

# Charting the Course: Navigating Proactive Security

Sam Kirkman, Director of Services, EMEA 19 November 2024

5:35 pm

### Charting the Course: Navigating Proactive Security

 $\bowtie$ 

#### 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

#### Quality | Efficiency | Value

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.



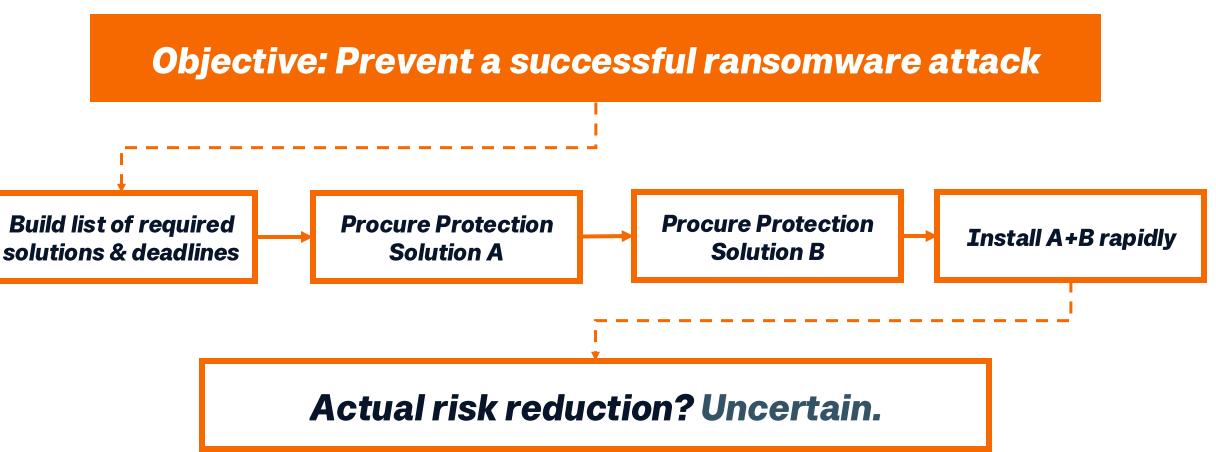
#### **Remediate:** Timely and Robust Fixing

