



Threat Exposure Management

Because 'Thoughts and Prayers' Isn't a Security Strategy

Presented By Sam Kirkman



Agenda

- The Dilemma: Products vs Solutions
- Proactive Security
- Communicating The Value
- Enabling Continuous Threat Exposure Management (CTEM)



Sam Kirkman

Director of Services, EMEA

Penetration Tester

Security Architect

Solution Engineer

Quality | Efficiency | Value

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

The Product-First Mindset

Vs.

The Solution-First Mindset





The Classic Approach

Objective: Prevent a successful ransomware attack

**Build list of required
products & deadlines**

**Procure Protection
Solution A**

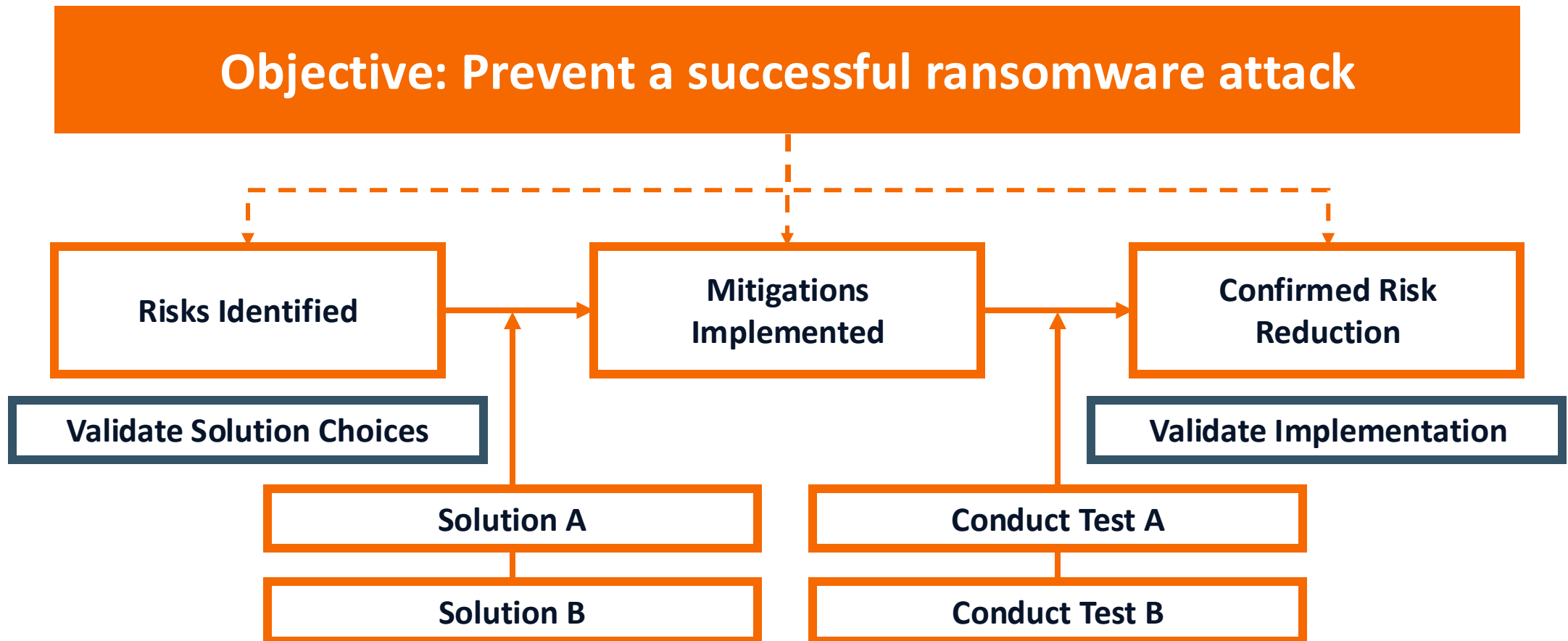
**Procure Protection
Solution B**

Install A+B rapidly

Actual risk reduction? Uncertain.



A Proactive Approach





Gartner

How to Manage Cybersecurity Threats, Not Episodes

“By 2026, organizations that prioritize their security investments based on a continuous exposure management program will be 3x less likely to suffer a breach.”

Continuous Threat Exposure Management (CTEM)



Medtronic: Shifting to Continuous Testing for Cyber Resilience



Situation

- Medtronic needed to protect its patients' data and intellectual property.
- They partnered with NetSPI since 2020 to conduct annual penetration testing and periodic spot checks.

Challenge

- The primary challenge was consistently identifying the attack surface and addressing vulnerabilities across a dynamic threat landscape.

Solution


- NetSPI shifted to a continuous approach to defining and monitoring the attack perimeter.
- This helped mitigate the risk of blind spots or overlooked vulnerabilities.

