REVERSEC

Leveraging Offensive Security Expertise for Cost-Conscious Security

Nick Jones – Global Head of Research

Agenda

1. The Cost of Being Secure
2. Less Security Testing is More
3. Prioritisation Through Threat Modeling
4. Alternatives to Traditional Penetration Testing

The Cost of Being Secure

Good Security Costs Too Much

Security Tooling
EDR + SIEM + CSPM/CWPP + Zero Trust + [...] = $$$$$$
Significant investment also required to integrate

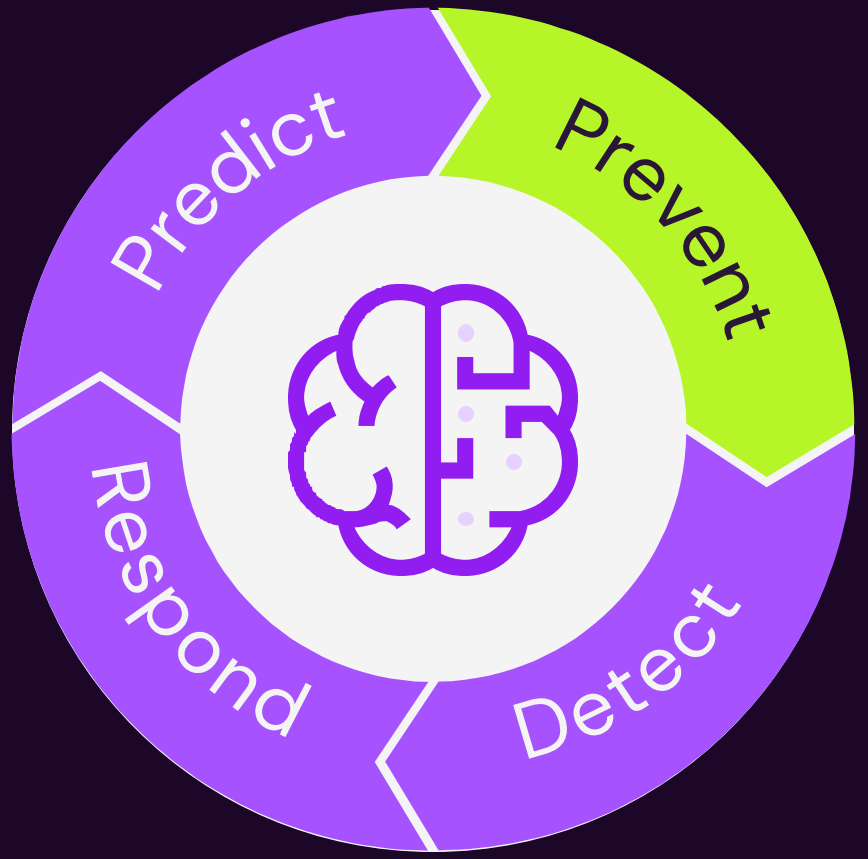
People
Skilled cybersecurity professionals are in short supply and high demand, meaning high cost and retention challenges

Software-as-a-Service Business Models
Many SaaS offerings charge extra for security features, audit logs, or enterprise-grade authentication

Compliance Demands
A lot of compliance frameworks require significant investment, and haven't kept up with modern security approaches