**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.

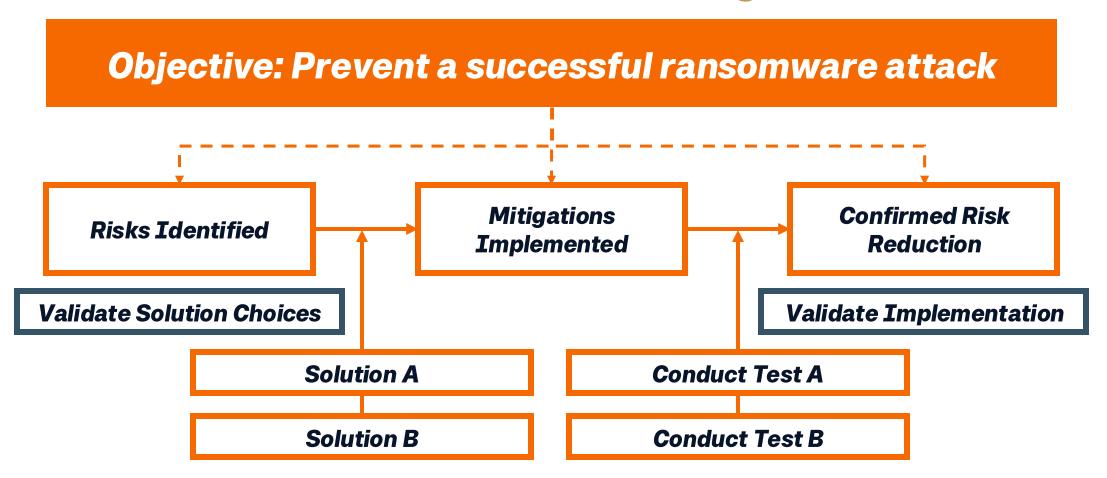


## **Proactive Intent: Reactive Approach**





### 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)



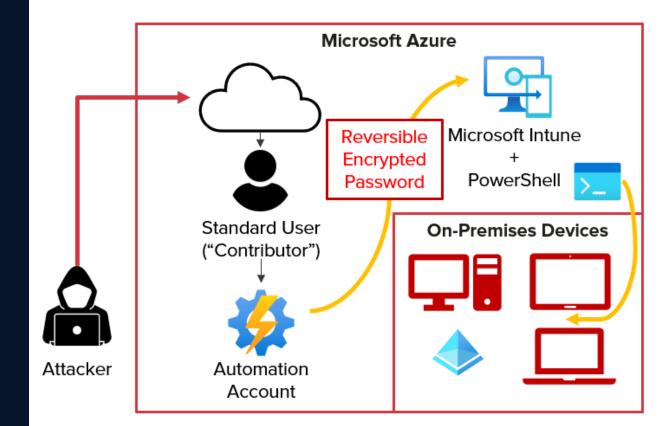
### **Azure Risk Identified**

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



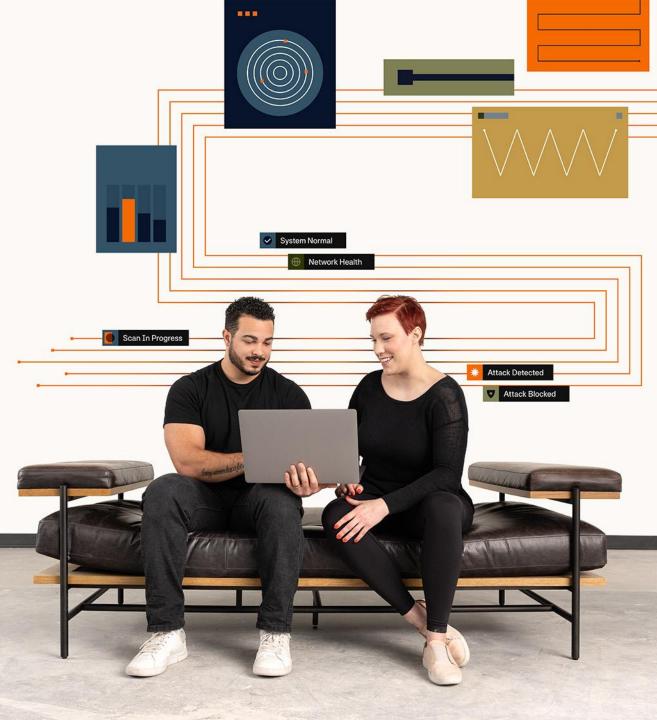
#### **NetSPI In-House Azure Security Experts**



