# UBA + Deception + EDR

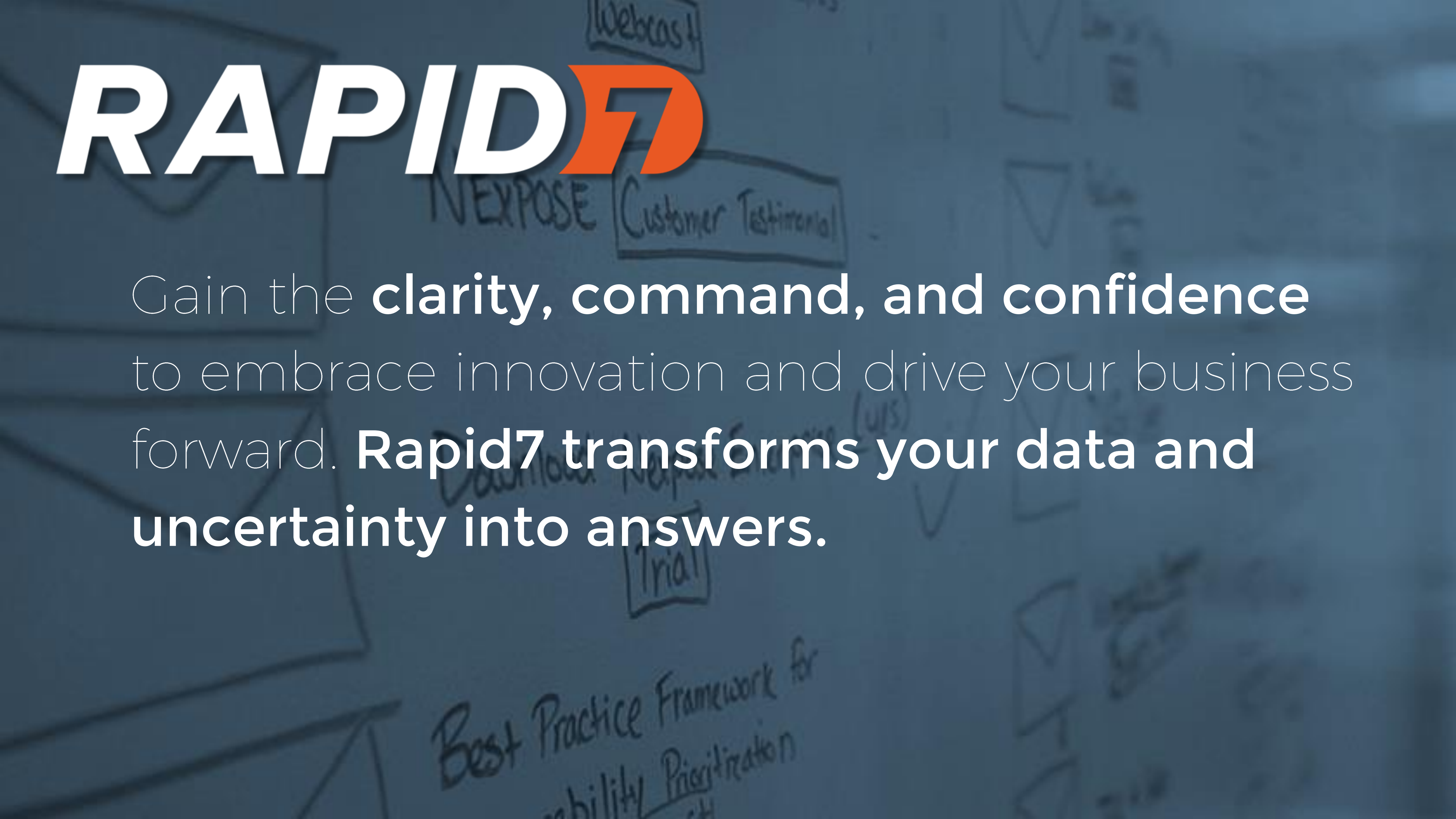
## Going Beyond Alerts To Uncover Answers with InsightIDR

Eric Sun, Solutions Mgr,

Incident Detection & Response

@exalted

RAPID7



RAPID7

Gain the **clarity, command, and confidence** to embrace innovation and drive your business forward. **Rapid7 transforms your data and uncertainty into answers.**

