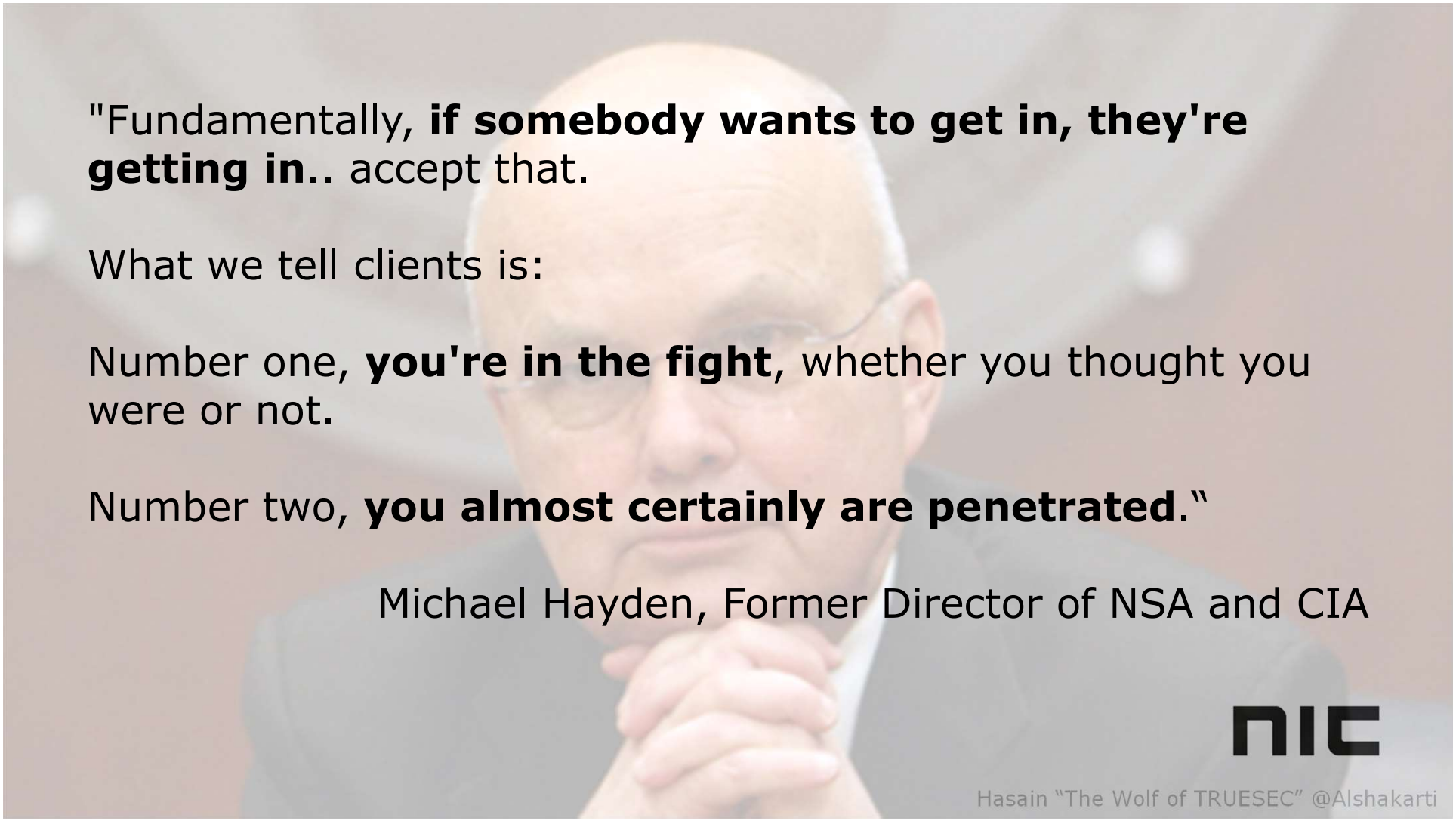

NIC
2019
Artificial Edition
6-8 February
Hasain "The Wolf of TRUESEC" @Alshakarti