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



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



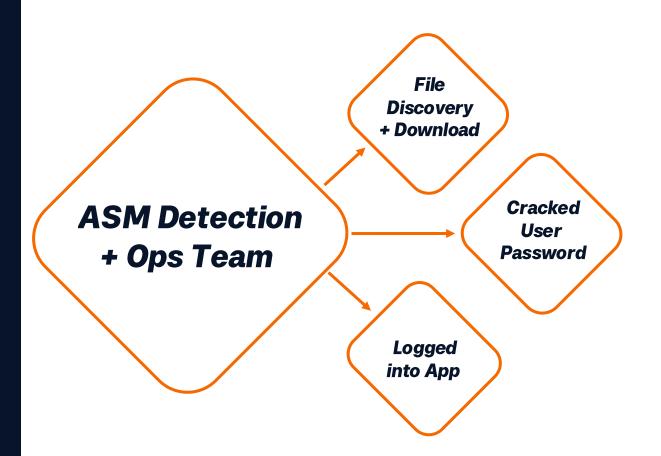
# **Customer Story**

#### 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



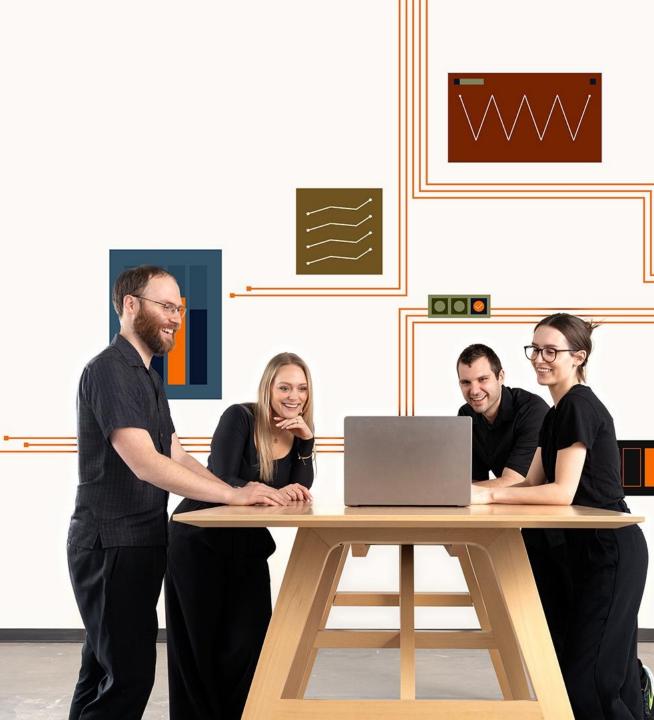
#### NetSPI ASM is technology enabled human delivered



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



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



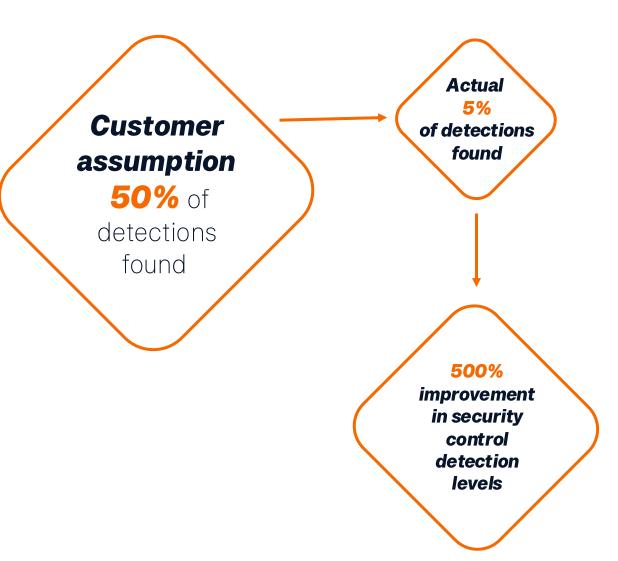
# **Customer Story**

#### 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"

 $\bowtie$ 

me	Heatmap											She	TECHNIQUES	WITH PROCEDURES
erations ^		ashboard is des	igned to prese	nt the tactics, te	chniques, and p	rocedures asso	ciated with your	operation in the	e context of a i	nore traditional N	/ITRE ATT&CK	heatmap format	. The percentag	je of coverage fo
kspace	each technique	is displayed by	the shade of t	ne color, the lig	nter the color th	e more coverag	ge you have.							
				Q Detected			Ø Alerted			Responded			O Prevented	
line map trage	74%	1% 3%	22%	74% 15	6 3%	21%	75% 7%	14%	4% 7	5% 6%	14% 4	77%	8%	12% 3%
, and the second	Untested N	None Partial	Full	Untested No	ne Partial	Full L	Intested None	Partial	Full Unt	ested None	Partial Fi	Untested	None	Partial Full
its	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
books	67%	0%	0%	25%	19%	14%	15%	19%	5%	28%	0%	0%	0%	37%
e	1 Techniques	0 Techniques	1 Techniques	6 Techniques	12 Techniques	12 Techniques	22 Techniques	11 Techniques	14 Techniques	5 Techniques	4 Techniques	4 Techniques	3 Techniques	4 Techniques
ort	3 Procedures	0 Procedures	7 Procedures	67 Procedures	79 Procedures	90 Procedures	239 Procedures	93 Procedures	39 Procedures	18 Procedures	14 Procedures	27 Procedures	12 Procedures	19 Procedures
	Gather Victim Network Information		Valid Accounts	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in- the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in- the-Middle	Ingress Tool Transfer	Exfiltration Over Alternative Protocol	Data Destruction
				Inter-Process Communication	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Lateral Tool Transfer	Archive Collected Data	Non-Standard Port	Exfiltration Over C2 Channel	Data Encrypted for Impact
				Scheduled Task/Job	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs	Credentials from Password Stores	Domain Trust Discovery	Remote Service Session	Input Capture	Protocol Tunneling	Exfiltration Over Web Service	Inhibit System Recovery
				System Services	Boot or Logon	Boot or Logon	Deobfuscate/De	Forced Authentication	File and	Hijacking Remote Services	Screen Capture	Proxy	Web Service	Resource Hijacking
				User Execution Windows Management Instrumentation	Initialization Scripts	Autostart Execution	code Files or Information	Input Capture	Directory Discovery	Use Alternate				
					Create Account	Boot or Logon Initialization	File and Proces	Modify Authentication	Network Service Discovery					
					Create or Modify System Process	Scripts Create or Modify		Process Ne	Network Share Discovery					
					Event Triggered	System Process	Permissions Modification	Network Sniffing						

