NetSPI

# Building a Proactive Security Playbook for Lasting Cyber Resilience

Sam Kirkman, Director of Services, EMEA

Business Hall Theatre A

11 December 2024

2:15 pm

# Building a Proactive Security Playbook for Lasting Cyber Resilience

## What will we cover?

- Cybersecurity today across Europe
- What is “Proactive Security”?
- Real-World examples of NetSPI helping clients through proactive security to:
  - Discover
  - Prioritise
  - Remediate

# Sam Kirkman

Director of Services, EMEA

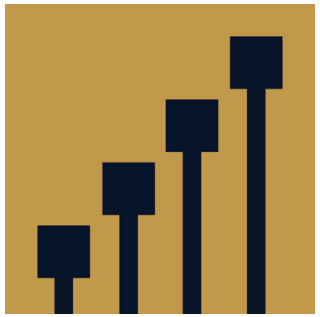
- Penetration Tester
- Security Architect
- Solution Engineer

https://www.linkedin.com/in/sam-kirkman-cybersecurity

# What challenges await in Europe?

**Legislation and Regulation**

- DORA
- NIS 2



**Geopolitical Drivers**

- Dependencies
- Disruption

**Emergent Technologies**

- Non-deterministic AI
- Data capture

# What is Proactive Security?

## Discover: Know What You Have

**Benefits:** Full sight of your assets and vulnerabilities lets you defend and mitigate across all edges and your business.

**Challenges:** Over reliance on technology can provide false sense of security, and lack of detailed understating of discovery methods and logic and disparate siloed capabilities.

## Prioritise: Evidence-Based Planning

**Benefits:** Knowing how and where to spend time and budget makes best use of limited resources.

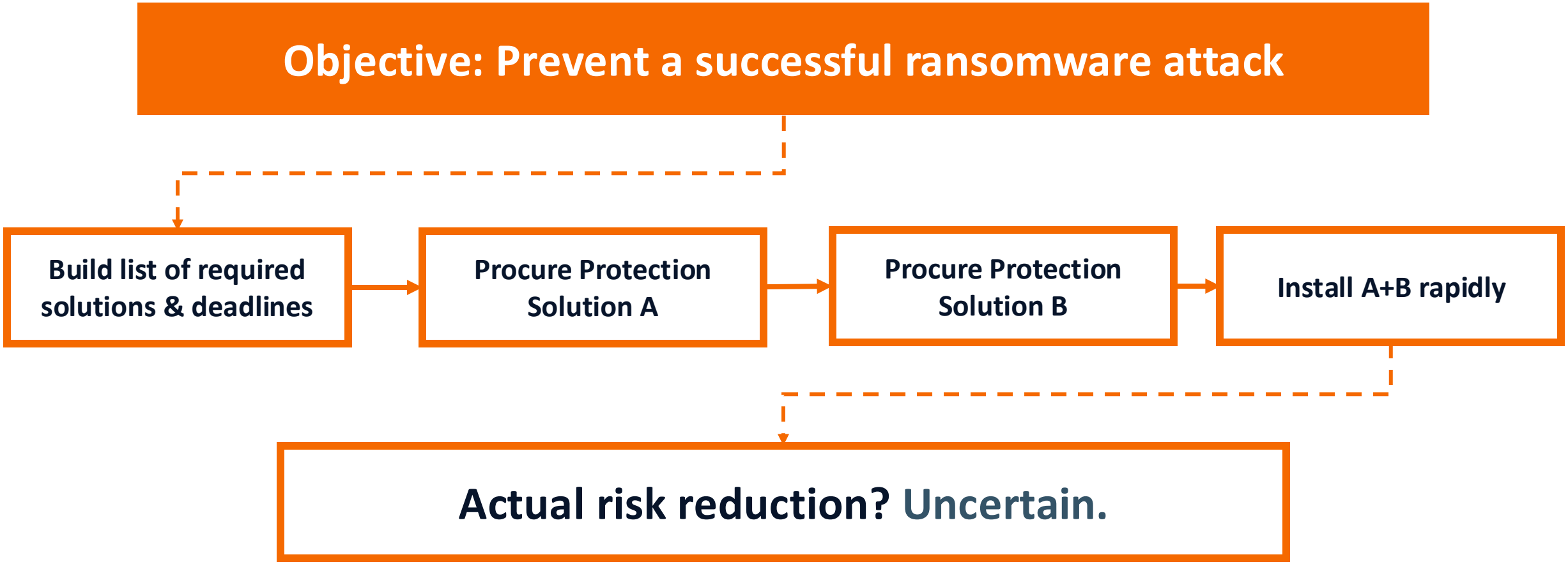
**Challenges:** It relies on solid integration of all technology and information gathering processes to supply accurate intelligence and priorities, and effect business support to enact them.

