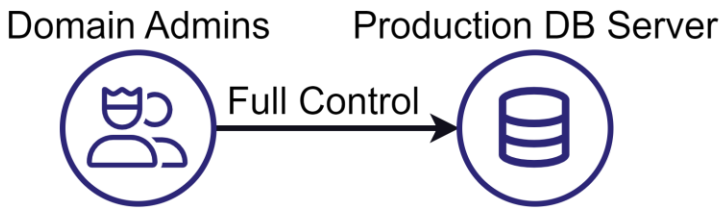
Authorization

- Authorization ultimately boils down to a set of access control rules that apply to the principal or the resource and are enforced by the Security Reference Monitor (SRM) of the operating system or an IAM component of a system
- The access control rules typically have the following elements:
  - **Subject:** The principal that seeks access
  - **Action:** What does the rule allow/deny the subject to do
  - **Object:** The resource that the subject can/cannot perform the action on
  - **Conditions:** Additional requirements that must be met in the current state of the subject or the resource (e.g., time or location restrictions)
  - **Decision:** Allow or Deny

What are Identity-Driven Attacks?

Authorization Examples

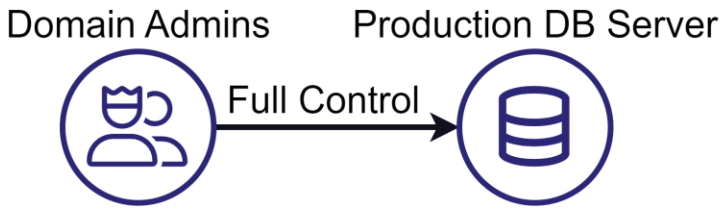
Subject	Action	Object	Conditions	Decision
Domain Admins	Full Control	Production DB Server		Allow

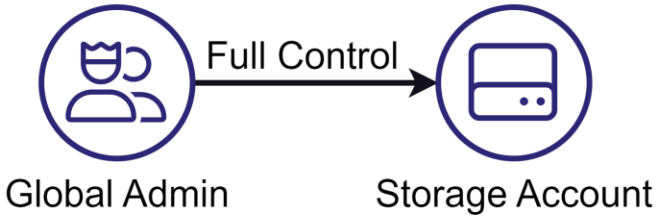


What are Identity-Driven Attacks?

Authorization Examples

Subject	Action	Object	Conditions	Decision
Domain Admins	Full Control	Production DB Server		Allow
Global Admin	Full Control	Storage Account	Compliant Device MFA	Allow

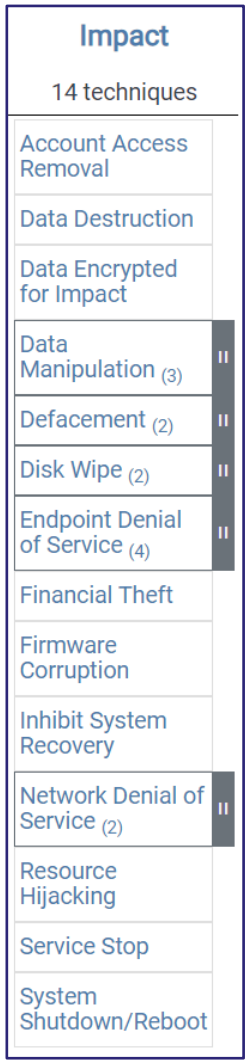




What are Identity-Driven Attacks?

Why Care?

- Attackers ultimately seek to impact the environment or steal data
  - Or demonstrate the ability to do so
- Barring physical destruction, virtually all attack paths require navigating the access control mechanism
  - Credential abuse
  - User impersonation
  - ACL modification
  - Exploitation/manipulation of components with permitted access



What are Identity-Driven Attacks?

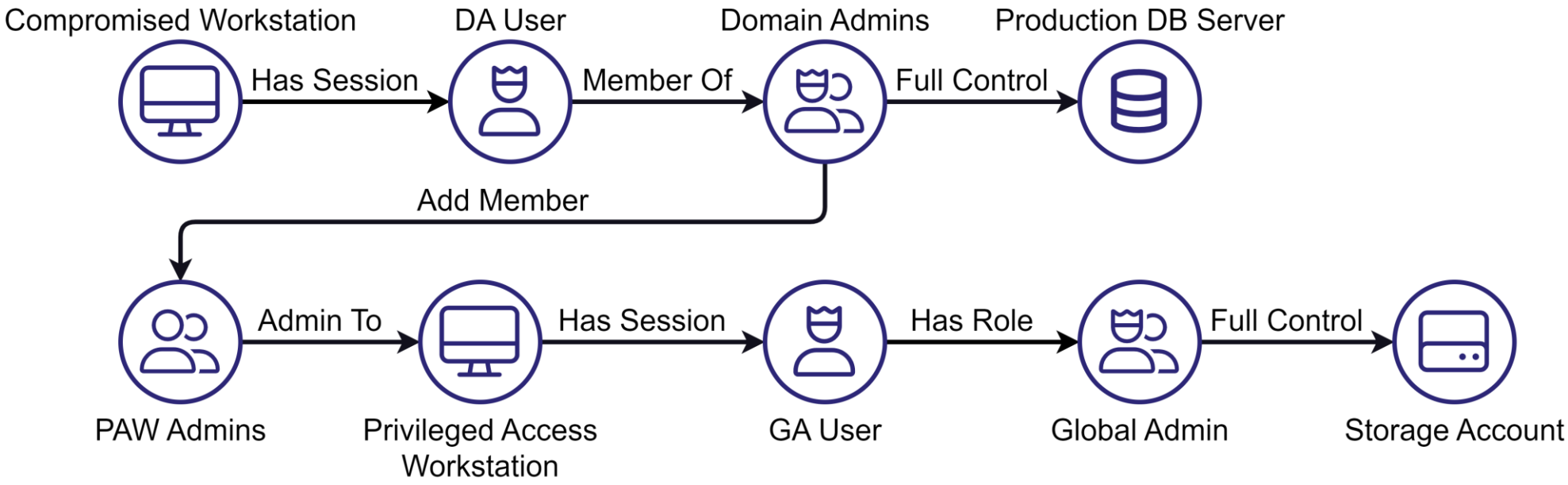
Common Strategy: Enterprise Identity Dominance

- Attackers typically aim to gain dominance of the IdP/IAM system (e.g., gain Domain Admin/Global Admin) and then leverage this access to move laterally to their objectives
- Controlling enterprise identities allows impersonating principals with access to the target resources
- Such privileged access enables rapid lateral movement, allows installing hard-to-find persistence
- At this point, defenders usually have less access than the attackers, turning IR into a more complex and collaborative effort

What are Identity-Driven Attacks?

