Cyber Hygiene

Anatomy of a Cyber Attack

Zac Warren

Chief Security Advisor, EMEA

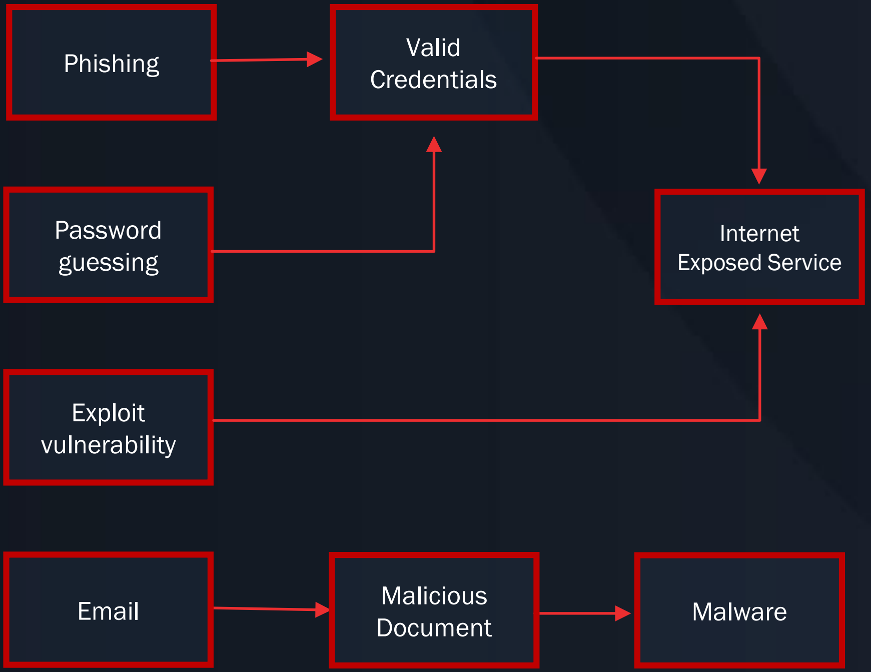
Tanium

Lifecycle of a Ransomware Attack

TANIUM

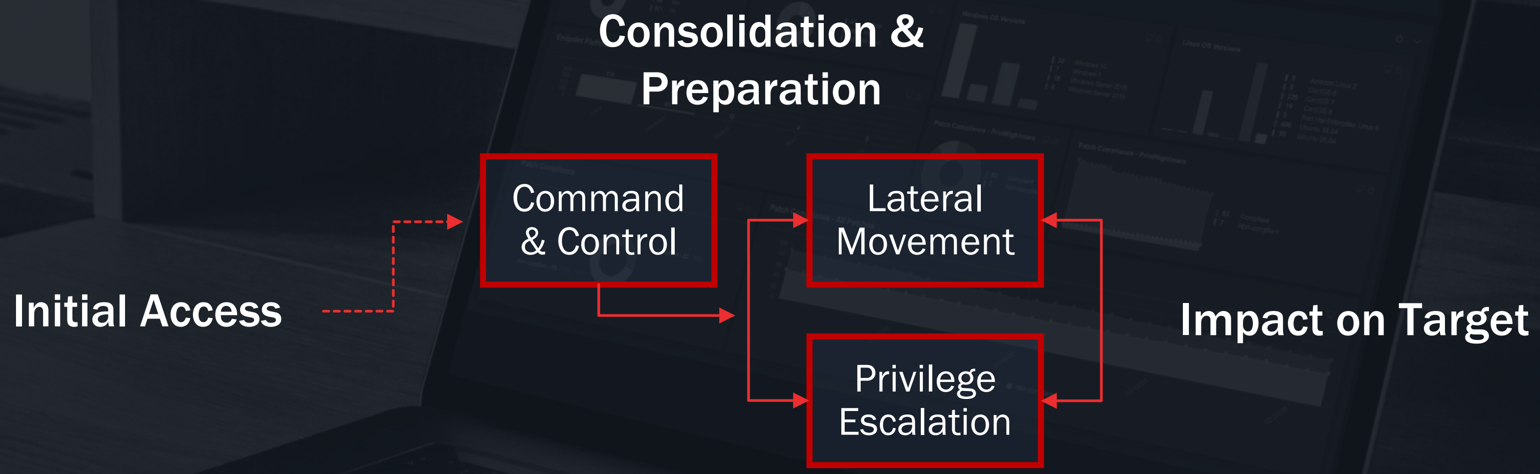
Lifecycle of a Ransomware Attack

Initial Access



Consolidation & Preparation

Impact on Target



Consolidation & Preparation

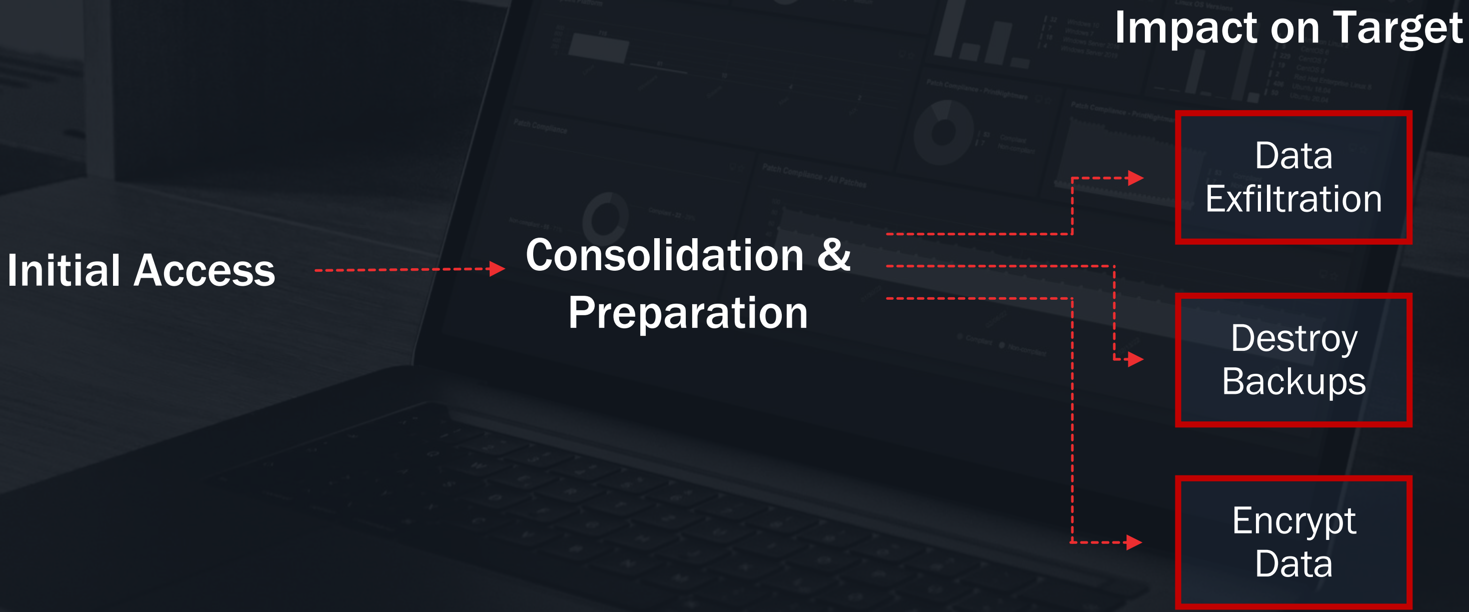
Initial Access

Command & Control

Lateral Movement

Privilege Escalation

Impact on Target



Impact on Target

Initial Access

Consolidation & Preparation

Data Exfiltration

Destroy Backups

Encrypt Data

Preparation and Counter Measures

TANIUM™

Visibility & Control

Continuous Safeguarding

Detection & Countermeasures

Visibility & Control

Asset Discovery	You can only protect what you know
Access Control	You need access to take actions
Identify Critical Assets	Budget is limited, focus on important assets