# We can help you with...

Vulnerability Management

SIEM

Application Security

IT Operations

User Behavior Analytics

Penetration Testing

Managed Services

Security Advisory Services

# UBA + Deception + EDR

## Going Beyond Alerts To Uncover Answers with InsightIDR

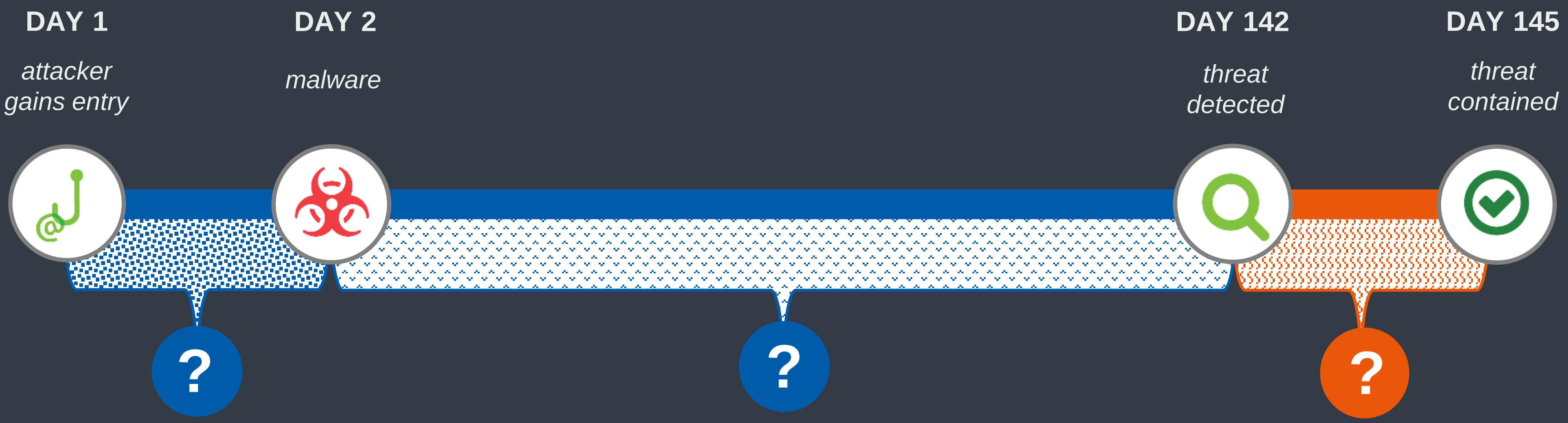
Eric Sun, Solutions Mgr,

Incident Detection & Response

@exalted

RAPID7

# Closing The Gap…



**DAY 1**

*attacker gains entry*

**DAY 2**

*malware*

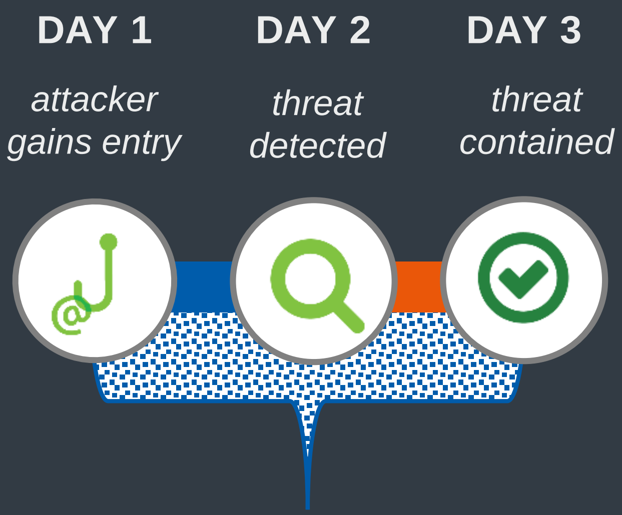