## Remediate: Timely and Robust Fixing

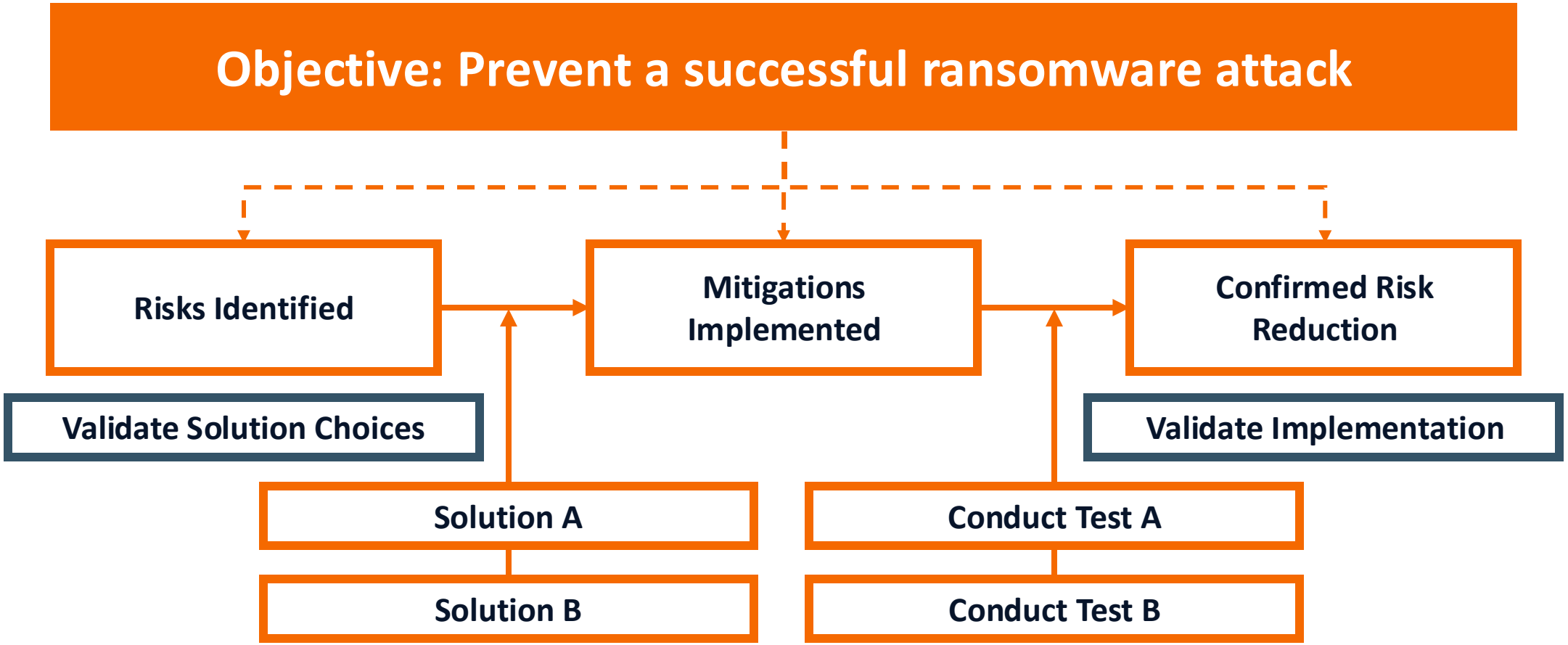
**Benefits:** Fixing things goes without saying, but how sure are you of its quality and coverage can you assert the control is effective and implemented before others are able to abuse any weaknesses?