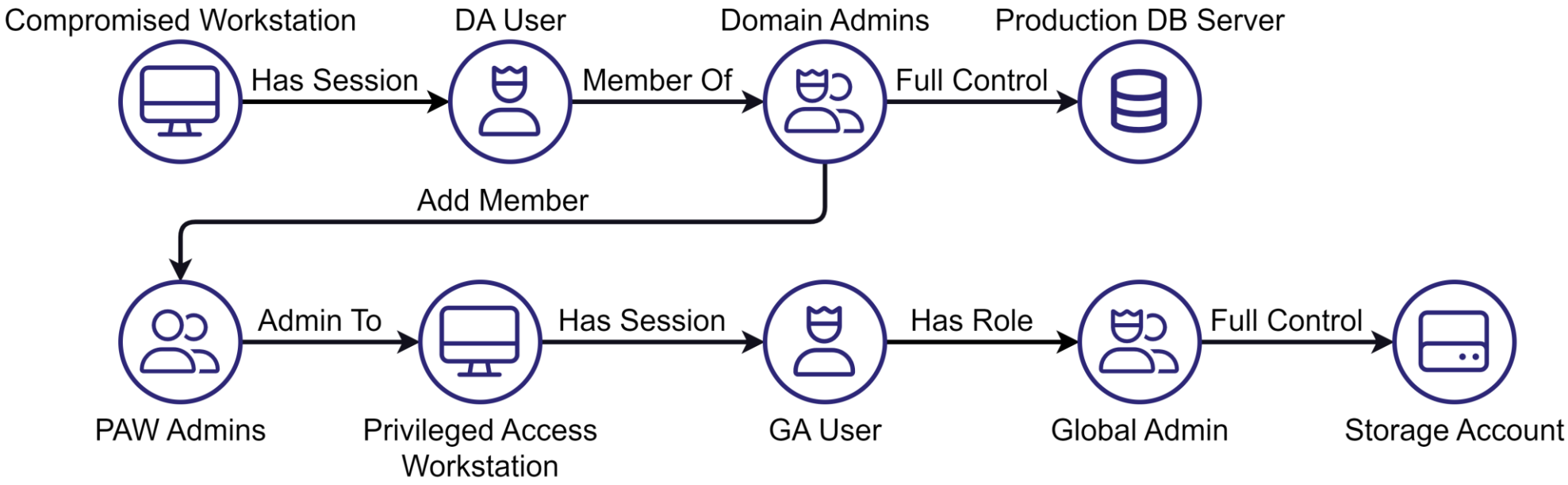
Attack Path Example

Subject	Action	Object	Conditions	Decision
Domain Admins	Full Control	Production DB Server		Allow
Global Admin	Full Control	Storage Account	Compliant Device MFA	Allow



What Makes an Attack Path?

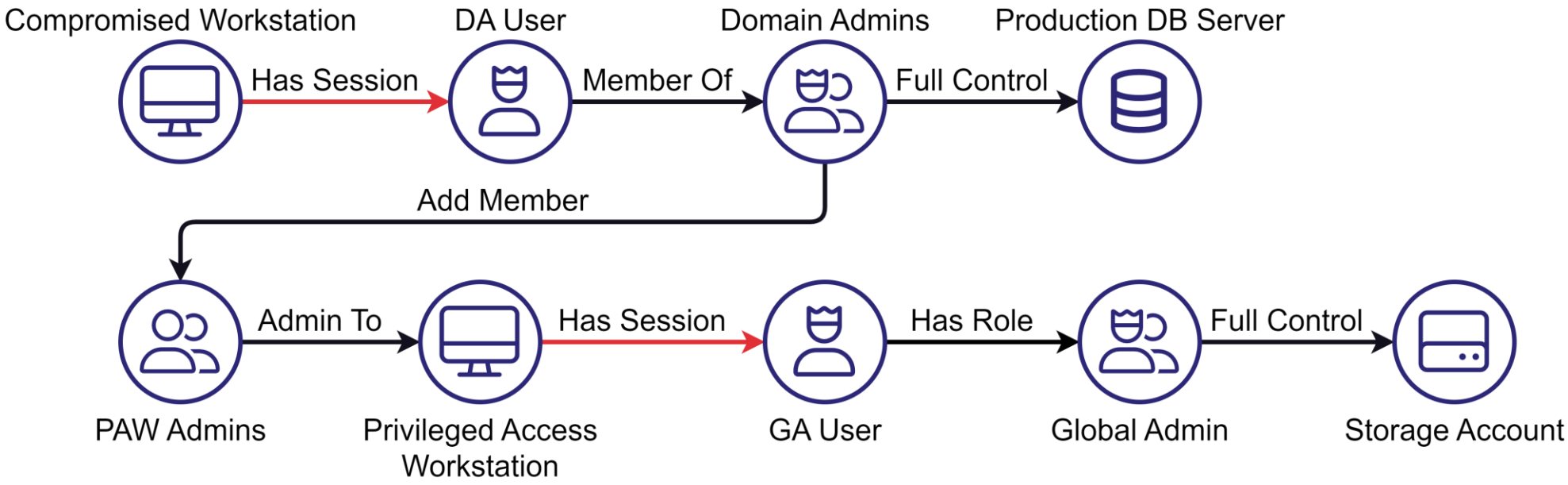
What's Wrong Here?



What Makes an Attack Path?

What's Wrong Here?

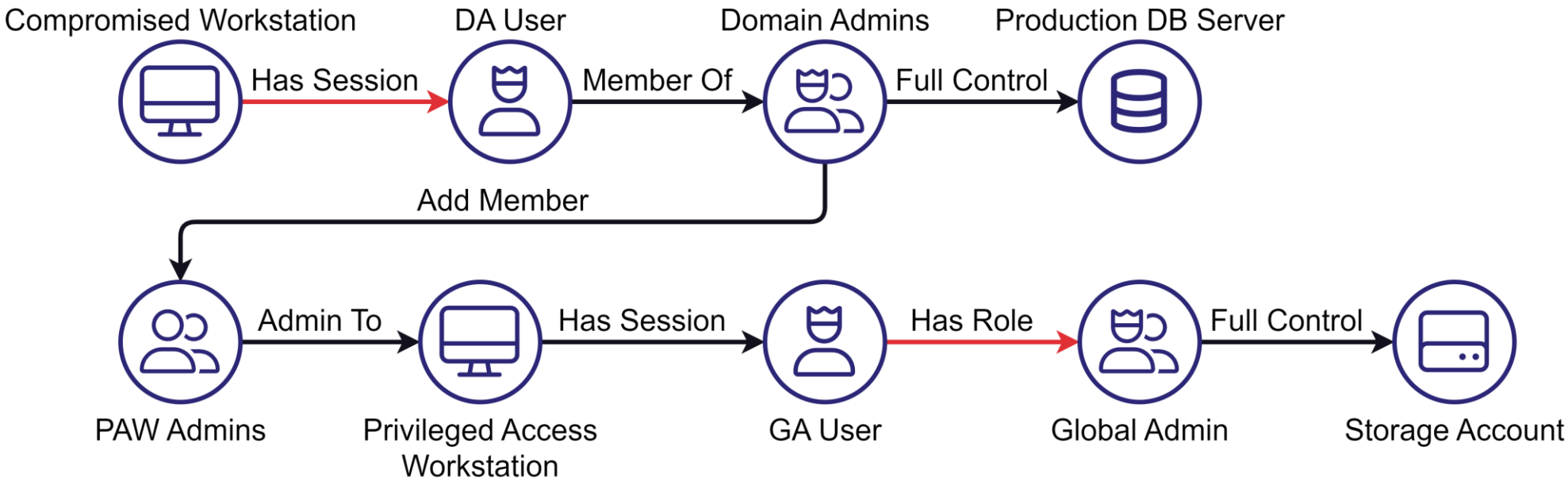
- The DA User shouldn't have a session on a workstation
- The GA User shouldn't have a session on a domain-joined workstation



What Makes an Attack Path?