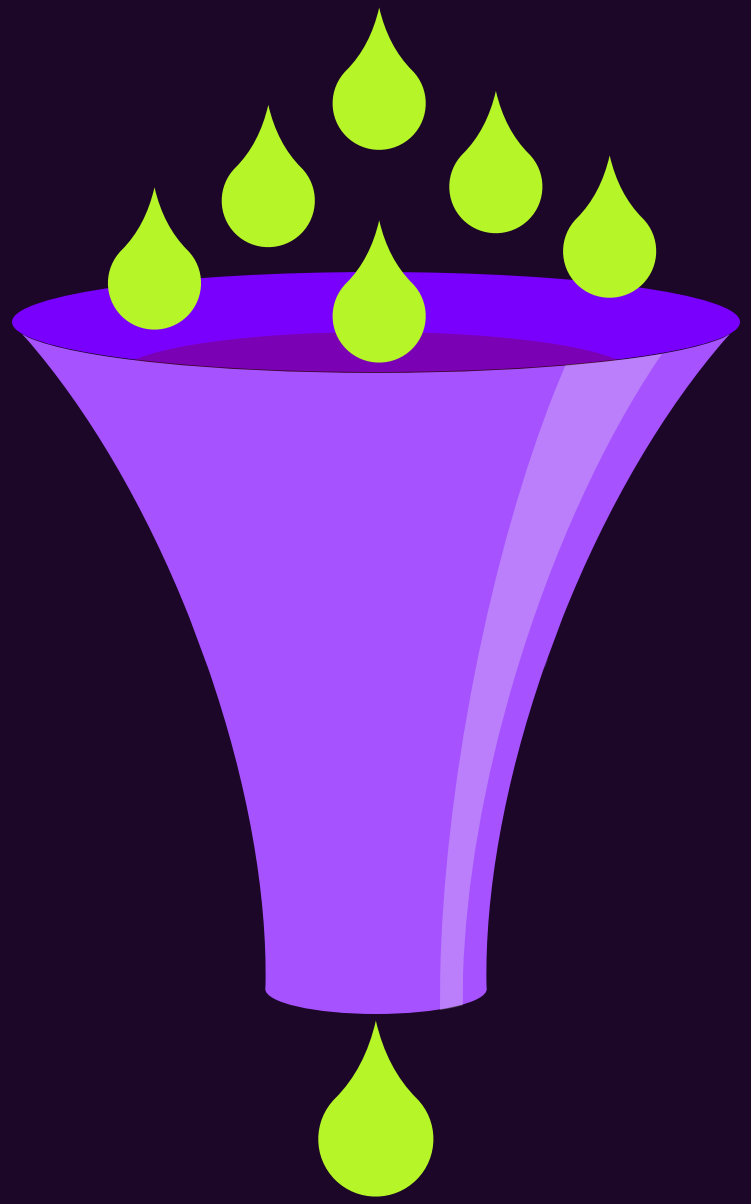
The Preventative Cost Trifecta

- Assessments and audits
- Remediation and hardening
- Regression testing



More Findings than Time

- Poor prioritisation
- Not tied to business risk
- Justifying security investment becomes harder



Ransomware: The Canonical Example

>10 years on, it's still a huge problem

We can't get the basics right

Multi-factor authentication	Permissions management	Network segregation	**Backups**

Current funding and assessment strategies are **not** working

Less Security Testing Is More

Outdated Assessment Approaches

01. Paper-Based Audits

Time-consuming, and the output rarely reflects reality on the ground

02. Point-In-Time Penetration Testing

Assessing workloads individually misses the paths a real-world attacker might take

Can be outdated before the report is even finished

03. “Red Team” Engagements

Expensive, and >90% of organisations aren’t mature enough to get maximum value out of them

Assess the Right Things

01

"we need a pentest before we can go live"

02

Does everything need an assessment?