**Challenges:** Timing is key, too late and you risk being compromised already, too soon and you may have made a rushed choice. A bad fix provides false security, as much basing fixes on fragile metrics, indicators and logic.

# Proactive Intent:
## Reactive Approach



# Adopting a Better Approach:
## Proactive Planning



# What assets do I have, and where are my vulnerabilities?

# NetSPI's Proactive Security Stories: Cloud Penetration Testing (CPen)

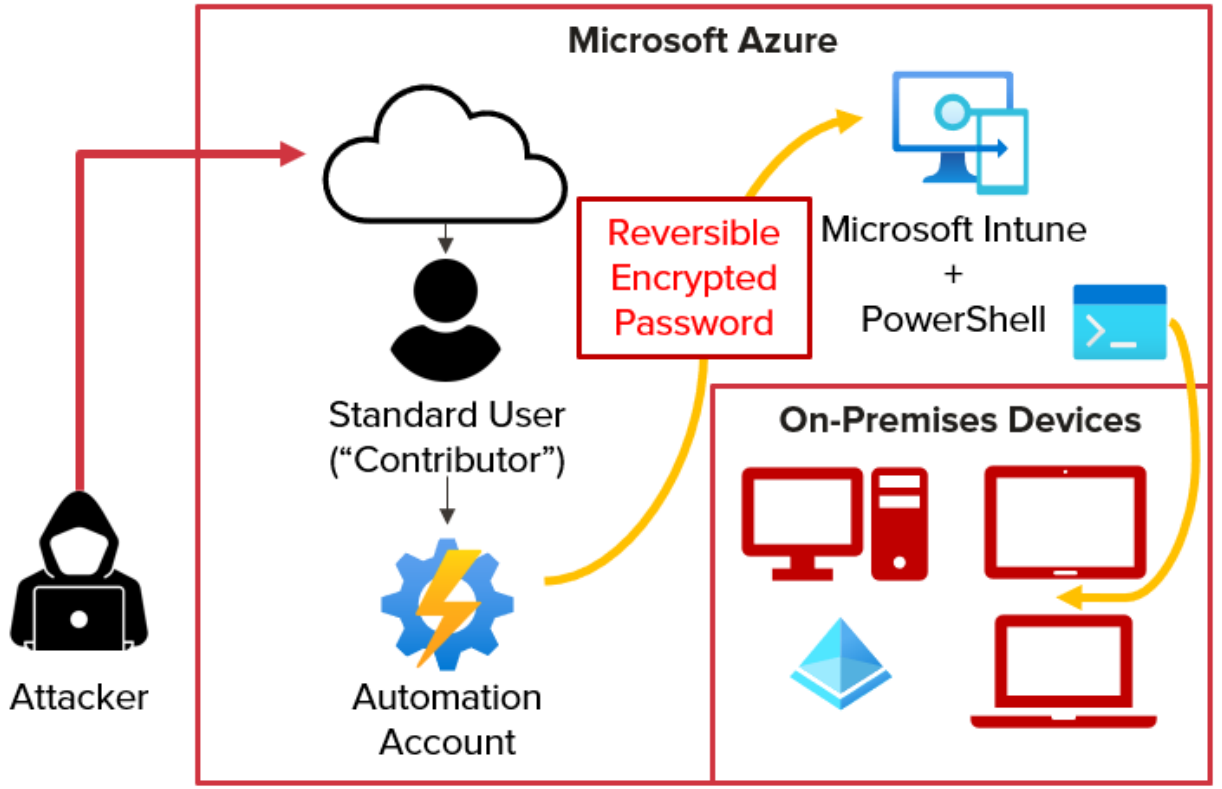
# Azure Risk Identified

*NetSPI Cloud Pentesting identifies a route to pivot from the cloud to the internal network*