What's Wrong Here?

- The DA User shouldn't have a session on a workstation
- The GA User shouldn't have a session on a domain-joined workstation
  - Or a hybrid account shouldn't have the GA role



What Makes an Attack Path?

Why is it Wrong?

- Most (arguably, *all*) of the attack paths we discover and abuse violate a less-known security principle called **The Clean Source Principle**

All security dependencies must be as trustworthy as the object being secured

What Makes an Attack Path?

What is a Security Dependency?

All security dependencies must be as trustworthy as the object being secured

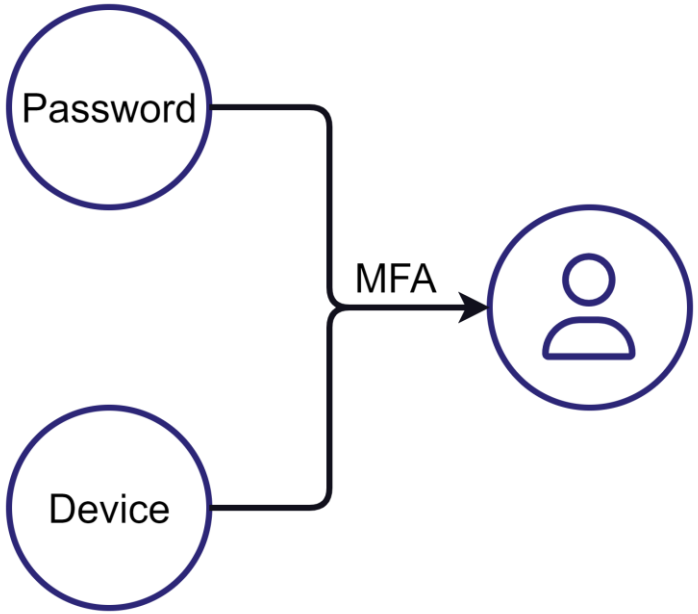
- If the security of one resource relies on the security of another, then it is a security dependency
- Controlling a security dependency **may** allow controlling resources that depend on it
  - Some attacks have multiple prerequisites
  - Controlling a single security dependency may be insufficient for controlling a resource that depends on it

What Makes an Attack Path?

Defining Control

All security dependencies must be as trustworthy as the object being secured

- Control is a relationship that can contribute to compromising the target resource or impacting its operability
- A set of one or multiple security dependencies can control a resource that depends on them

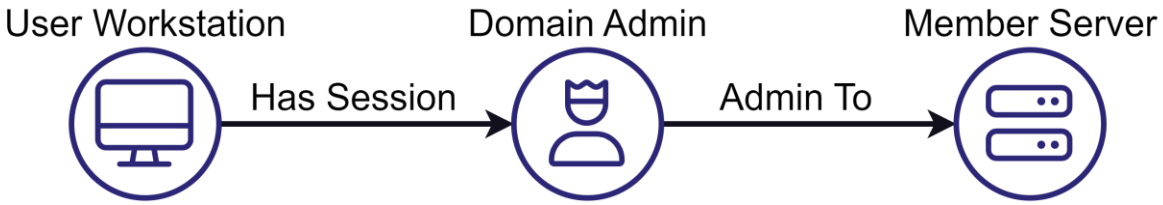


What Makes an Attack Path?

Control Transitivity

All security dependencies must be as trustworthy as the object being secured

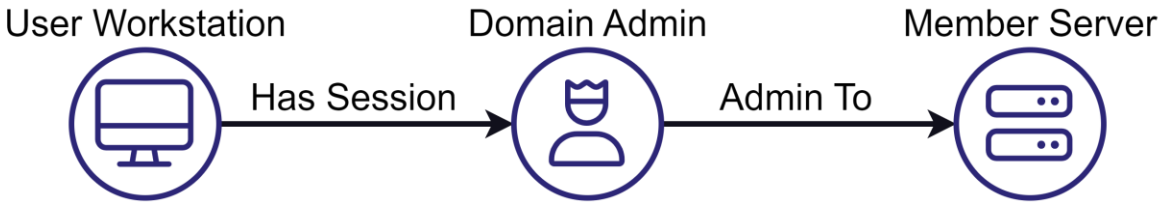
- **Control is transitive**
  - Security dependencies are also transitive
- If A controls B and B controls C, then A controls C



What Makes an Attack Path?

Attack Path Definition

A chain of control relationships with at least one violation of the Clean Source Principle

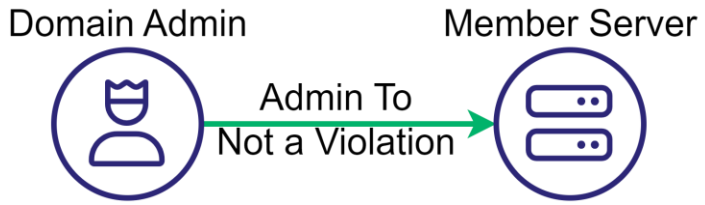


What Makes an Attack Path?

Attack Path Definition

A chain of control relationships with at least one violation of the Clean Source Principle

- It's not an attack path if there's no violation

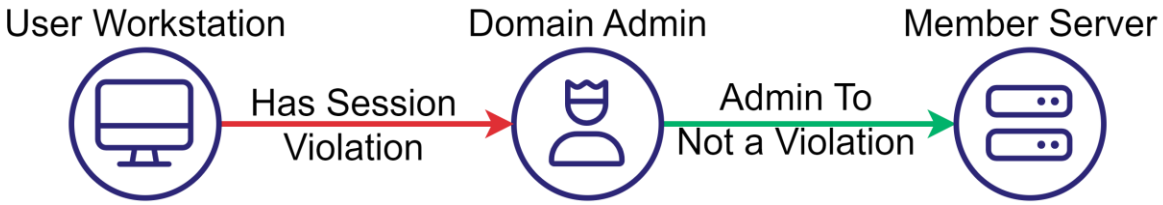


What Makes an Attack Path?