### Gartner. Peer Insights<sub>™</sub>

MITRE | ATT&CK\*



### **NetSPI Proactive Security Solutions**

#### **PTaaS**

Pentesting programs from Appsec to Al

- 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



### The Most Trusted Products, Services, and Brands Choose NetSPI

			20% of the Fortune 500
<b>Hewlett Packard</b> Enterprise	Microsoft	CHUBB	9/10 Top U.S. Banks
<b>C</b> GONG	🔀 Broadridge <sup>.</sup>	IHG HOTELS & RESORTS	3/5 Largest Global Healthcare Companies
			3/3 Largest Cloud Providers

"NetSPI is exemplary at penetration testing, dynamic application security testing, and breach and attack simulation..."

Craig Guiliano, Cyber Intelligence Officer, Chubb

#### **Recognized by:** Ò \* \* **Trusted Pentesting Security Expertise** Gartner **C**3EST **21K** engagements\* 4M assets tested\* FORRESTER<sup>®</sup> 1.5M vulnerabilities reported\* NetSPI U 20+ vears of testing **GIGAO**M OSCP OSCE CISSP Red Team

Ops 1

### Why Choose NetSPI as Your Trusted Partner

	People	<ul> <li>300+ in house security experts</li> <li>Rigorous methodology and consistent testing results</li> <li>Highly skilled deep bench with vast domain expertise</li> </ul>
	Process	<ul> <li>Programmatic approach with strategic guidance</li> <li>White glove customer support and advisory programs</li> </ul>
		<ul> <li>Dedicated client delivery management team</li> </ul>
		<ul> <li>Deep visibility and detailed risk assessment</li> </ul>
•	Technology	<ul> <li>Continuous testing and improvement</li> <li>Consistency, quality and result transparency</li> </ul>
		Consistency, quality and result transparency

"The significant thing that has changed every year we add more attack surface to be tested [by NetSPI ASM], but instead of [the number of ] vulnerabilities going up they're actually going down."

Nancy Brainerd, Senior Director and Deputy CISO, Medtronic



# Let's stay in touch!

#### Sam Kirkman

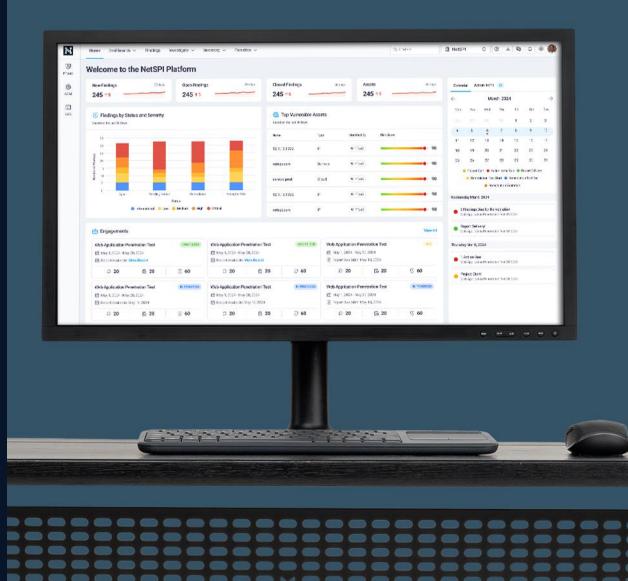
Director of Services, EMEA

sam.kirkman@netspi.com

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

241 N 5th Ave Suite 1200 Minneapolis, MN 55401

netspi.com



22