**DAY 142**

*threat detected*

**DAY 145**

*threat contained*

# Closing The Gap...



**DAY 1**

*attacker gains entry*

**DAY 2**

*threat detected*

**DAY 3**

*threat contained*

# IDR: Top Security Team Challenges

## Alert Fatigue

- Too many of the wrong alerts, not enough context

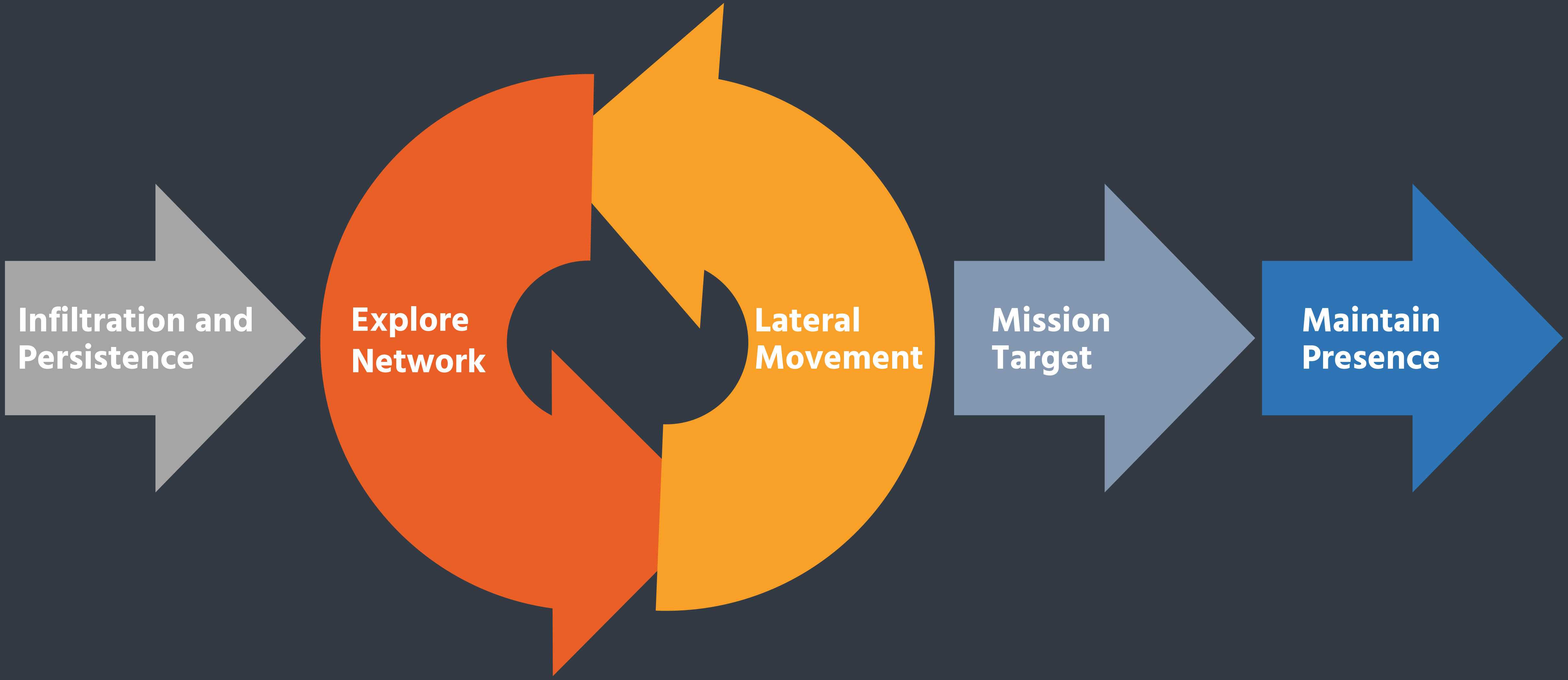
## Incident Investigations

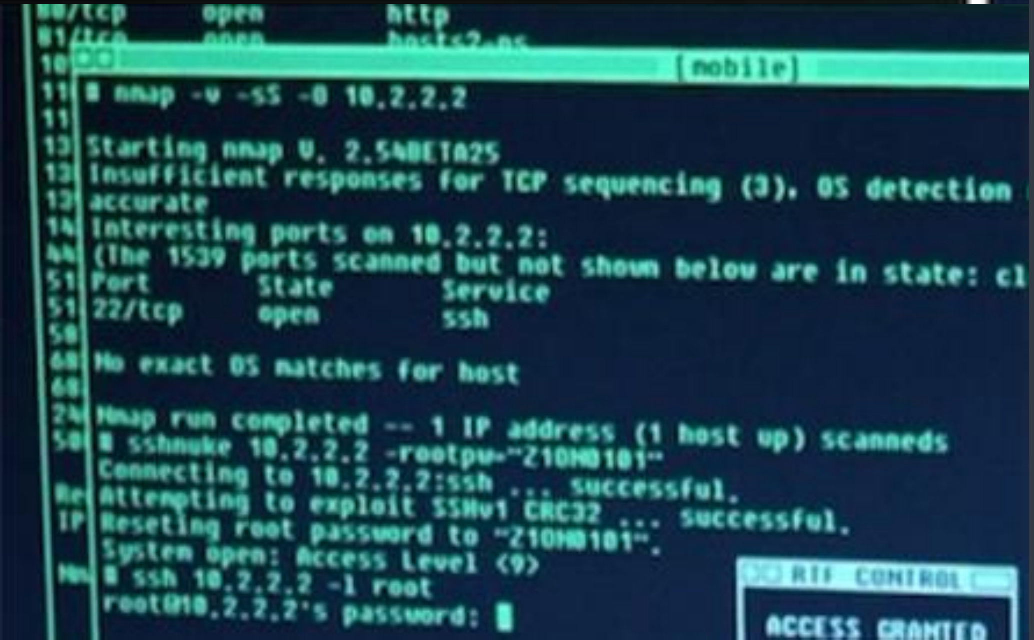
- Lots of tedious actions, where to prioritize?

## Portal Fatigue

- Jumping between solutions to monitor network