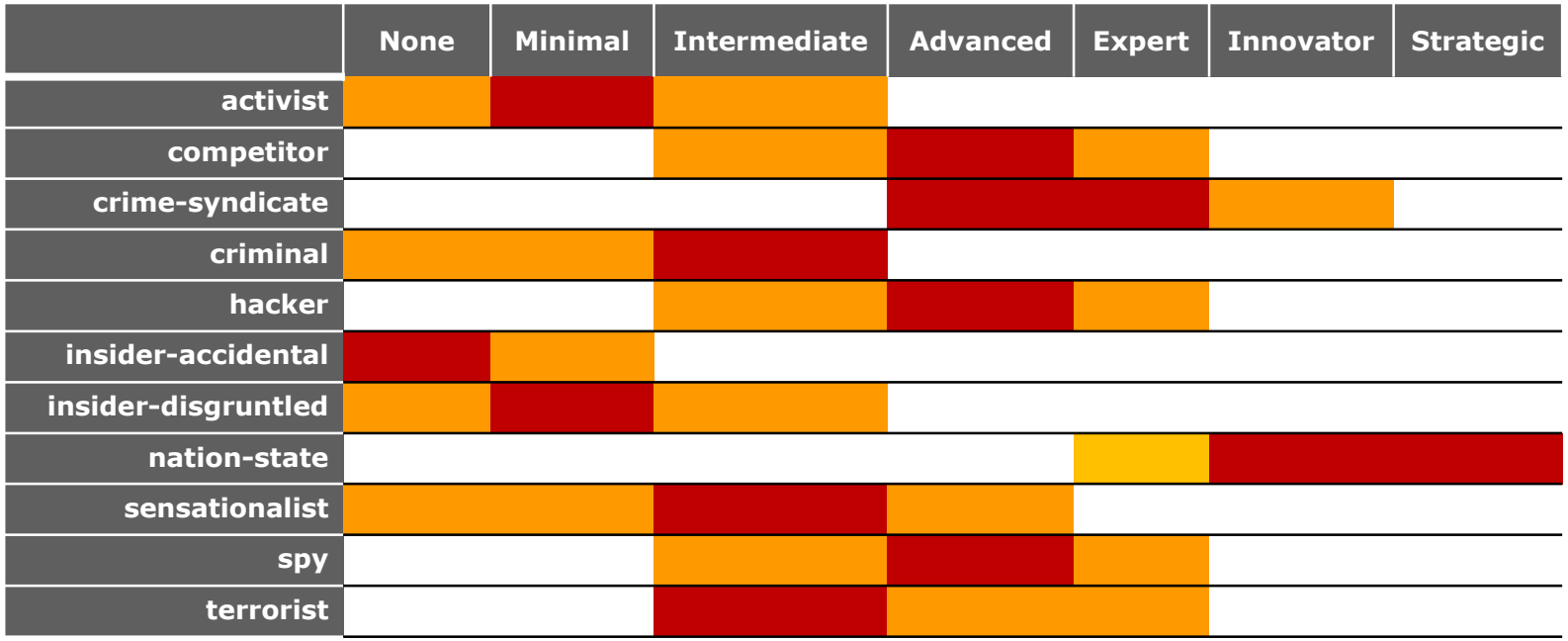
Are you prepared for a cyberattack - Red Teaming Methodology