Attack Path Definition

A chain of control relationships with at least one violation of the Clean Source Principle

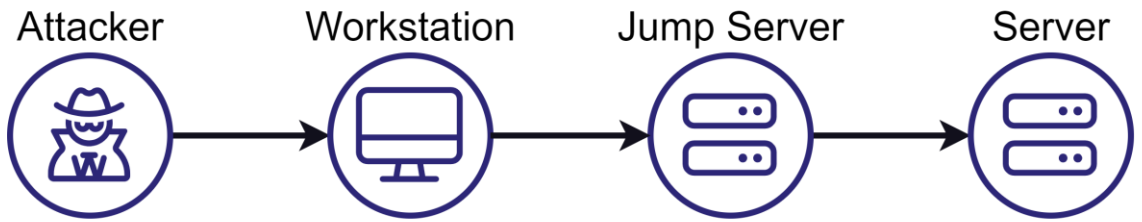
- It's not an attack path if there's no violation



What Makes an Attack Path?

A Very Common Anti-Pattern

A chain of control relationships with at least one violation of the Clean Source Principle

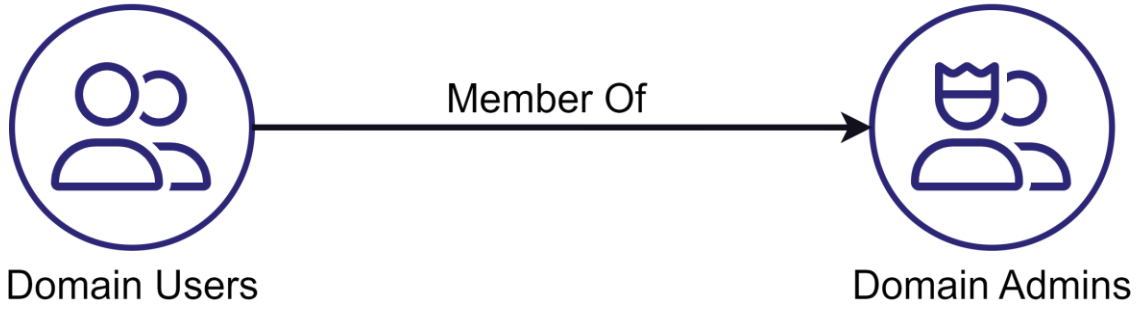


What Makes an Attack Path?

Thought Exercise: Can Domain Users be Domain Admins?

A chain of control relationships with at least one violation of the Clean Source Principle

- Is this a violation of the Clean Source Principle?



What Makes an Attack Path?

Thought Exercise: Can Domain Users be Domain Admins?

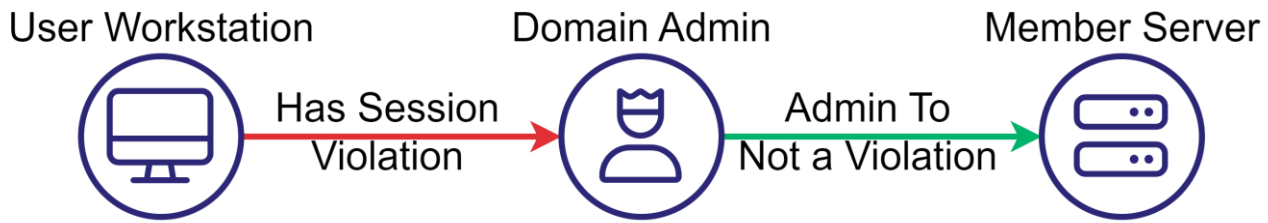
A chain of control relationships with at least one violation of the Clean Source Principle

- Is this a violation of the Clean Source Principle?
- In practice, yes
- In theory, if the organization decides to add Domain Users to the Domain Admins group and the same security controls are enforced on all Domain Users as on Domain Admins, then it is not a Clean Source Principle violation

Rethinking Attack Paths

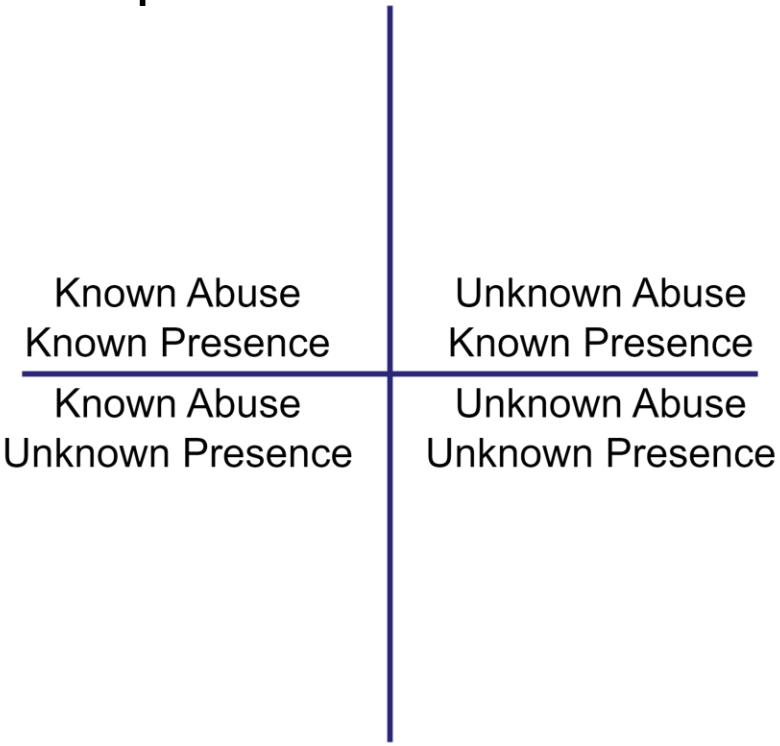
Apply the Definition to Every Attack Path

- Thinking in terms of Security Dependency, Control, Trustworthiness, and Clean Source will ultimately help you discover new attack paths
- Every time you see an attack path, ask the following questions:
  - Does the edge represent control?
  - What are the security dependencies that allow such control?
  - Is the source node as trustworthy as the destination node?
  - Where is the Clean Source violation?