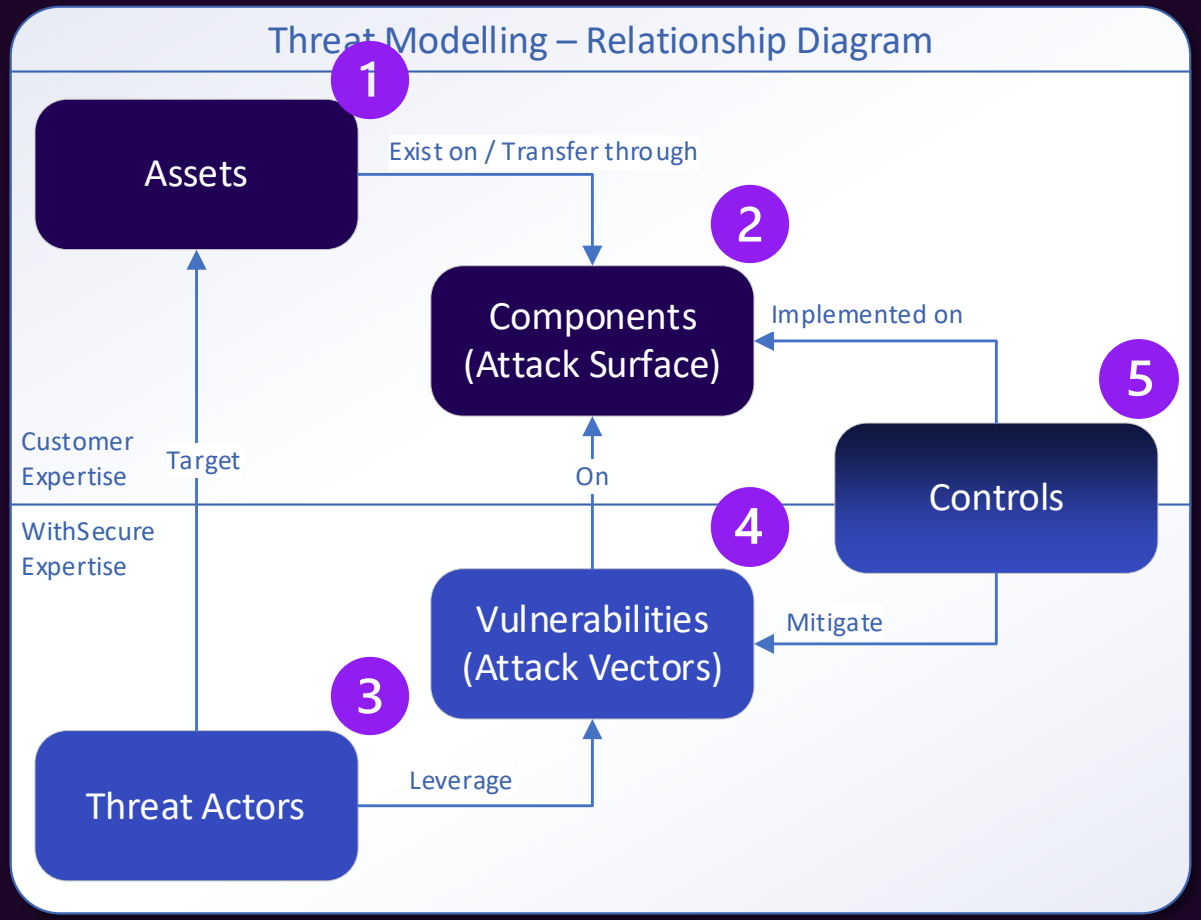
03

How do we decide what deserves an assessment?

Prioritisation Through Threat Modeling

Threat Modelling TL;DR

1. Identify the **assets**
2. Define the **attack surfaces**
3. Identify **threat actors** and their **objectives**
4. Determine the potential **attack vectors**
5. Select and prioritize **controls**