Hasain “The Wolf” @Alshakarti

TRUESEC

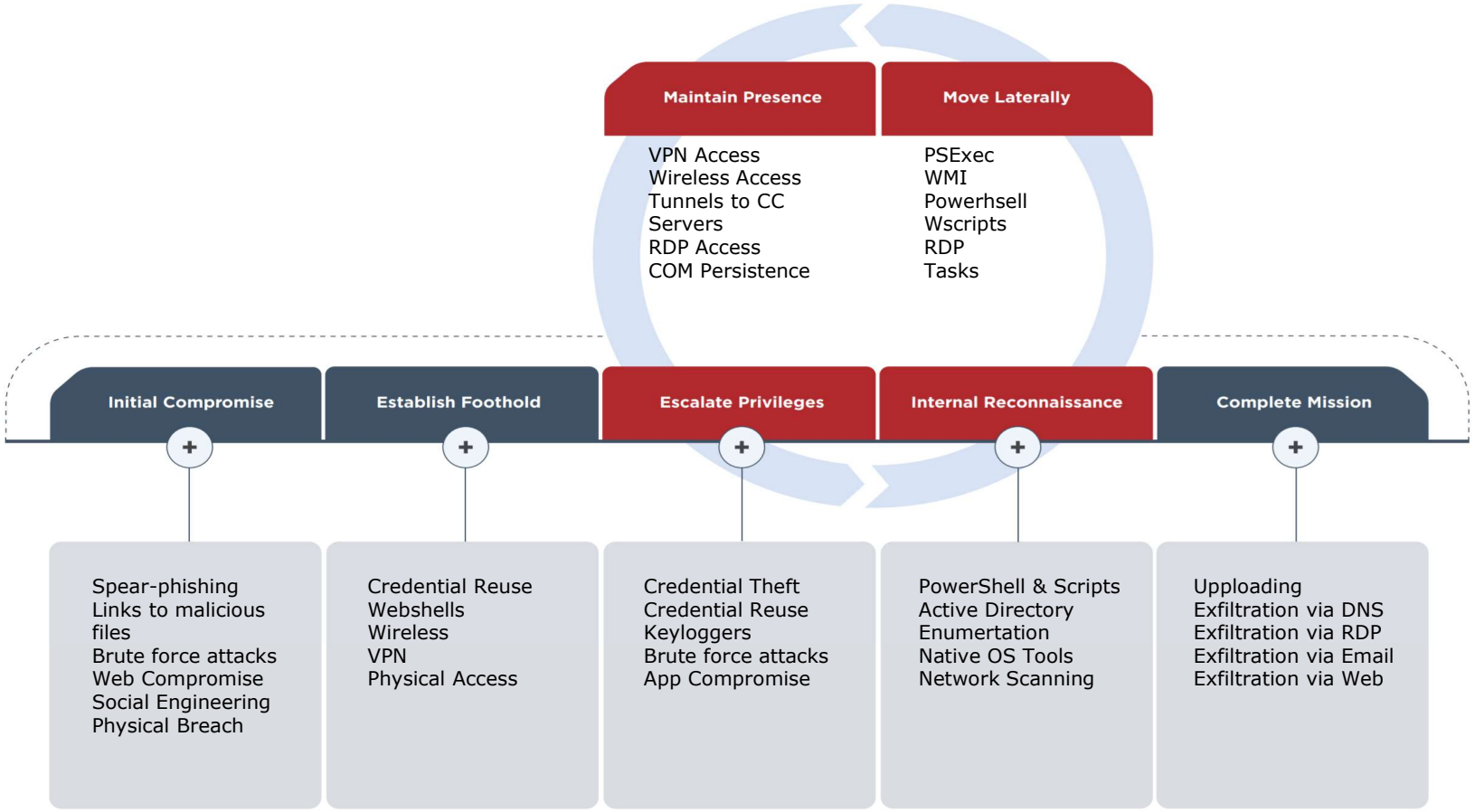

"Fundamentally, **if somebody wants to get in, they're getting in**.. accept that.
What we tell clients is:
Number one, **you're in the fight**, whether you thought you were or not.
Number two, **you almost certainly are penetrated**."
Michael Hayden, Former Director of NSA and CIA
Hasain "The Wolf of TRUESEC" @Alshakarti

