MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THE PARADIGM OF CORPORATE DOMAIN SECURITY IS BROKEN

Clayton Fields

Vice President, Javelin Networks

Non-Domain Computer

Domain Computer

APT
FULL CONTROL ON THE SERVER/PC
ROUTERS / SW / CONTROLLERS
WHY?
NONE DOMAIN
PC
SERVER
MOVE FORWARD?
NO
YES
STOP
DEAD END
HOW?
STEAL CREDS
OTHER
STEAL LOCALLY STORED
STEAL REMOTE STORED CREDS
DOMAIN
PC
SERVER
MOVE FORWARD?
NO
YES
STOP
DEAD END
HOW?
OTHER
STEAL CREDS
PASSWORDS, TICKETS DUMPING, HASH
STEAL
LLMNR MITM OR SILVER TICKET
CONTINUE THE ATTACK
DONE
OR
NO
PRIMARY OBJECTIVE: BYPASS ENDPOINT PROTECTION, INFILTRATE NETWORK, ENCRYPT TARGETS, AND ASK FOR RANSOM
SECONDARY OBJECTIVE: STEAL DATA SABOTAGE ORGANIZATION CONTROL CLOUD/SAAS APPLICATIONS
$
CONTINUE THE ATTACK
YES

DOMAIN SECURITY IS DIFFERENT

01

Active Directory exposes critical topology data and attributes to every endpoint

02

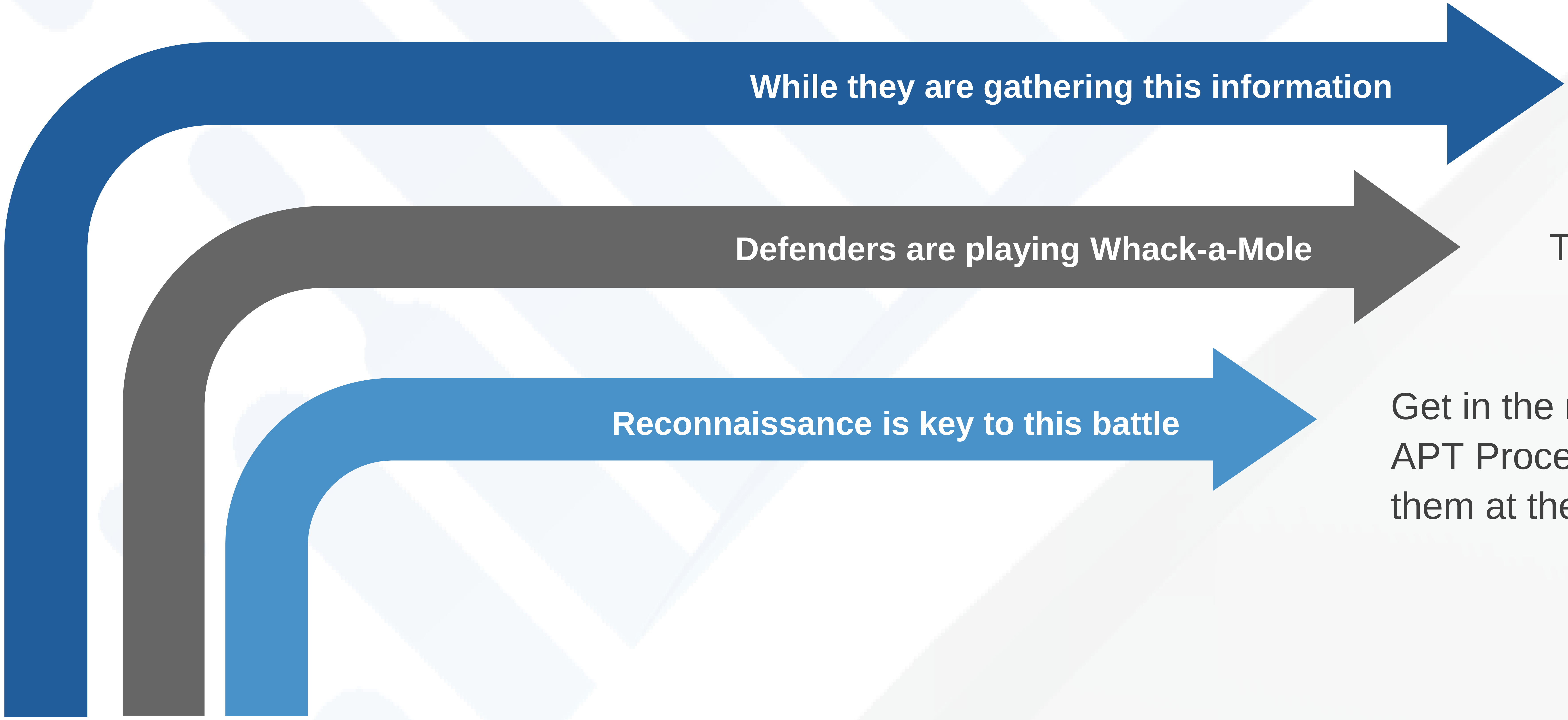
Persistent threats need this data to formulate their campaign