Attack Path Discovery

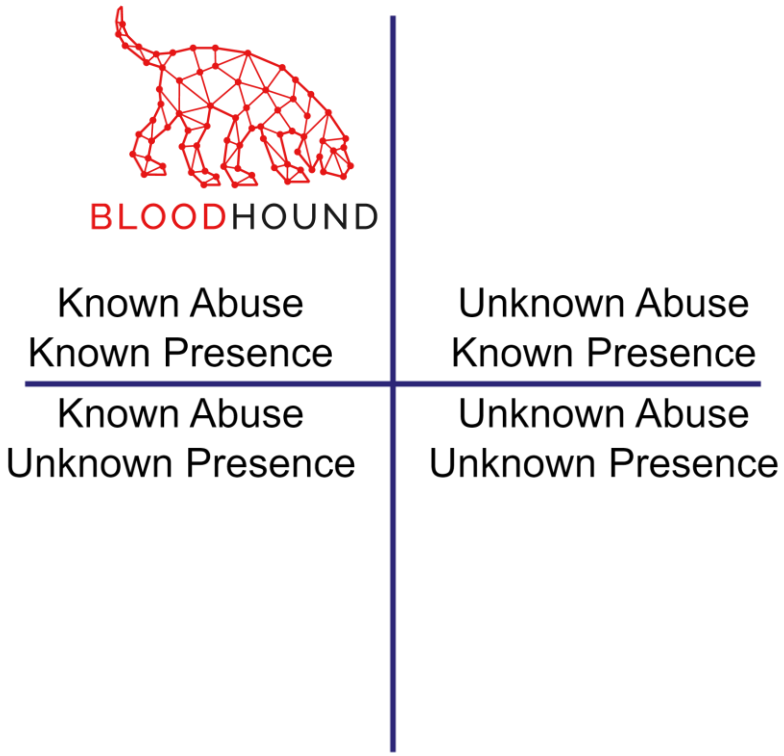
- Methodically discovering new attack paths requires analyzing security dependencies, trustworthiness, and Clean Source Principle violations
- Violations of the Clean Source Principle **may** introduce attack paths
- Criteria:
  - We know how to abuse the violation
    - Abuse = Control the dependent resource
  - We know that it is present in the environment



Attack Path Discovery

Easy Mode

- The top left quadrant is where we want to be
- IdP and IAM mechanisms govern access, so we should use them to identify attack paths
- BloodHound is a great tool for identifying attack paths in Active Directory and Entra ID
- It can find paths that we know how to abuse and we know are present in the environment
- BloodHound does not have full coverage



Attack Path Discovery

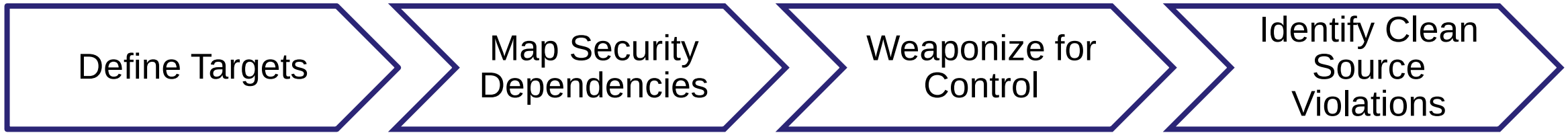
BloodHound Refresher

- BloodHound applies graph theory to the attack path identification problem
  - Principals and resources are represented as nodes
  - Control relationships are represented as edges
  - Pathfinding algorithms identify known attack paths
- The BloodHound GUI allows finding the shortest paths from any selected node to a target
- Inbound control shows the known, abusable security dependencies of the resource
- Outbound control shows the known resources a node can control

Attack Path Discovery

When BloodHound Doesn't Have the Solution

- In mature environments, it is often not as simple as running pathfinding queries in BloodHound
- In such cases, we need to utilize a framework for discovering attack paths



Attack Path Discovery

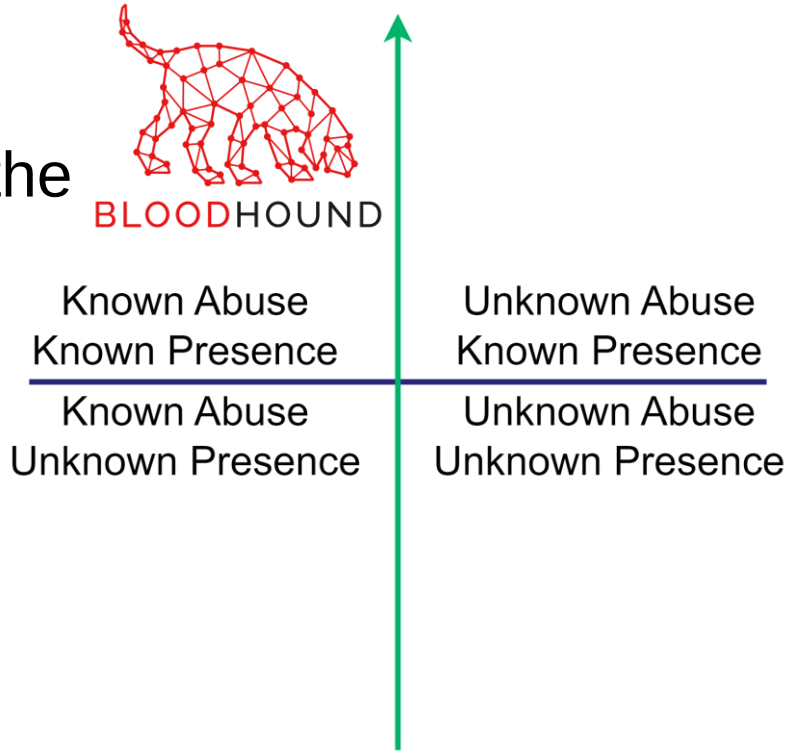
Target Definition

- This approach is objective oriented
  - Not opportunistic or exploratory
- The first step is defining targets based on the red team objectives

Attack Path Discovery

Identifying Security Dependencies: Study the Environment

- Vertical upward transition boils down to **Reconnaissance, Enumeration and Discovery**
  - Moving upward = learning what is present
- Methodically map all the security dependencies of the target resource
- The Discovery column of the MITRE ATT&CK matrix is a good place to start