# Steps in an Internal Attack Chain



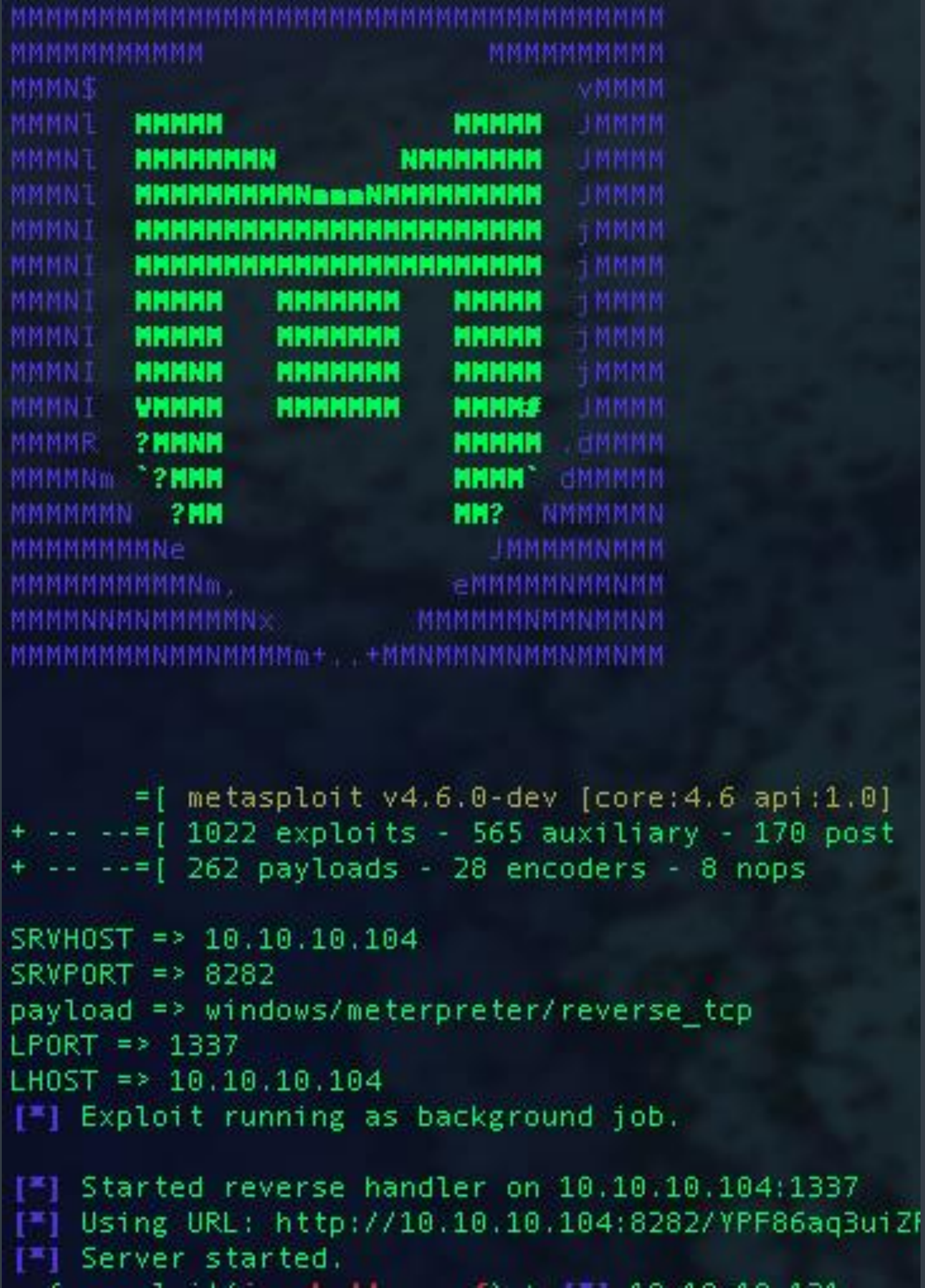


```
80/tcp      open        http
81/tcp      open        hosts2-ns
# nmap -v -sS -O 10.2.2.2

Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: cl
Port        State       Service
22/tcp      open        ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanneds
# sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z1ON0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password: █
```

