NetSPI

AI-pocalypse Averted: Emerging Services and Proactive Cloud Security

Nick Lynch, Principal Security Consultant

Clinical Theatre 2

12 March

16:20 – 16:35

Nick Lynch

Principal Security Consultant

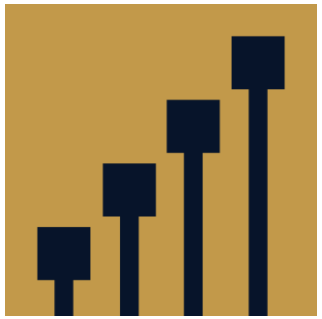
- Penetration tester
- Cloud specialist in AWS, Azure, and GCP
- Former cloud security engineer and architect

https://www.linkedin.com/in/nlynchnetspi/

What challenges await in Europe?

Legislation and Regulation

- DORA
- NIS 2



Geopolitical Drivers

- Dependencies
- Disruption

Emergent Technologies

- Non-deterministic AI
- Cloud

AI Service Considerations - Cloud

IDENTITY AND ACCESS MANAGEMENT

THREAT ACTORS

DATA SECURITY

AI Testing Categories

LLM WEB APPLICATION TESTING

LLM BENCHMARKING AND JAILBREAKING

CUSTOM AI SECURITY TESTING

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.