03

Active Directory enables lateral movement without Zero-Day vulnerabilities

DEFENDERS MUST PROTECT 100% OF ENDPOINTS

Attackers only need 1 endpoint connected to a Domain environment



While they are gathering this information

THEY ARE WINNING

Defenders are playing Whack-a-Mole

THEY ARE LOSING

Reconnaissance is key to this battle

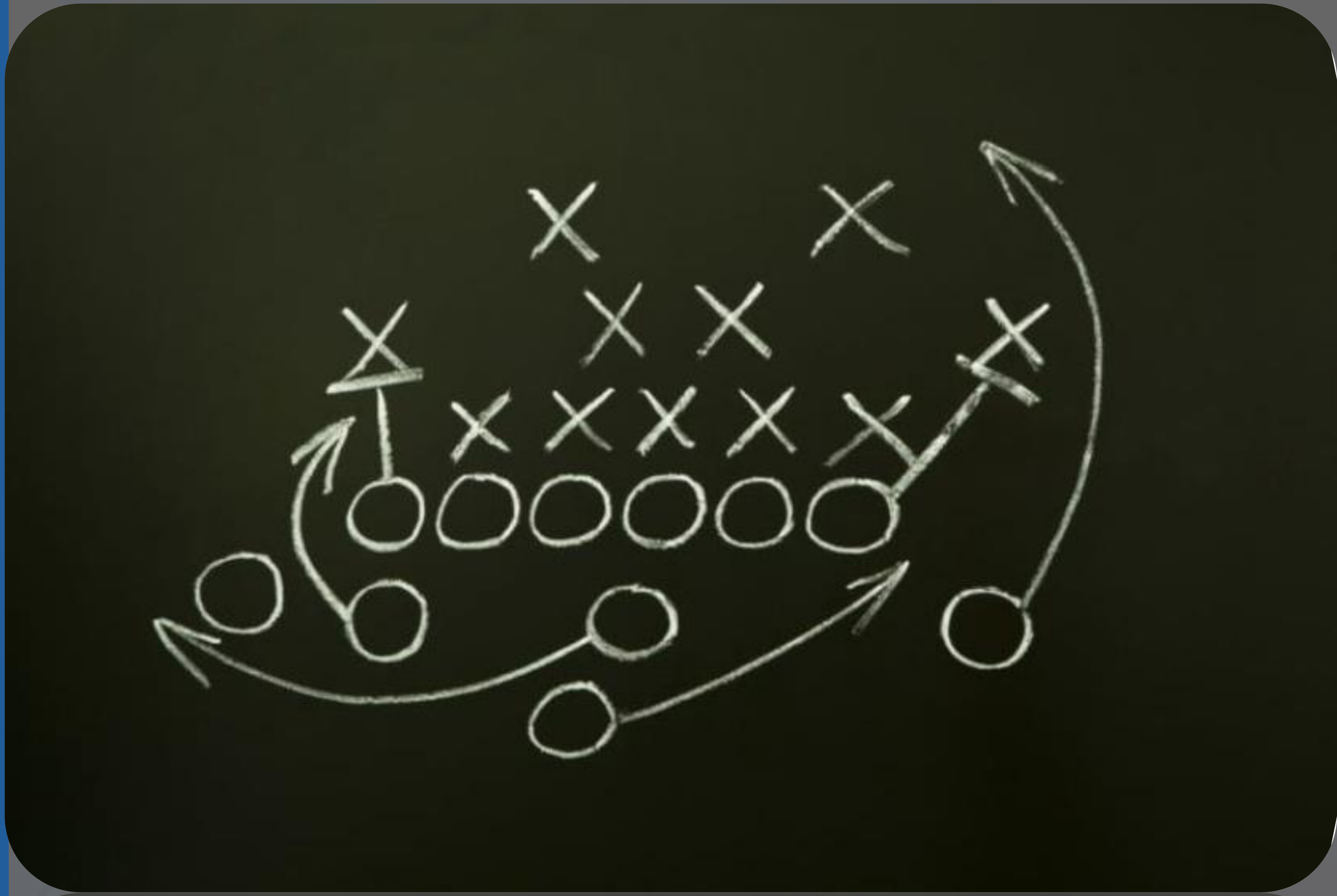
Get in the middle of the APT Process and beat them at their own game