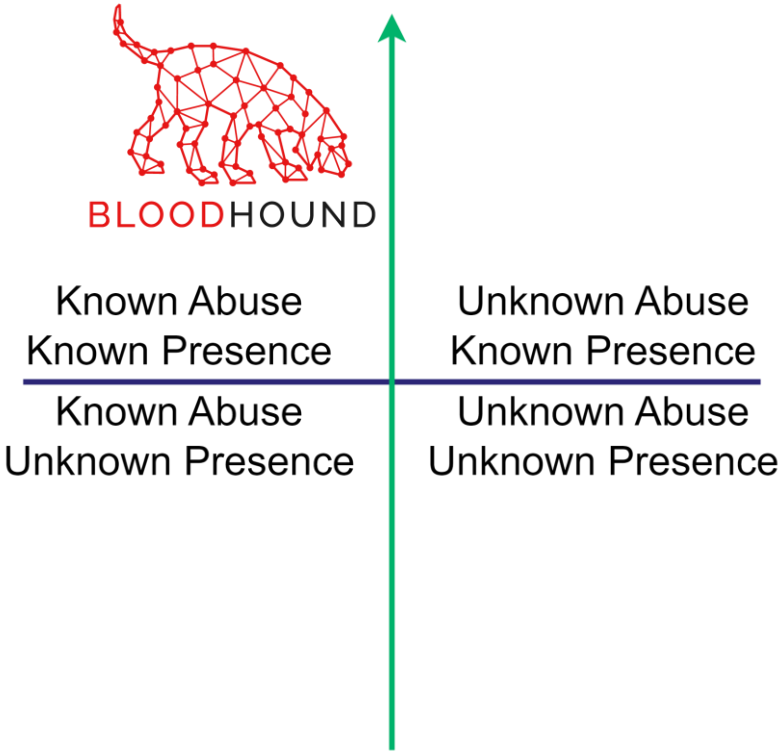


Define Targets → **Map Security Dependencies**

Attack Path Discovery

Identifying Security Dependencies: Study the Environment

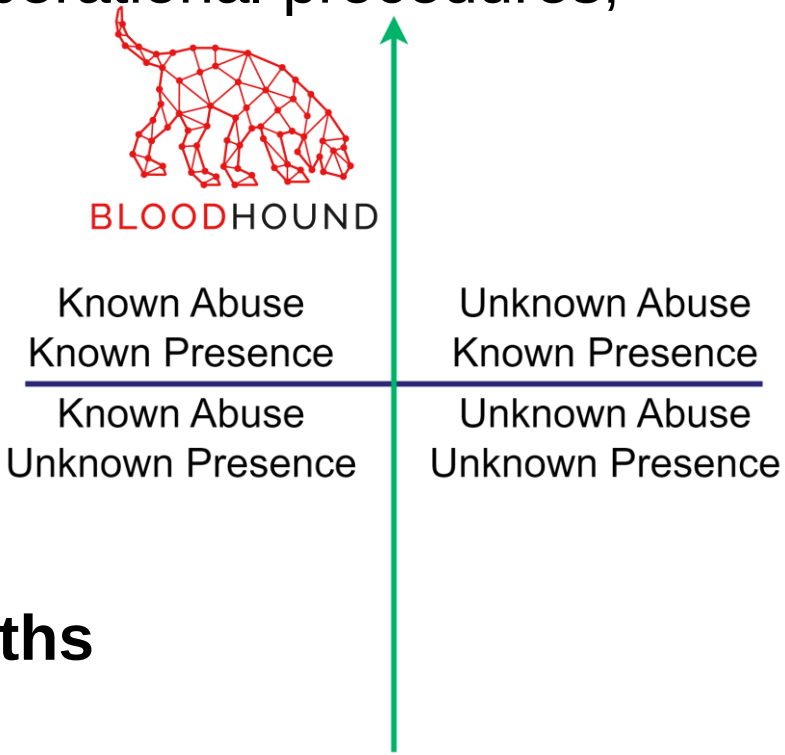
- The bottom left quadrant represents the known tradecraft which may or may not affect the environment
- Various tools can help collect the data required for moving up to the top left quadrant
  - AzureHound
  - SharpHound and its alternatives



Attack Path Discovery

Identifying Security Dependencies: Study the Environment

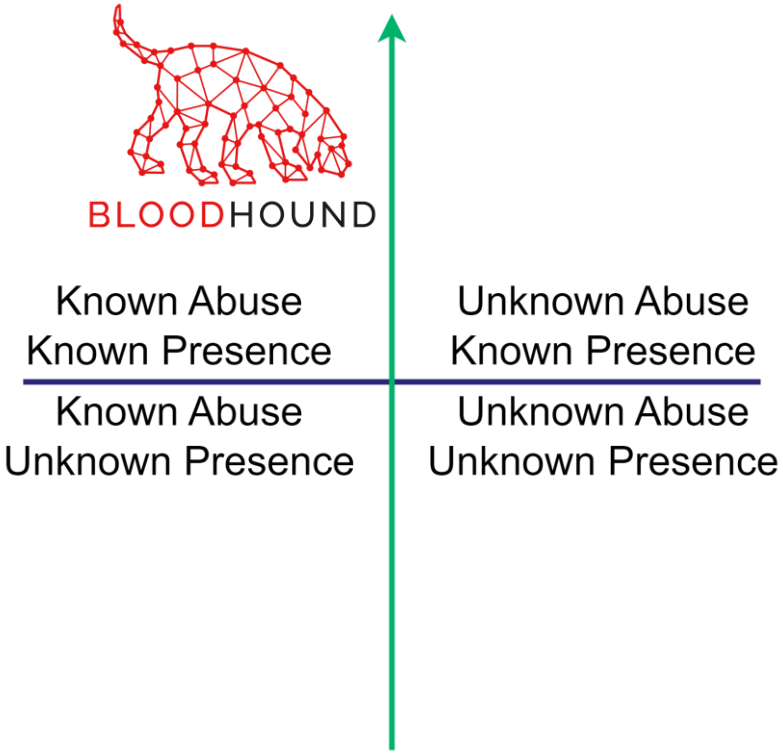
- Explore internal Wikis, Confluence, SharePoint, and all available documentation to learn about technologies used, operational procedures, policies, processes, etc.
  - Proxy browser traffic or use tools such as AtlasReaper
- **Don't target solely off-the-shelf technology**
- **In-house and less common technologies are typically interesting targets**
- **People and processes often introduce viable paths**



Attack Path Discovery

Identifying Security Dependencies: Study the Environment

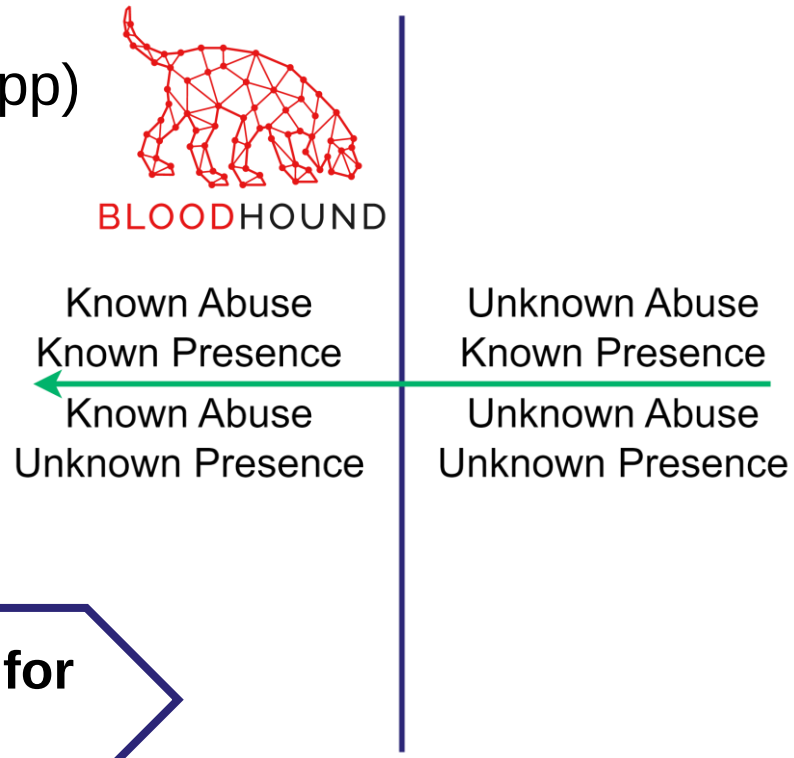
- Relying solely on existing tools and tradecraft leads to missed opportunities
- **The more you know,**
  The more opportunities you have