Threat actor sophistication mapping



=**Primary** sophistication

= **Secondary** sophistication


Maintain Presence
Move Laterally
VPN Access
Wireless Access
Tunnels to CC
Servers
RDP Access
COM Persistence
PSExec
WMI
Powerhsell
Wscripts
RDP
Tasks
Initial Compromise
Establish Foothold
Escalate Privileges
Internal Reconnaissance
Complete Mission
Spear-phishing
Links to malicious files
Brute force attacks
Web Compromise
Social Engineering
Physical Breach
Credential Reuse
Webshells
Wireless
VPN
Physical Access
Credential Theft
Credential Reuse
Keyloggers
Brute force attacks
App Compromise
PowerShell & Scripts
Active Directory Enumertation
Native OS Tools
Network Scanning
Uppoading
Exfiltration via DNS
Exfiltration via RDP
Exfiltration via Email
Exfiltration via Web

Fieldkit

1. Devices to plant
2. Long-range wifi
3. Malware USB drives
4. Burner phone
5. Temp SIM cards
6. Get-out-of-jail
7. Faked access card
8. Tape, cables, adapters, multitools

Not in picture:

- Button-CAM / voice recorder
- Long-range camera
- Different bags + outfits
- Car
- Forced entry tools (e.g. lockpicks)

Reply Reply All Forward IM

Thu 11/10/2018 15:47

Alexander Andersson

RE: [redacted] Follow up {I7t:381812} {I7t:381812}

To [redacted]

Dear [redacted]

Thank you for your answer. I can assure you. As a cyber security company, our goal is to increase our customers security capabilities and protect users.
A service offering of ours is to assess cyber resilience and in these assignments we need to be able to use custom caller id.
You can read more about Truesec on https://www.truesec.com/.

Please let me know if you need any further information or assurance.

Best regards,
Alexander

From: [redacted]
Sent: 11 October 2018 15:37
To: Alexander Andersson <alexander.andersson@truesec.se>
Subject: RE: [redacted] Follow up {I7t:381812} {I7t:381812}

Dear Alexander,

Yes it is possible to set the caller ID to whatever you want however we will need some assurance you will not do anything nefarious with this. We can then allow you to use any caller ID.

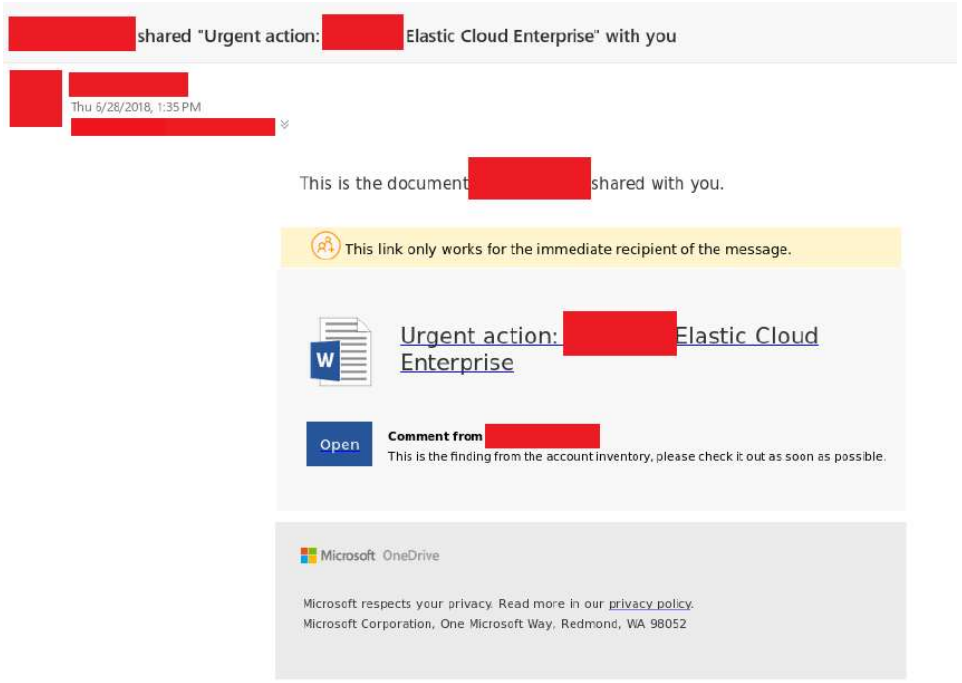
The main reason we have this in place is to stem fraudulant activity.