CYBER RESILIENCE

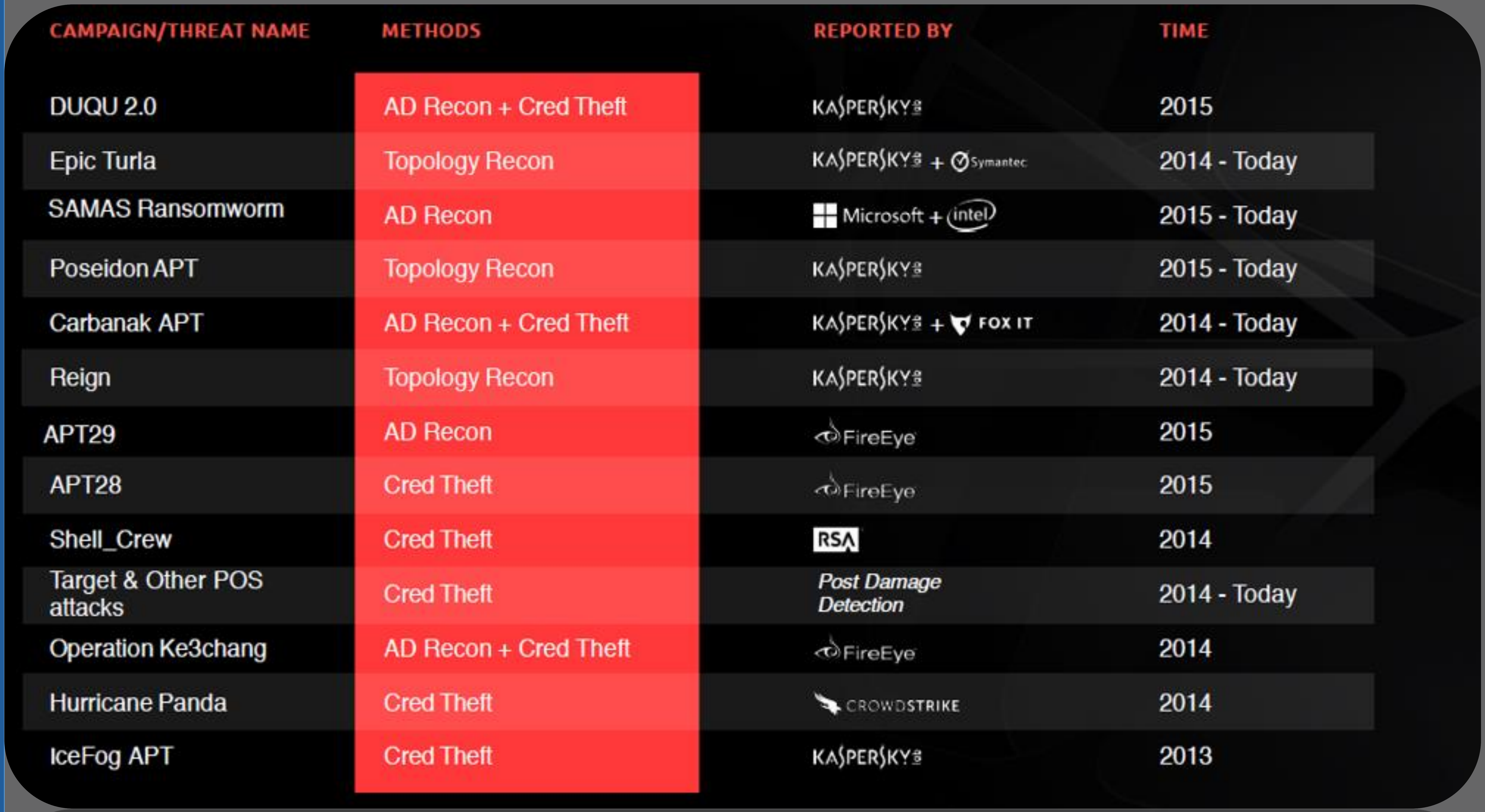
Focusing on middle of attack process

Yields Faster:

- Discovery of Gaps
- Remediation of Holes
- Mitigation of the “unknown/0day/etc”
- Containment!