## Risks Identified

**Potential Result:**

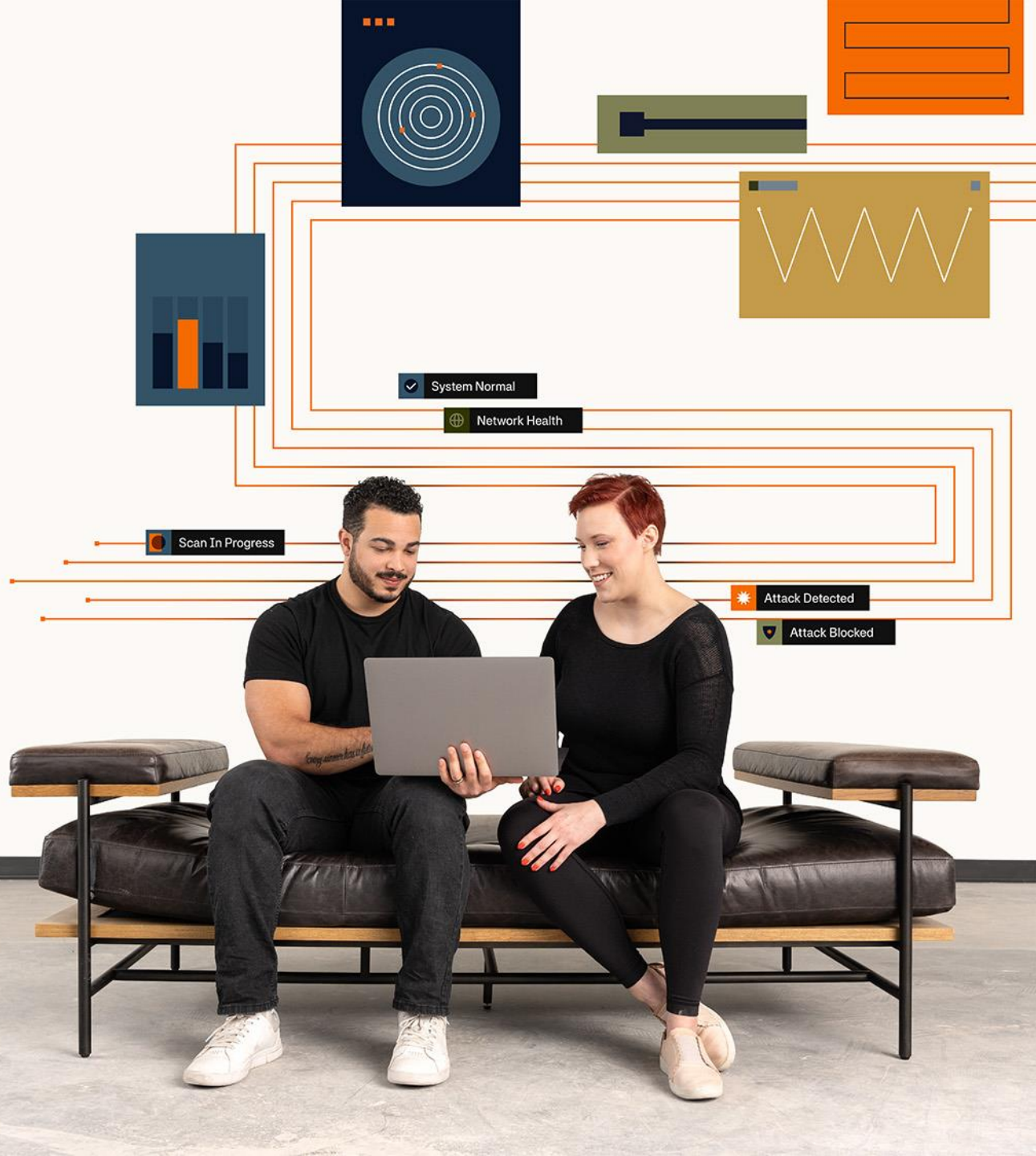
- Full compromise of all endpoint devices
- Extensive access to sensitive data
- Powerful persistence mechanism
- Insider threat attack vector