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

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

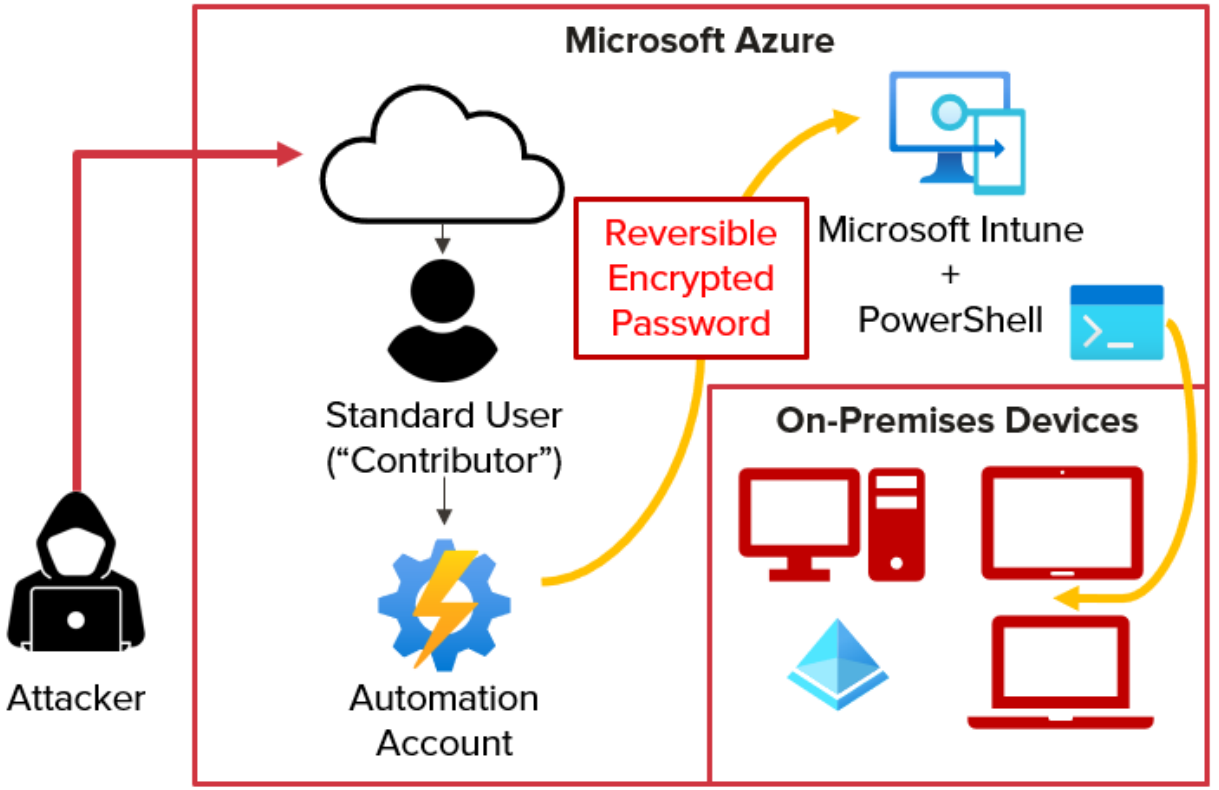
Azure Risk Identified

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



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

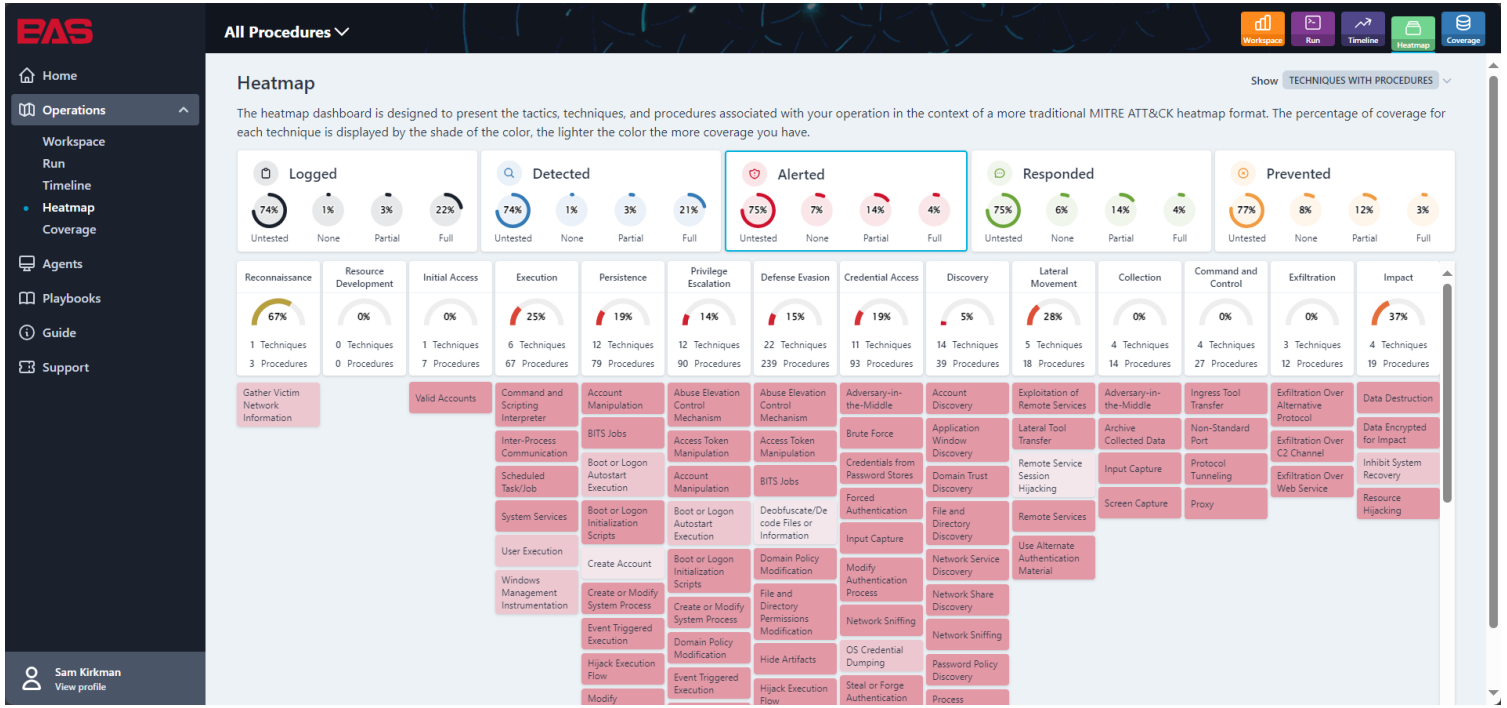
Risks Uncovered

- 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®

Continuous Automated Validation

Breach and Attack Simulation

- Not just for on-premises
  - NetSPI Azure BAS plays coming soon
  - Come talk to us to find out more

Visit Stand #cS092

netspi.com/emea

Nick Lynch

Principal Security Consultant, EMEA

nicholas.lynch@netspi.com

https://www.linkedin.com/in/nlynchnetspi/

241 N 5th Ave Suite 1200

Minneapolis, MN 55401

netspi.com