Kind Regards,

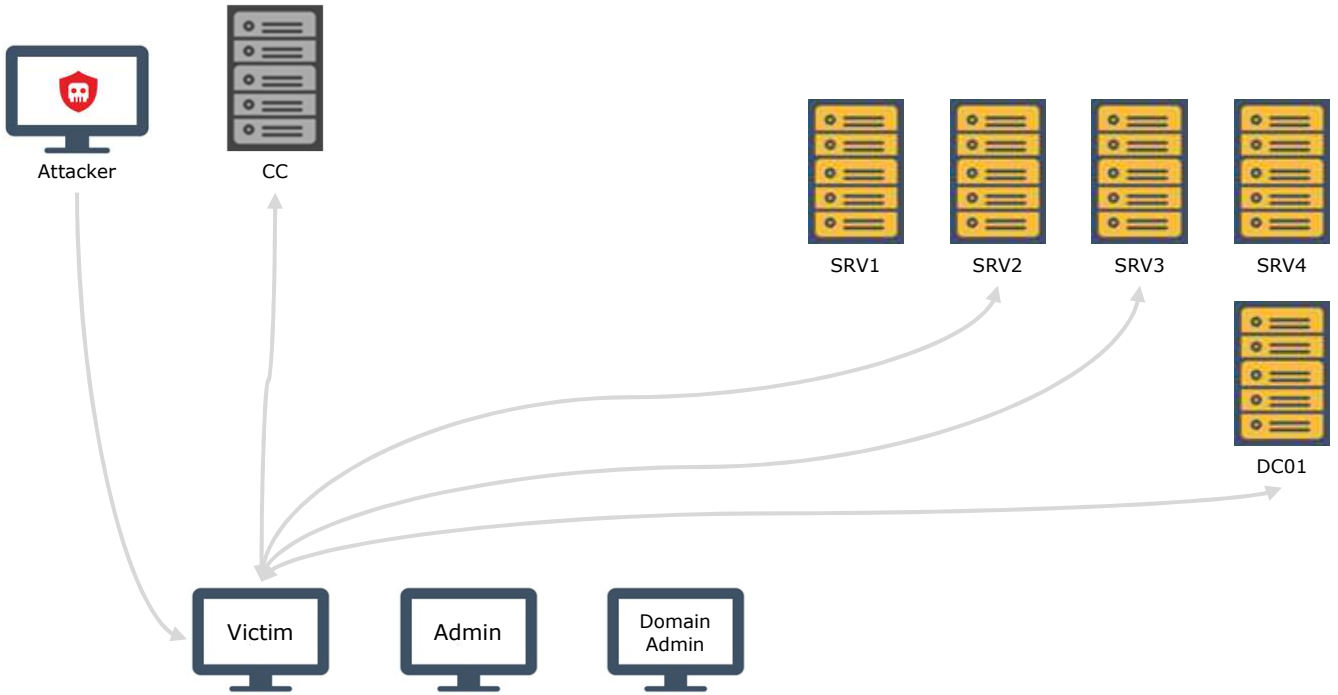
[redacted]


Reply
Reply All
Forward
IM
Thu 11/10/2018 16:56
[redacted]
RE: [redacted] Follow up {I7t:381812} {I7t:381812}
To
Alexander Andersson
You replied to this message on 12/10/2018 10:38.
Dear Alexander,
I have allowed any caller ID for you.
Kind Regards,
[redacted]