**NetSPI In-House Azure Security Experts**

# How can I establish continuous monitoring of my assets and effectively prioritize remediation efforts?

# NetSPI's Proactive Security Stories: Attack Surface Management (ASM)



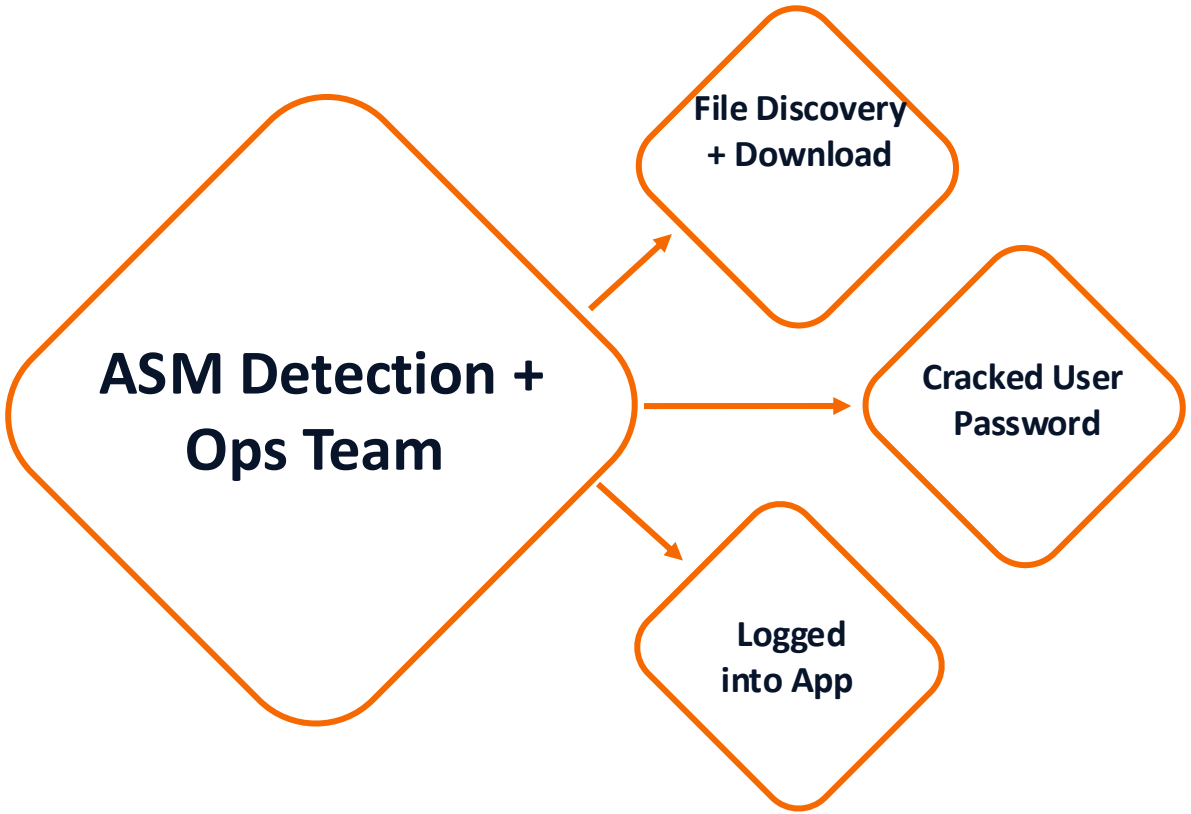
# Customer Story

## Anatomy of  Health Care App at Risk

*NetSPI ASM prevents potential application takeover and PII data exposure*

## Risks Averted

- Exposure of source code and credentials
- Database exposure
- Exploitation of healthcare PII data
- Application infrastructure takeover
- Compliance and HIPPA fines and penalties




**NetSPI ASM is technology enabled human delivered**

Is it possible to truly validate the effectiveness of my security controls?