Threat Modelling by App

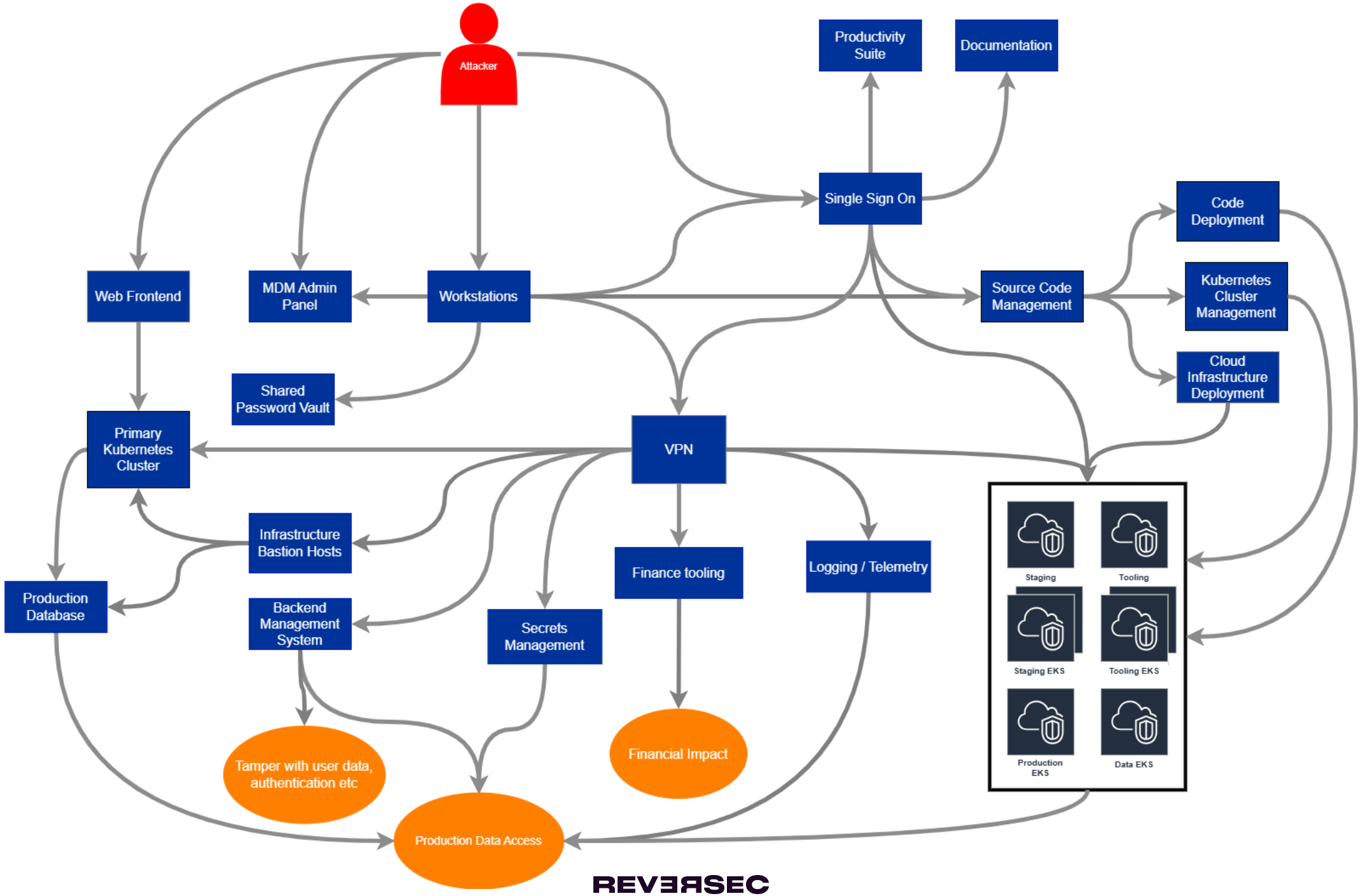
WITH secure

Threat Modelling an Organisation

Assets = business level critical assets

Factor in organisation-wide risks

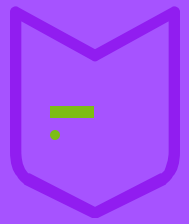
Identify what will *really* hurt the business


Attacker
Productivity Suite
Documentation
Single Sign On
Code Deployment
Web Frontend
MDM Admin Panel
Workstations
Source Code Management
Kubernetes Cluster Management
Shared Password Vault
Cloud Infrastructure Deployment
Primary Kubernetes Cluster
VPN
Infrastructure Bastion Hosts
Finance tooling
Logging / Telemetry
Production Database
Backend Management System
Secrets Management
Staging
Tooling
Staging EKS
Tooling EKS
Production EKS
Data EKS
Tamper with user data, authentication etc
Financial Impact
Production Data Access

Deciding What To Assess

- Compliance Demands
- Chokepoints
- Authentication Systems
- Critical Adminstration Assets

Prioritising Remediations

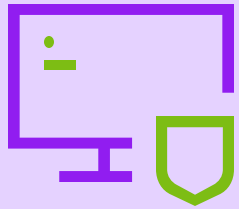


Threat Model Informs Priority

Use the organization-wide threat model to inform the prioritization of findings tied to individual assets

Focus on Chokepoints

Some controls & fixes will break several attack paths at once



Business Context Matters

The closer you can tie improvement activities to business risk, the easier it is to unlock investment from leadership

Alternatives to Traditional Penetration Testing

Objective Driven Assessments

Business targets

- Steal key data/IP
- Move money
- Deploy malicious code to prod

Realistic starting points

- Leaked access keys
- Compromised dev/insider threat
- Application compromise

Attack Path Mapping

Objective-focused

Not ad-hoc “Vulnerabilities”
Business-Impacting scenarios
not just Technical Achievements
(e.g. get Domain Administrator)