Teach a Man to Phish…



Hasain "The Wolf of TRUESEC" @Alshakarti


Attacker
CC
SRV1
SRV2
SRV3
SRV4
DC01
Victim
Admin
Domain Admin

Prevent Breach

- Code review
- External pentesting
- Security assessment

Assume Breach

- War Game and Red Team exercises
- Central monitoring and detection
- Live pentesting

Red Team – What/Who

A group of security-minded engineers and pentesters who:

- Simulate Real-World attacks
- Identify gaps in security
- Demonstrate impact

Red Team - How

- End-to-end security assessment
- Active and passive reconnaissance
- A wide range of attack methods and tooling

Red Team - Rules

Strict code of conduct:

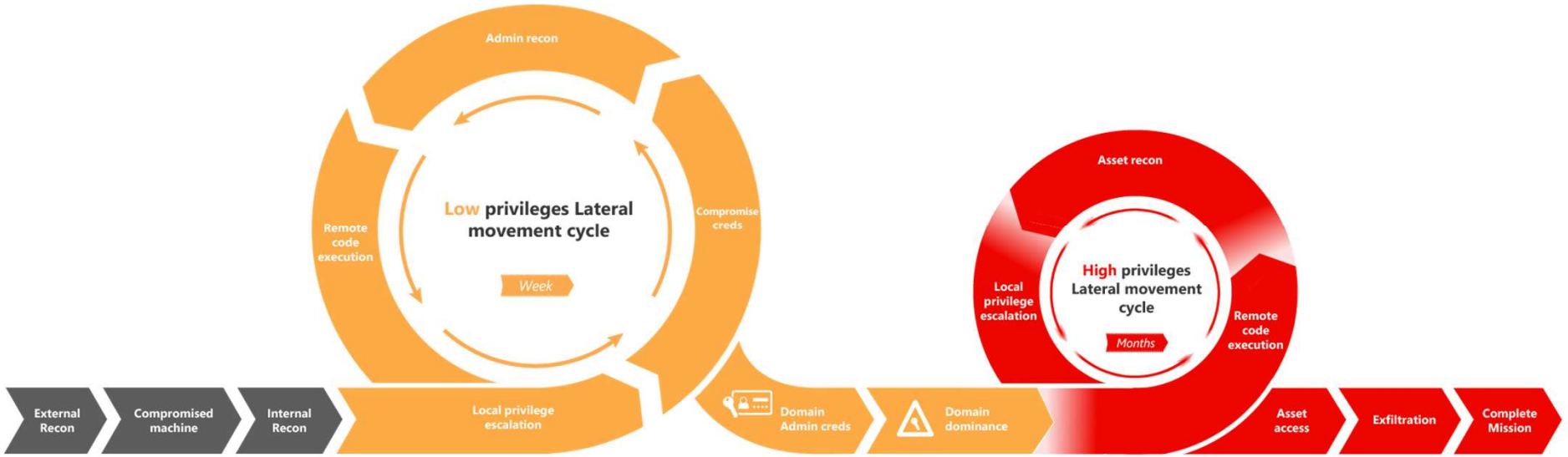
- SLA impact or downtime
- Perform destructive actions
- Weaken in-place security protections
- Safeguard vulnerability and critical information

Red Team - Post-Mortem

Detailed custom reports:

- Breach Timeline
- Mean Time to Compromise
- Mean Time to Privilege Escalation or “Pwnage”
- Mean Time to reach High Value Tagets
- Lists of Vulnerabilities