Attack Path Discovery

From Security Dependencies to Control

- BloodHound has blind spots
  - Some are broad (e.g., analyzing file share access)
  - Some are specific (e.g., access to an internal web app)
- Develop "attack primitives"
- Group/role names, usernames, descriptions, and internal documentation can reveal security dependencies and suggest abuse options

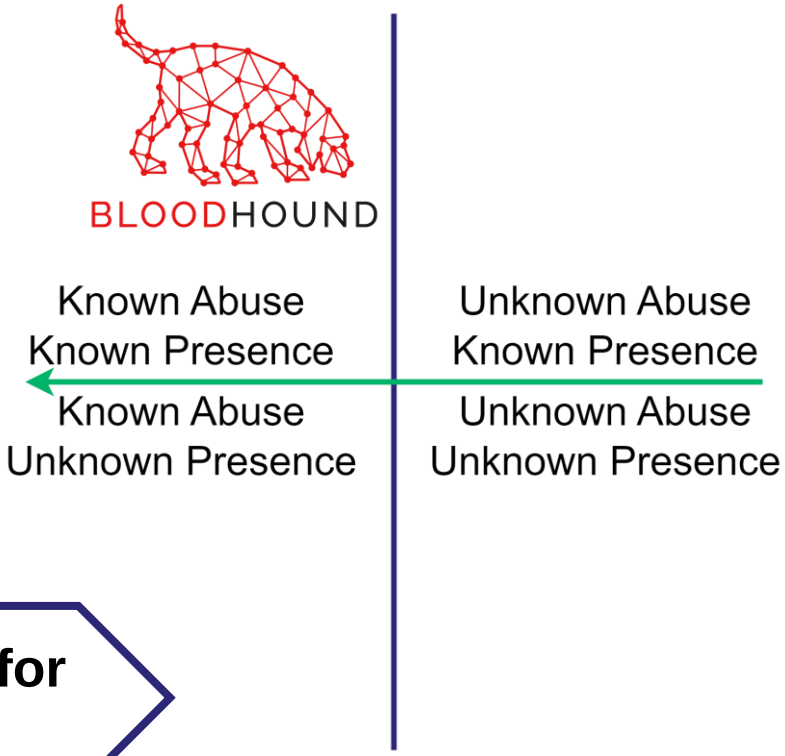


Define Targets → Map Security Dependencies → **Weaponize for Control**

Attack Path Discovery

From Security Dependencies to Control

- You can learn how to weaponize security dependencies in stock technology (bottom right)
  - Security/Vulnerability Research, Bug Bounties
  - Tradecraft Development
  - Training
- You can learn how to abuse patterns in common processes or procedures



Define Targets → Map Security Dependencies → **Weaponize for Control**

ADVERSARY TACTICS

SPECTEROPS

Identity-Driven Offensive Tradecraft

Learn to identify and execute a wide range of elaborate attacks against both on-premises and cloud technologies using identity-based attacks.

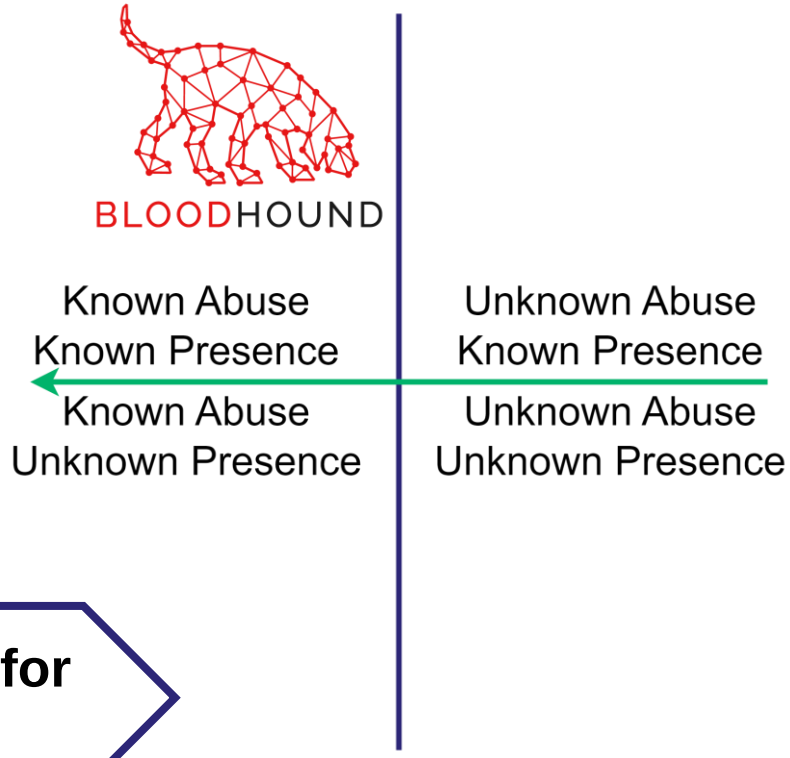
New Course Coming October 2024!

- **Attack Path Discovery:** Learn to identify Clean Source Principle violations and uncover attack paths.
- **Exploit Identity Architectures:** Gain skills to navigate and exploit on-prem and hybrid identity systems for lateral movement and privilege escalation in complex environments.
- **Advanced Authentication and Authorization Attacks:** Develop expertise in intricate authentication and authorization mechanisms to conduct sophisticated attacks and achieve red team objectives.
- **Abuse Legitimate Configuration Management Systems:** Utilize legitimate configuration management solutions and processes to execute adversary tactics with precision and effectiveness.
- **Hands-on Labs:** Practice skills in a specially designed lab environment that simulates a real-world client environment incorporating a variety of technologies and Attack Paths, including cross-tenant and supply chain attacks.
- **Red vs. Blue Insight:** Learn defenders' perspective and detection logic, as well as OPSEC considerations to counter the detections and keep hacking.

Attack Path Discovery

From Security Dependencies to Control

- You can learn how to weaponize technology and processes in specific environments (top right)
  - Red Teaming
  - Penetration Testing
  - Security Assessments