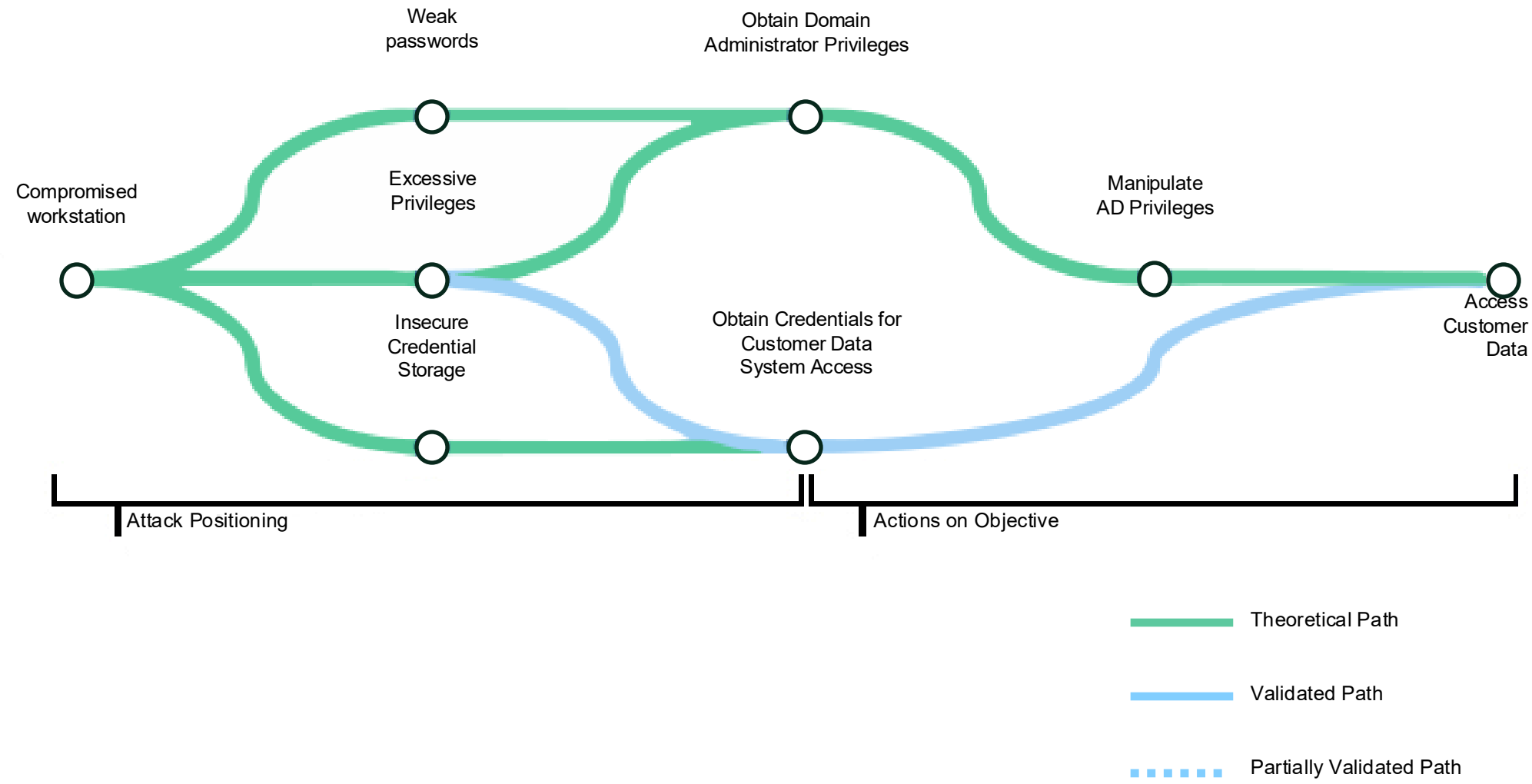
Broad scope

Holistic
Assesses entire digital estate
Not limited to e.g. specific-component
Exploits the ties between the various
technologies and landscapes

Collaborative

Transparency
No Stealth / Evasion
Interviews with key SMEs
…therefore Time-efficient

Attack Path Mapping



What value do we provide?

Collaborative and **time-efficient** “white-box” exercise that looks at an environment **holistically**

Focused on **objectives** that matter to the business, not just protection of technical systems

Technical testing to **validate** and **prioritise** identified paths and help discover further paths

Remediations aimed at actions to improve **organisational resilience**

Red Team Engagements

You probably don't need one

- All about stealth, validating detection and response
- Depth, not breadth

Red Teaming is the final step

- Confirm and harden your attack surface
- Build your detection and response
- Test hardening, detection & response collaboratively
- … **then** maybe a red team!

REVERSEC

Thanks for Listening!
Come talk to us at Stand 650

Abstract

Effective prioritization of security activities allows a balance to be struck between the cost to identify critical security issues and the cost to mitigate them. Budget constraints require security teams make daily decisions about which security activities are worth the cost, which is of particular concern in the current economic environment.

This talk highlights how to leverage offensive security expertise to enrich your organizations understanding of relevant threats and the most cost-effective paths towards addressing the risks they present. It will cover:

- The delicate balancing act security teams are required to maintain between spending money identifying security issues, mitigating those issues through security controls, and maintaining those security controls to ensure their continuing effectiveness.
- The importance of properly targeted penetration testing, emphasizing that finding and securing every vulnerability in an organisation is often both costly and unnecessary.
- A threat-informed approach to prioritize both testing and remediation efforts, ensuring that resources are allocated effectively to identify and address the most critical vulnerabilities.

Attendees will walk away from this talk with a clear understanding of:

- How to leverage offensive security expertise to identify realistic attack paths based on your organization's risk
- How to use this additional understanding to create impactful mitigation strategies that address your real world cyber risk, rather than simply tick a box in a benchmark.
- How to effectively prioritise spending on penetration testing and security audits for the best security outcomes