Knowledge sharing with Blue Team



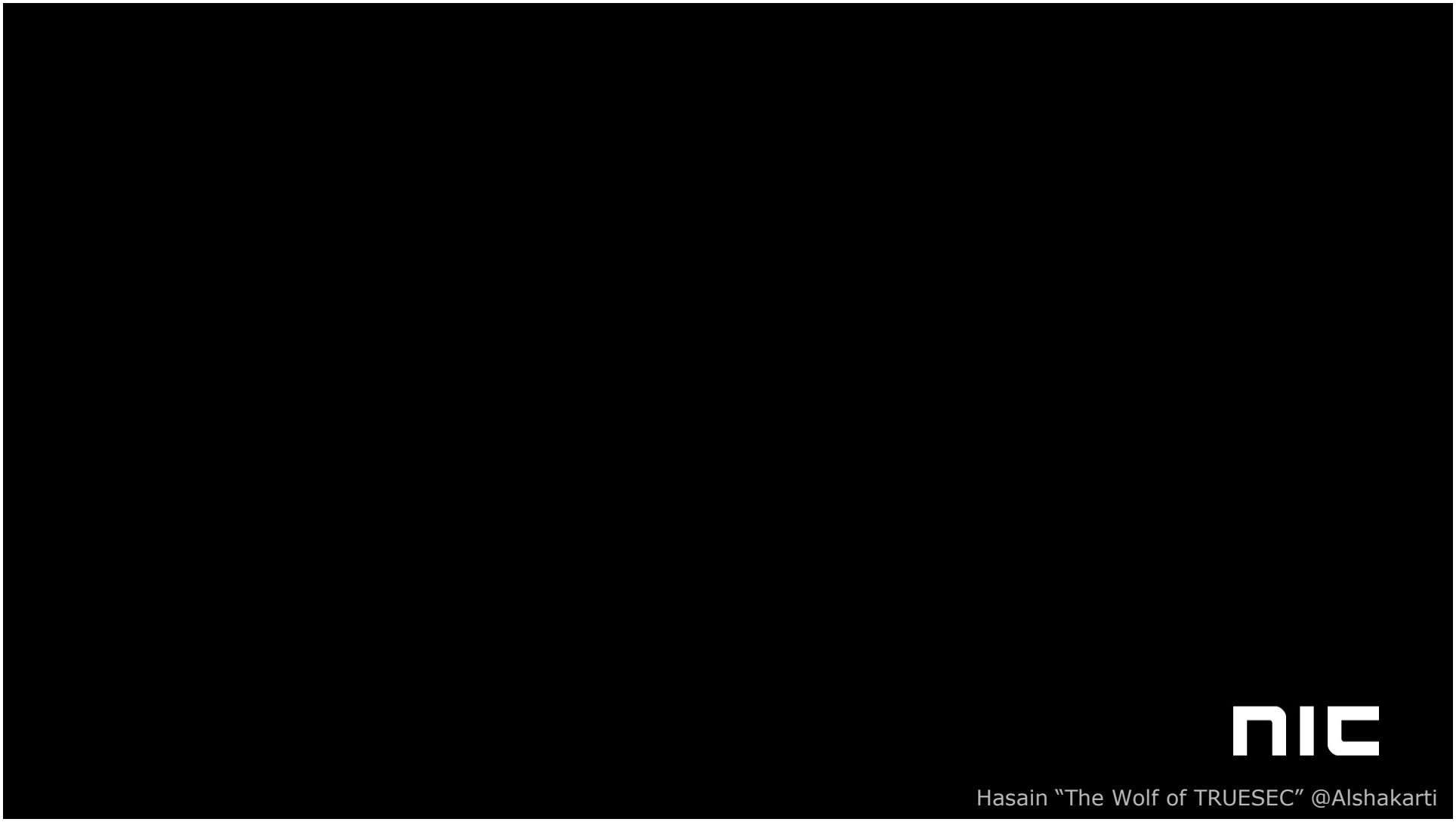
Hasain “The Wolf of TRUESEC” @Alshakarti

Want to take this one step further?

- Seek to **delay and respond** rather than **prevent** an attack
- Investments in **detection** and **monitoring controls**
- Investments in **incident response**
- Investments in **technical analysis capabilities**

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2019


Hasain “The Wolf of TRUESEC” @Alshakarti