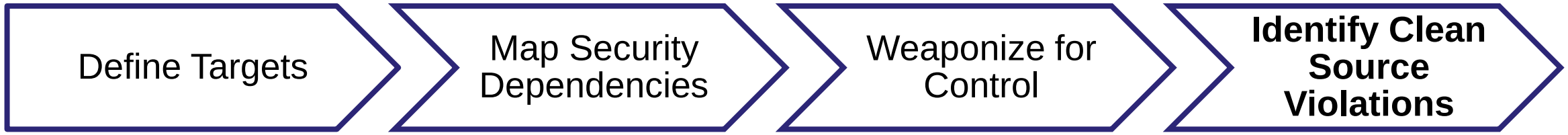


Define Targets → Map Security Dependencies → **Weaponize for Control**

Attack Path Discovery

Identify Clean Source Violations

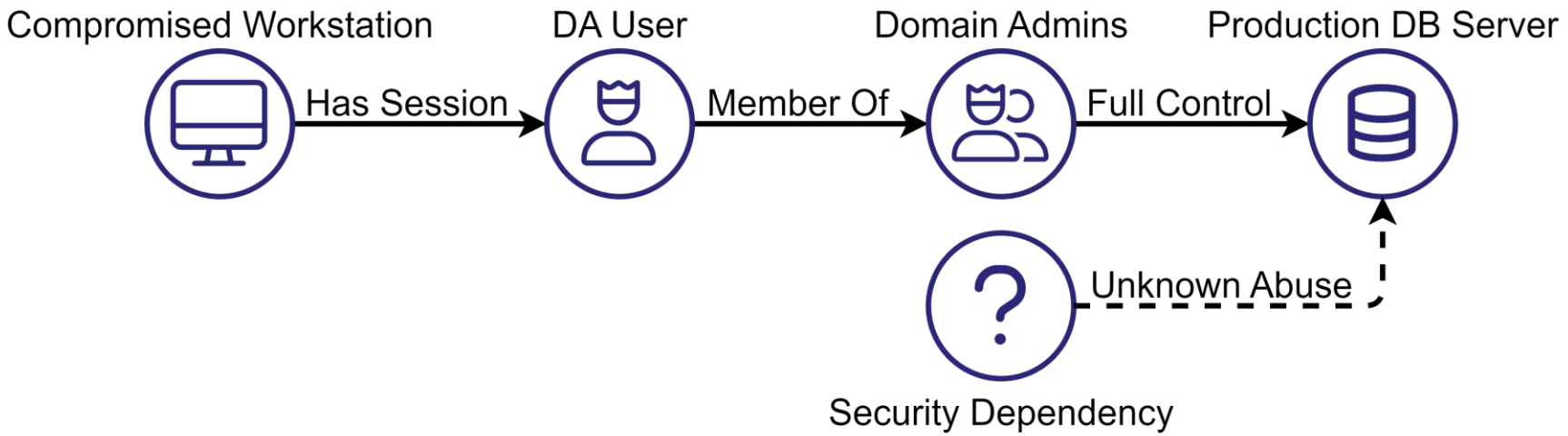
- All systems have security dependencies, but **only Clean Source violations introduce attack paths**
- With the target in mind, explicitly map all the identified security dependencies



Attack Path Discovery

Identify Clean Source Violations

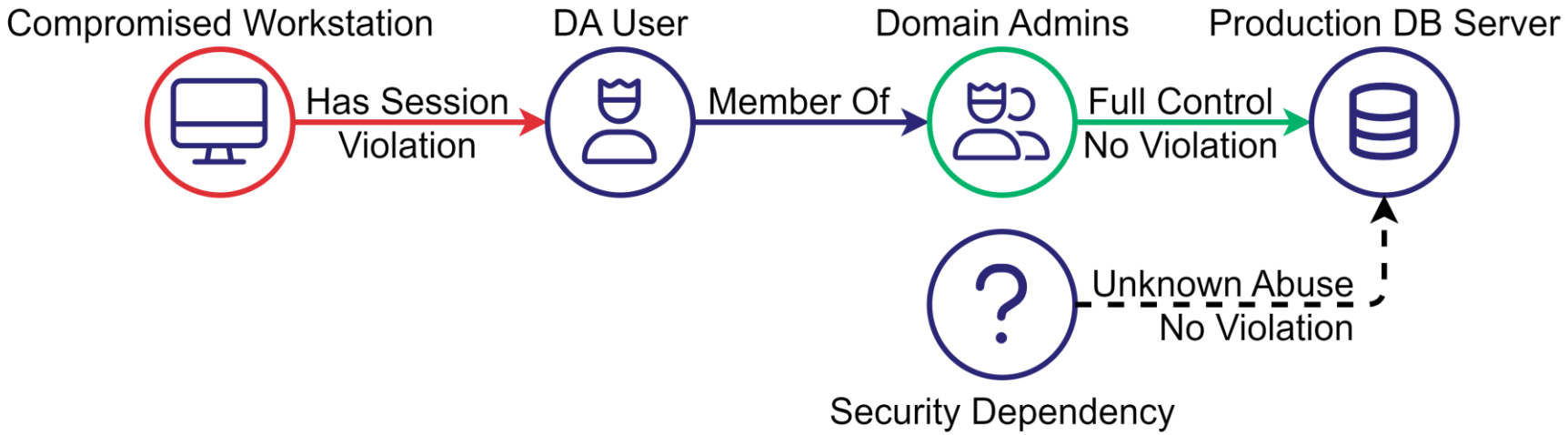
- Use the BloodHound convention for principals/resources (security dependencies) as nodes and control relationships as edges
- Use different annotations to distinguish between edges you know how to abuse and edges you don't, e.g., dashed vs. solid



Attack Path Discovery

Identify Clean Source Violations

- Rate the trustworthiness of every security dependency in relation to the target resource
  - Use only three ratings: More, Less, Same
- Only dependencies with a known abuse, originating from less trustworthy to more trustworthy or the same make an attack path



Conclusion

- All attack paths are identity-driven
- Every attack path abuses at least one clean source principle violation
- Explicitly mapping security dependencies and their trustworthiness helps discover known and unknown attack paths
  - Applies to people, processes, and technology
- The more proficient you are in identity-driven offensive tradecraft, the more attack paths you can discover and abuse

Conclusion

- All attack paths are identity-driven
- Every attack path abuses at least one clean source principle violation
- Explicitly mapping security dependencies and their trustworthiness helps discover known and unknown attack paths
  - Applies to people, processes, and technology
- **The more proficient you are in identity-driven offensive tradecraft, the more attack paths you can discover and abuse**


SPECTER BASH
OCTOBER 7 - 10, 2024
9:00am – 5:00pm Central Time
The Inverness Denver (Hilton)
200 Inverness Drive West • Englewood, Colorado 80112
COURSES:
Red Team Operations
Detection
Identity-Driven Offensive Tradecraft
Tradecraft Analysis
Azure Security Fundamentals
EXCLUSIVE IN-PERSON SWAG
CUTTING EDGE INSIGHTS
LEARN COMPREHENSIVE SKILLS IN HANDS-ON LABS
EVENTS WITH INDUSTRY PEERS
SPECTEROPS.IO/SPECTER-BASH
SPECTEROPS

CONFERENCE:
MARCH 31 – APRIL 1, 2025

TRAINING:
APRIL 2 – 5, 2025

TAKE ADVANTAGE OF SPECIAL EARLY BIRD PRICING NOW

- **Location: Convene** – 1201 Wilson Boulevard, Arlington, Virginia 22209
- **Call for Papers opening October 1, 2024**
- **FREE conference pass with paid training ticket**
- **Courses:** Red Team Operations, Identity-Driven Offensive Tradecraft, Tradecraft Analysis and Azure Security Fundamentals

SPECTEROPS.IO/SO-CON

Questions?

Thank You!