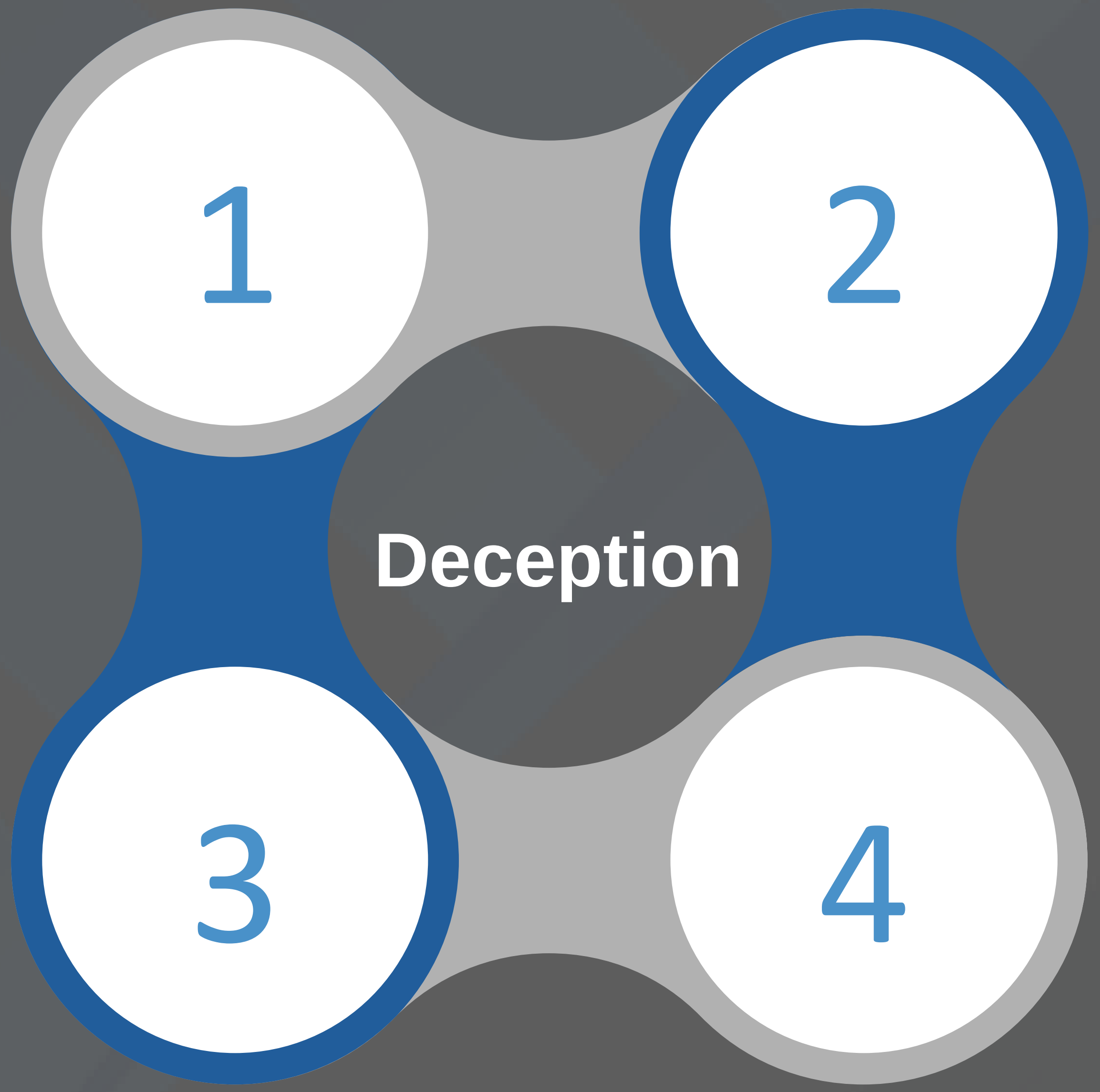
ATTACKERS KNOW: 90% OF NETWORKS RUN MICROSOFT ACTIVE DIRECTORY



CAMPAIGN/THREAT NAME	METHODS	REPORTED BY	TIME
DUQU 2.0	AD Recon + Cred Theft	KASPERSKY	2015
Epic Turla	Topology Recon	KASPERSKY + Symantec	2014 - Today
SAMAS Ransomworm	AD Recon	Microsoft + intel	2015 - Today
Poseidon APT	Topology Recon	KASPERSKY	2015 - Today
Carbanak APT	AD Recon + Cred Theft	KASPERSKY + FOX IT	2014 - Today
Reign	Topology Recon	KASPERSKY	2014 - Today
APT29	AD Recon	FireEye	2015
APT28	Cred Theft	FireEye	2015
Shell_Crew	Cred Theft	RSA	2014
Target & Other POS attacks	Cred Theft	*Post Damage Detection*	2014 - Today
Operation Ke3chang	AD Recon + Cred Theft	FireEye	2014
Hurricane Panda	Cred Theft	CROWDSTRIKE	2014
IceFog APT	Cred Theft	KASPERSKY	2013

CONSIDER: APPLY MILITARY TACTICS TO DEFEND AND CONTAIN

Counterintelligence is a military tactic founded on the Art of War skill Deception



Is not a product, but a tactic

Needs to be authentic, scalable

Needs to be at attacker finger tips all the time, every time

Should result in containment, not a playground.