Visibility & Control

Continuous Safeguarding

Detection & Counter Measures

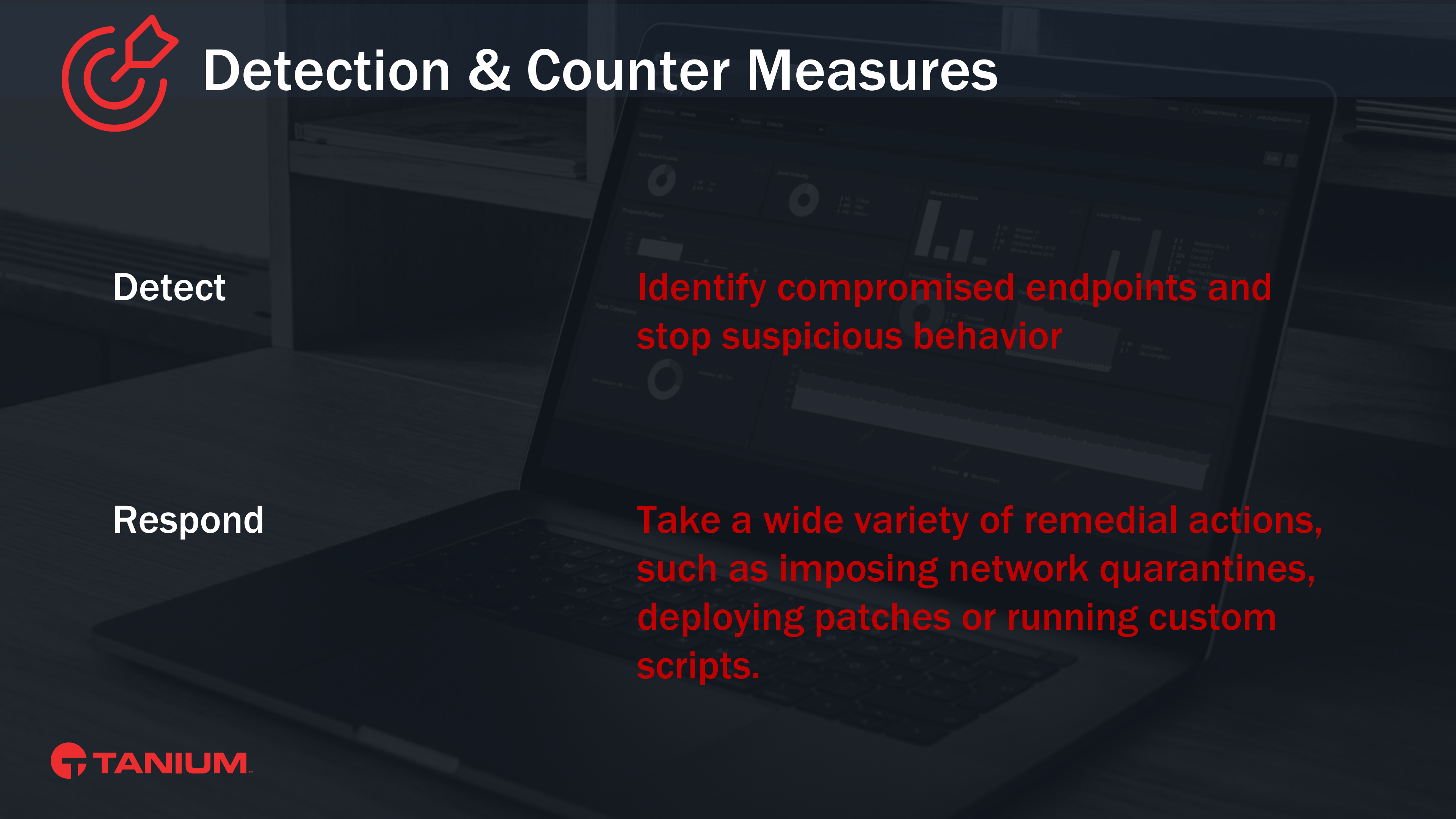
Continuous Safeguarding

Administrator Overview	Know and restrict your powerful users
Patching	Close (unknown) vulnerabilities
Vulnerability & Compliance	Increase attacker costs & efforts

Visibility

Continuous Safeguarding

Detection & Counter Measures



Detection & Counter Measures

Detect

Identify compromised endpoints and stop suspicious behavior

Respond

Take a wide variety of remedial actions, such as imposing network quarantines, deploying patches or running custom scripts.

3 Take-a-ways

Visibility & Control

Continuous Safeguarding

Detection & Countermeasures

TANIUM

Thank You

Zac Warren – zac.warren@tanium.com