Results


- The shift resulted in a reduced number of vulnerabilities, even as the company's attack surface expanded.
- Together, we achieved better cyber resilience through proactive testing and mitigation efforts.

“The significant thing that has changed is every year we add more attack surface to be tested, but instead of the vulnerabilities going up, they’re actually going down.”

Nancy Brainerd, Senior Director and Deputy CISO



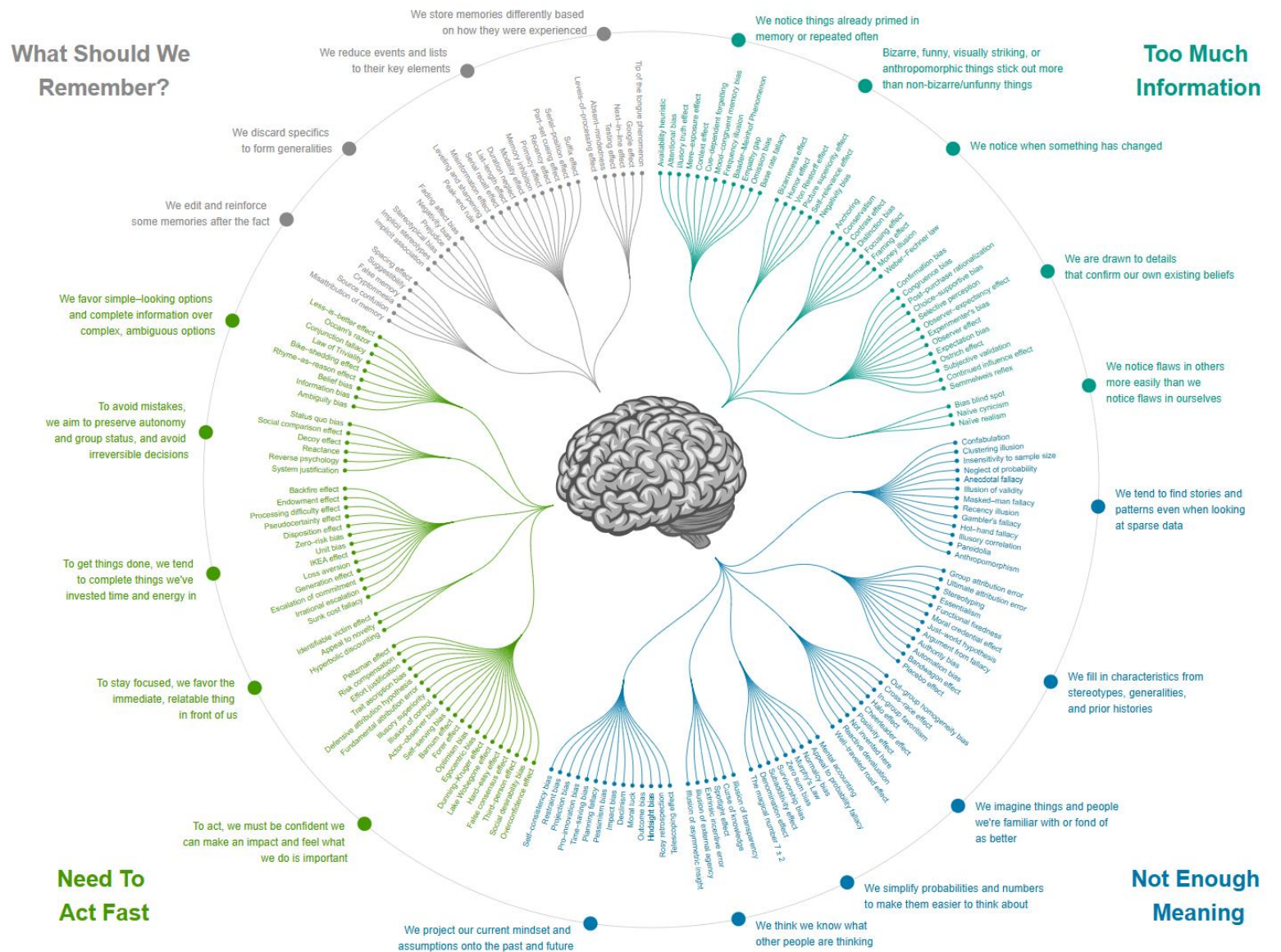
Key Takeaway:
**Continuous Threat Exposure
Management (CTEM) is the most
effective strategy to deliver positive
security outcomes.**



Decoding Communication



Cognitive Biases



https://upload.wikimedia.org/wikipedia/commons/6/65/Cognitive_bias_codex_en.svg

Same language, different perspectives

Audience	Primary Concerns	Communication Focus
Executive Leadership	Business impact, compliance, reputation	ROI, competitive advantage, risk reduction
Board of Directors	Governance, liability, shareholder value	Strategic risk, oversight responsibilities
Technical Teams	Implementation details, technical feasibility	Specific vulnerabilities, technical specifications
Operational Staff	Day-to-day procedures, usability, workload	Practical guidance, clear instructions
Finance/Procurement	Cost justification, budget constraints	TCO, cost-benefit analysis
Legal/Compliance	Regulatory requirements, legal exposure	Compliance frameworks, liability reduction
Customers/Public	Personal data security, service reliability	Trust, protection measures, transparency

Cialdini's Six Principles of Persuasion

01

Reciprocity

Offer value, before requesting action

02

Commitment

Ask for small commitments/agreements and build upon them.