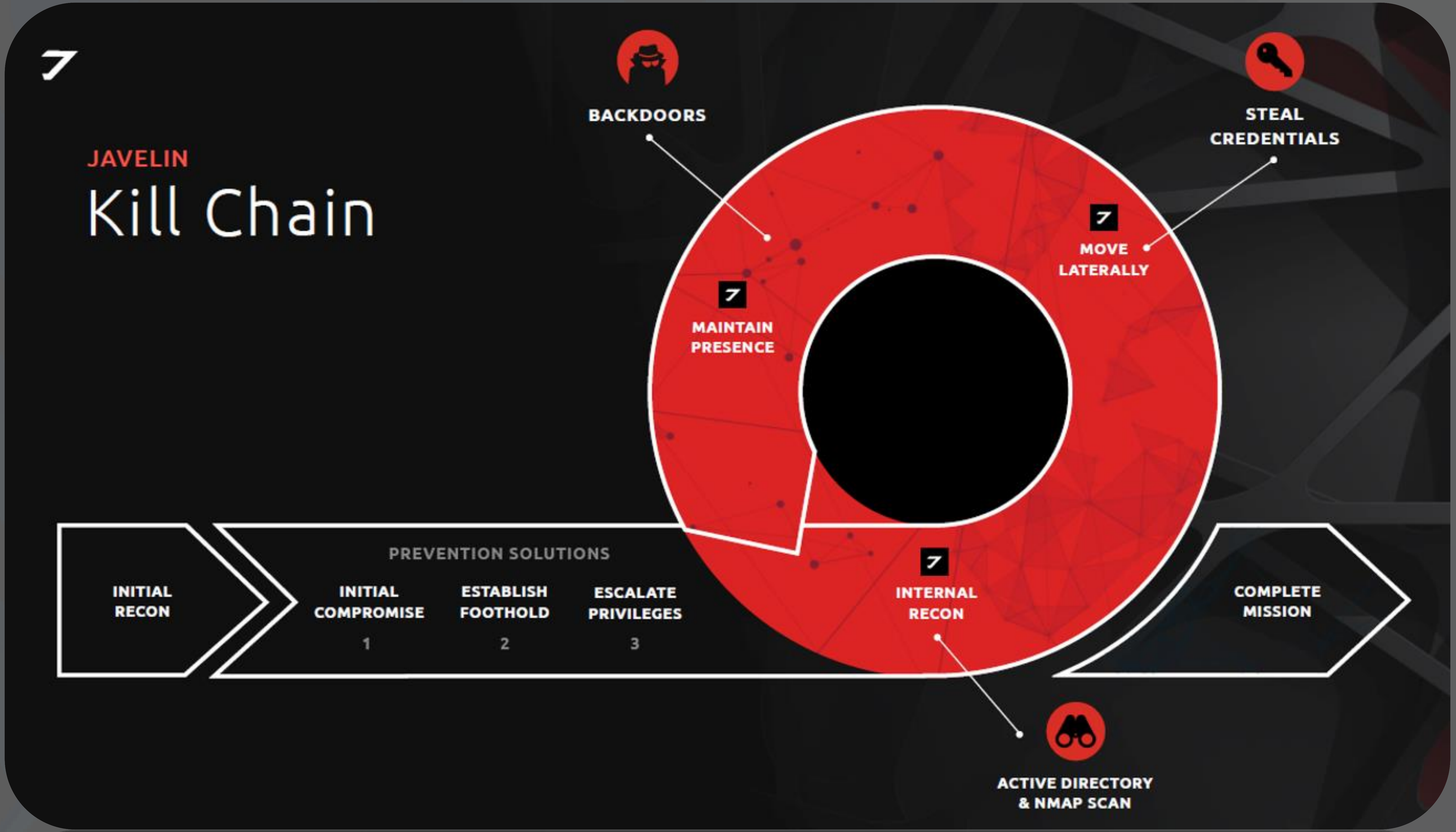
If one cannot contain, or mitigate immediately; the fight is lost in 30 minutes….

InfoSecWorld Conference & Expo 2018

RED TEAM STYLE

It only takes 30 minutes to own Domain Adminstrator

- Are you ready?
- Set
- GO!
- Secure your AD.



MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Clayton Fields
Vice President, Javelin Networks