# NetSPI's Proactive Security Stories: Breach and Attack Simulation (BAS)

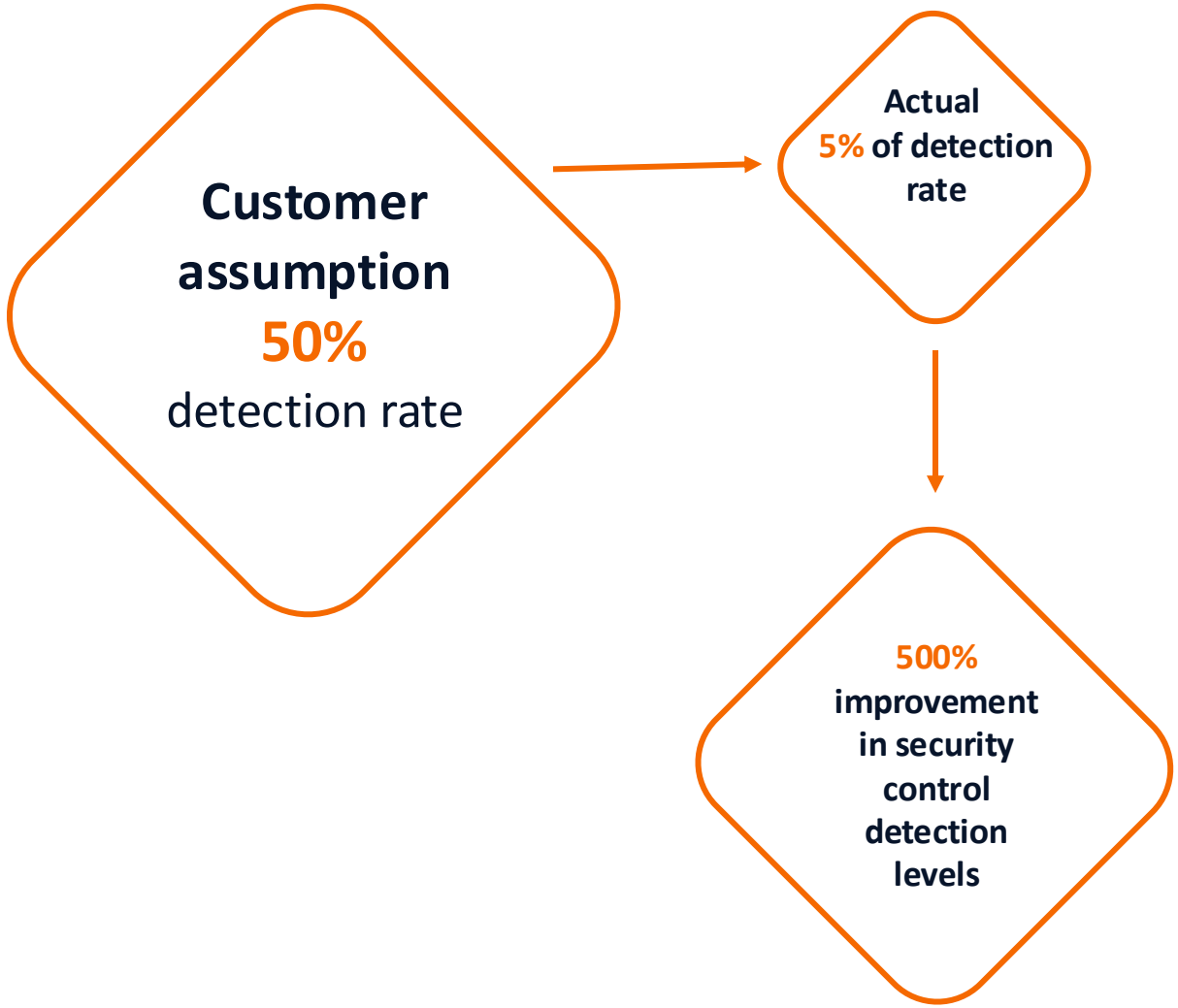
# Customer Story

**Mind the Gap:**
**Security Control Assessment**

*NetSPI uncovers and reduces a 45% gap In customer security posture*

## Risks Uncovered

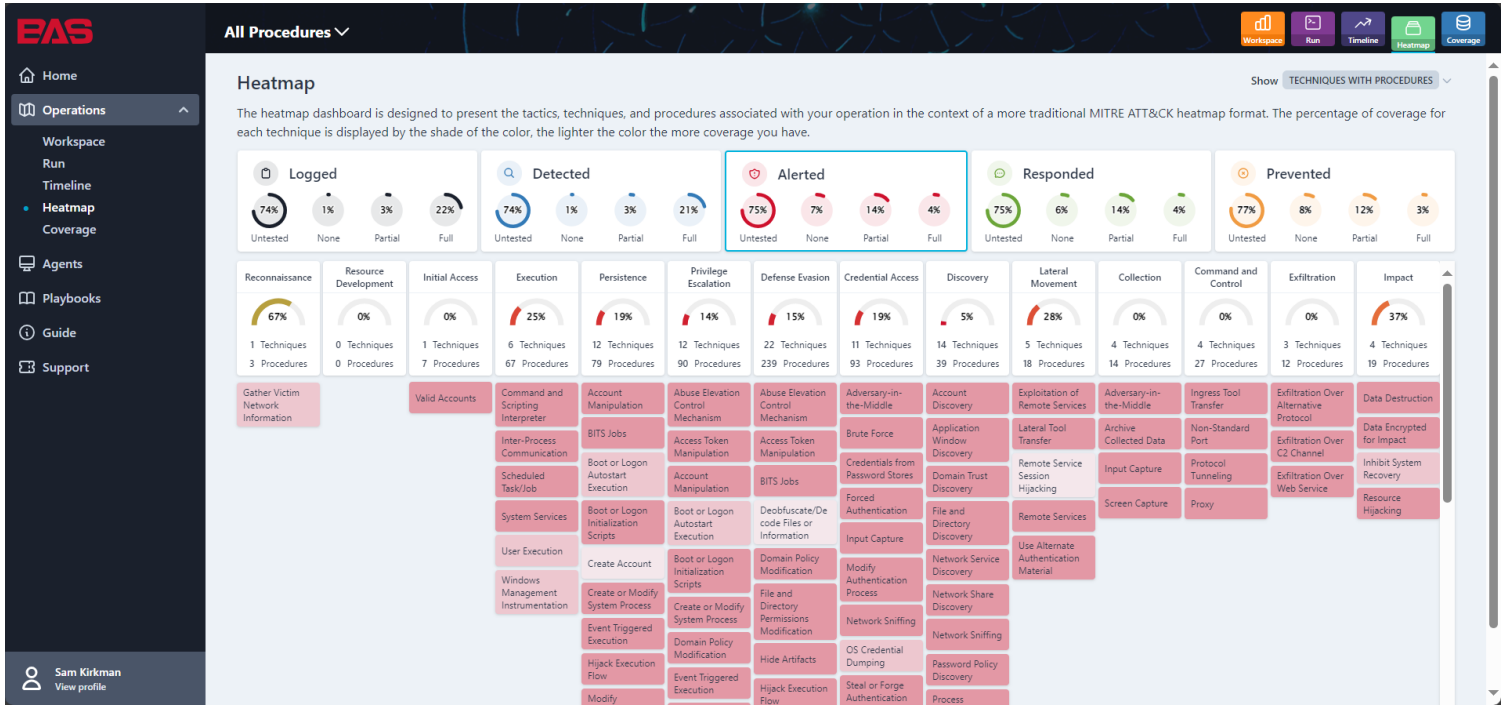
- Misconfigured EDR
- Underdeployed EDR
- Missing log ingestion
- Incorrect log storage



# Continuous Automated Validation

## Breach and Attack Simulation

**“Best ROI On Security $$ I've Seen In 25 Years”**




Gartner Peer Insights™

MITRE | ATT&CK®

# NetSPI Proactive Security Solutions

## PTaaS

**Pentesting programs from Appsec to AI**

- Expert delivered pentesting via SaaS platform
- Real-time in-platform reporting
- Decrease detection and remediation time
- Easily integrate with ticketing systems
- Meet compliance needs

## ASM

**Attack Surface Management**

### EASM

- Always-on external asset discovery and monitoring
- Eliminate noise with validation, prioritization
- Deep context with potential attack path scenarios

### CAASM

- Total internal asset visibility and contextualization
- Real-time, centralized risk and vulnerability mapping
- Visualize impact with blast radius

## BAS

**Security control validation**

- Validate security detection control efficacy
- Simulate real-world attacker behaviors
- Fine-tune security controls and optimize security stack
- Strengthen ransomware prevention defenses
- Track progress and demonstrate ROI

**We bring together dedicated security experts, intelligent process, advanced technology to contextualize the priorities that will have the biggest impact on your business**

# Visit Stand #320

## netspi.com/emea


**Sam Kirkman**

Director of Services, EMEA

sam.kirkman@netspi.com

https://www.linkedin.com/in/sam-kirkman-cybersecurity/

241 N 5th Ave Suite 1200

Minneapolis, MN 55401

**netspi.com**