03

Social Proof

Who else has taken this path?

04

Authority

Leverage frameworks, standards and other authoritative sources.

05

Liking

It's hard to agree with someone you don't like.

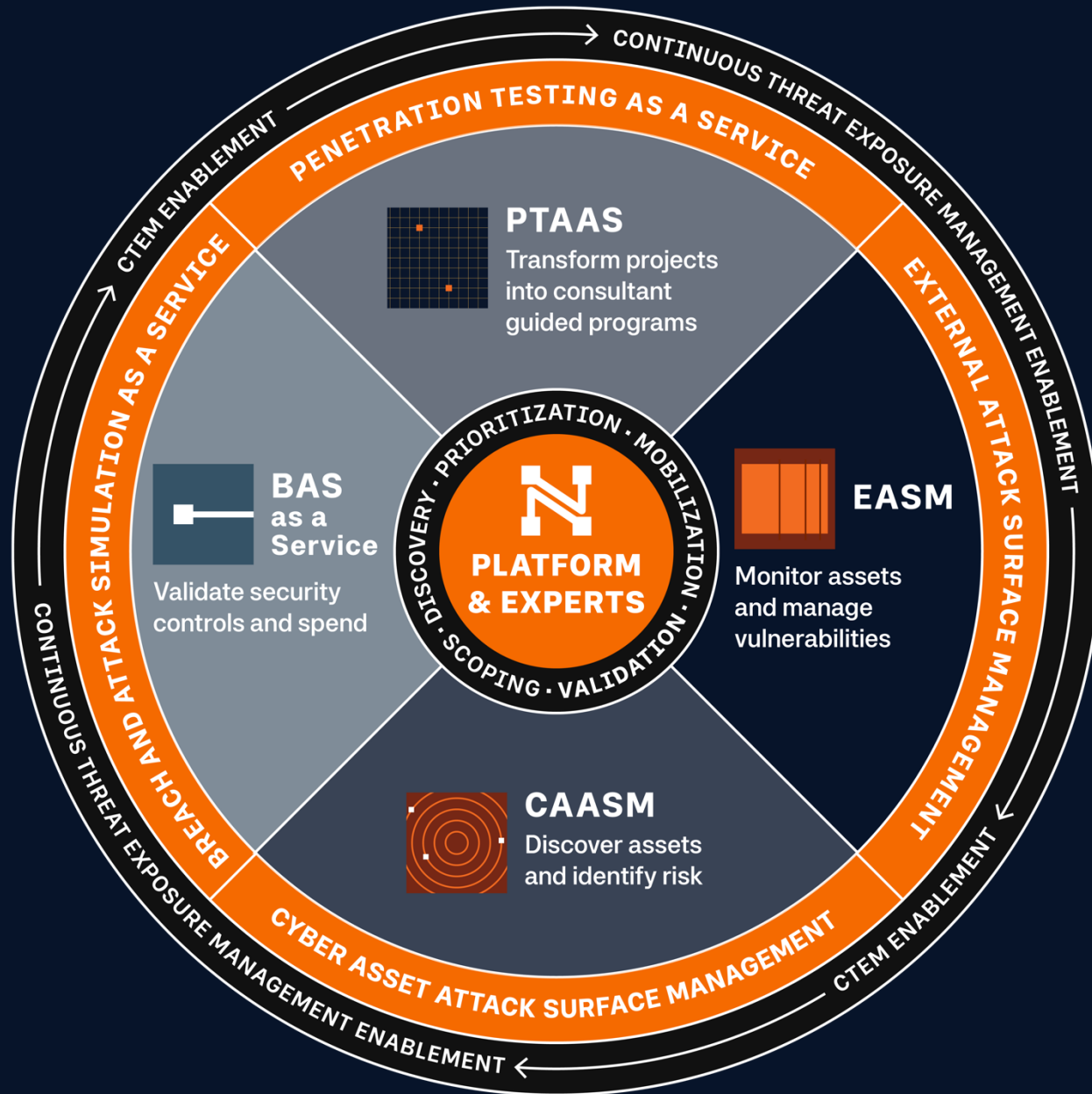
06

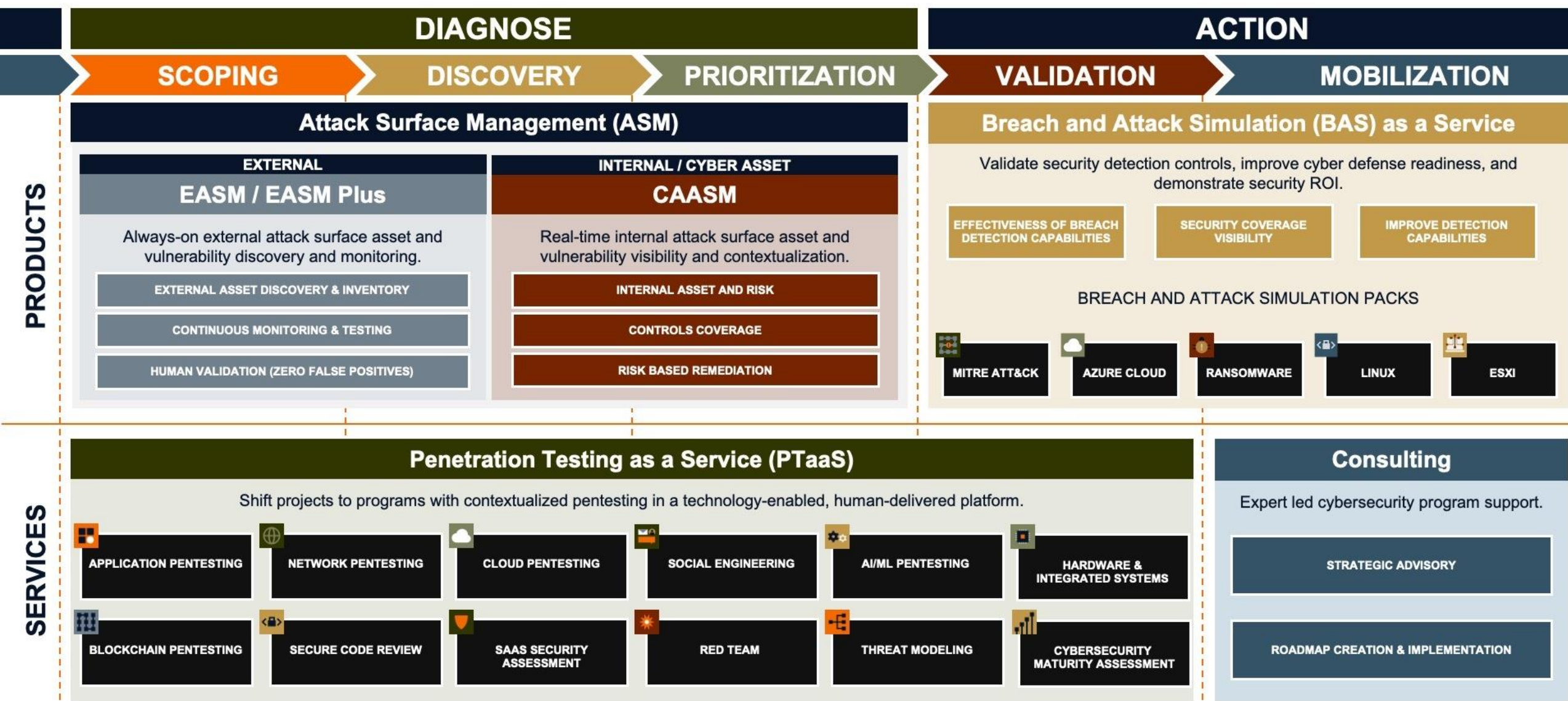
Scarcity

Resources are always finite. Why should we spend them here?

Same language, different perspectives, addressed

Stakeholder	Primary Concerns	Likely Objections	Persuasion Approach	Concession Options
Finance	ROI, cash flow	"Too expensive now"	Risk quantification, phased funding	Delayed implementation timeline, vendor financing
Technical	Integration, resources	"Team is overloaded"	Managed services option, implementation support	Phased rollout, shared resources
Executive	Business disruption	"Will slow operations"	Minimal-impact deployment, business benefits	After-hours implementation, tailored user experience
Operational	Unit-specific impact	"Not our priority"	Specific use cases, competitive advantage	Business-specific customization





Get a free copy of *Continuous Threat Exposure Management For Dummies, NetSPI Special Edition*

Sam Kirkman

Director of Services, EMEA

sam.kirkman@netspi.com

[https://www.linkedin.com/in/
sam-kirkman-cybersecurity/](https://www.linkedin.com/in/sam-kirkman-cybersecurity/)

241 N 5th Ave Suite 1200
Minneapolis, MN 55401

netspi.com



Visit Stand **B90** and grab an **Aperol Spritz!**