# Network Scans

- Once attacker is in, needs to learn more about network
- Other machines, ports, vulnerabilities?
- Network scanning tool, e.g. Nmap
- Very difficult to identify by log/network file analysis alone

# Demo:
# Deception Tech in IDR

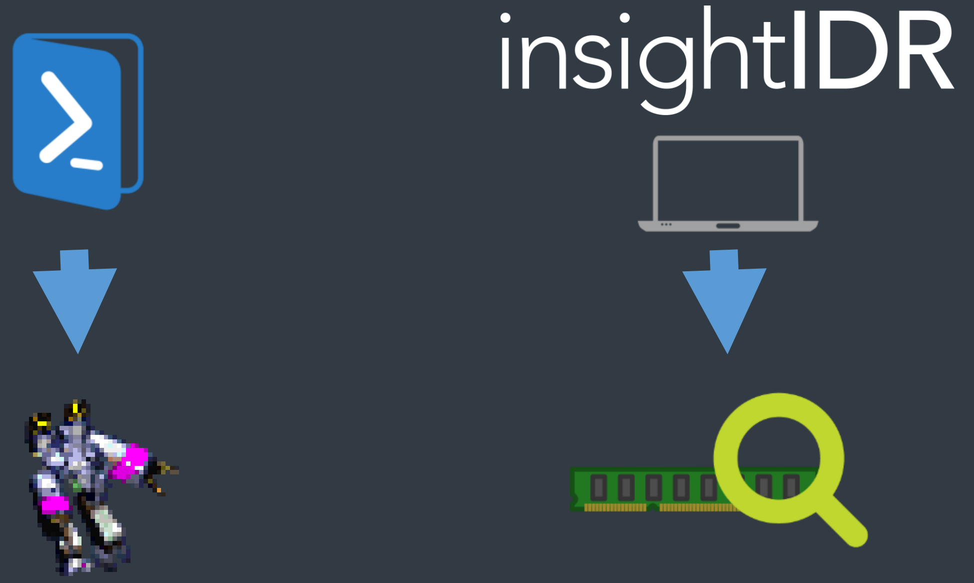


```
      =[ metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --=[ 1022 exploits - 565 auxiliary - 170 post
+ -- --=[ 262 payloads - 28 encoders - 8 nops

SRVHOST => 10.10.10.104
SRVPORT => 8282
payload => windows/meterpreter/reverse_tcp
LPORT => 1337
LHOST => 10.10.10.104
[*] Exploit running as background job.

[*] Started reverse handler on 10.10.10.104:1337
[*] Using URL: http://10.10.10.104:8282/YPF86aq3uiZ
[*] Server started.
```

# Remote File Execution

- Attackers exploit machines using built-in tools (e.g. PSExec, PowerShell)
- Detection requires endpoint visibility

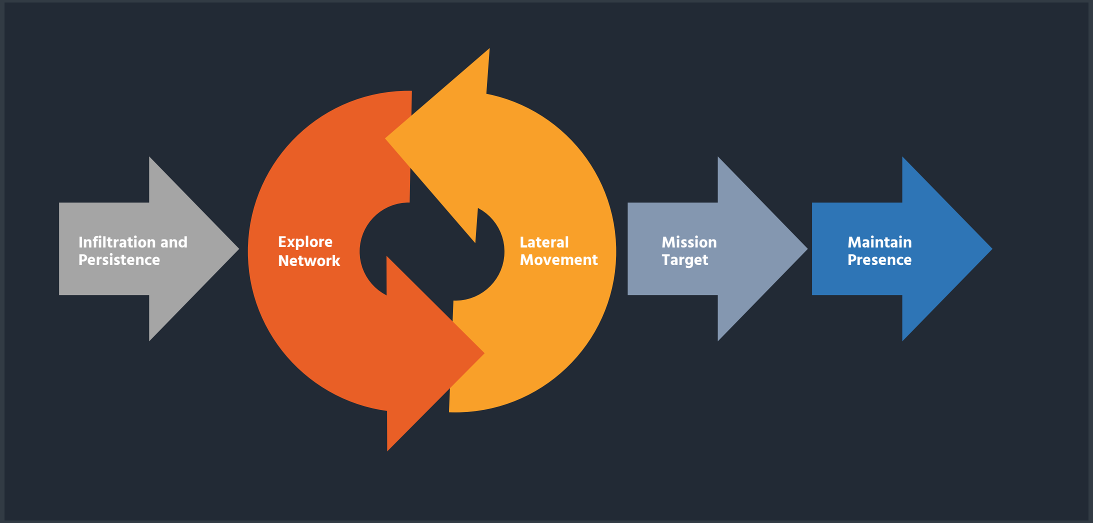
# Demo



# The Foundation for Reliable Detection

1. Good detection requires good data collection!
2. Attacker Recon: Deception Tech
3. Remote File Execution: EDR
4. Lateral Movement: UBA
5. One alert ≠ the full story. Context is everything!

THE ATTACK CHAIN

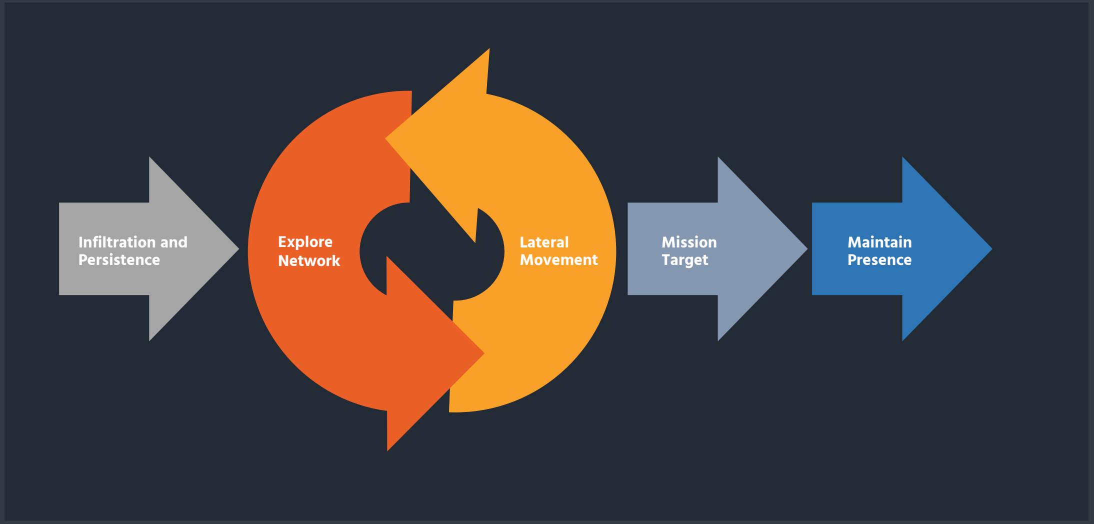


# The Foundation for Reliable Detection

## insightIDR

- User Behavior Analytics
- Deception Tech
- Endpoint Detection

THE ATTACK CHAIN



RAPID7

# Learn More about InsightIDR at our Demo Stations!

www.rapid7.com/solutions/incident-detection

@rapid7