VECTRA
A SUBSIDIARY OF ENSIGN INFOSECURITY

From Reports to Results: Turning MITRE ATT&CK Insights into Actionable Security Programmes

How red teamers can bridge the gap between technical findings and executive decisions.

Shaun Burger

7th March 2025

Shaun Burger

Director of Cyber Assurance Vectra Corporation

- **Over 15 years** of experience collaborating with executive and leadership teams.
- **Certified Red Team Professional** with deep expertise in offensive security strategies.
- Extensive experience as both a **Red Team practitioner** and an executive-level leader, specialising in offensive security and strategic business decision-making.
- Regularly collaborates with boards and leadership teams to translate complex security insights into actionable decisions that drive measurable improvements.
- Passionate about leveraging **Red Team** data to influence and elevate organisational security maturity.
- **Based in Adelaide, Australia**, with a commitment to advancing cybersecurity on a global scale.

VECTRA
A SUBSIDIARY OF ENSIGN INFOSECURITY

Agenda

Introduction
Framing the challenge: Moving beyond static reporting.

The Problem with Point-in-Time Findings
Why traditional red team reports fall short.

Using ATT&CK for Actionable Outcomes
Leveraging the framework to prioritise, operationalise, and measure improvements.

Bridging the Gap Between Technical and Business
Translating red team insights into language beyond KPIs that leadership understands.

Case Study: Lessons from the Australian Hospital Engagement
How ATT&CK mapping influenced decisions and investment priorities.

Driving Organisational Change
Building continuous improvement cycles and aligning with broader security goals.

Call to Action
Practical steps for turning insights into impactful actions.

Q&A

VECTRA
A SUBSIDIARY OF ENSIGN INFOSECURITY

Transforming Reports into Continuous Growth

- **Static assessments hinder growth:** Reports rarely lead to ambitious, measurable goals for security improvement. How do we justify future budgets?
- **Disconnect between findings and actionable improvements:** Reports often stop at identifying vulnerabilities, leaving gaps in operationalisation.
- **OKRs (Objective Key Results) as a roadmap for improvement:** Enable teams to strive for meaningful progress aligned with organisational security goals.

A Framework for Setting and Achieving Security Goals

- **Attack emulation – case study – Australian hospital**
  - **APT40 (Kryptonite Panda, GINGHAM TYPHOON, Leviathan, Bronze Mohawk):** Assessed to conduct malicious cyber operations for the People's Republic of China's Ministry of State Security, APT40 has targeted organisations in various countries, including Australia. They rapidly exploit newly public vulnerabilities in widely used software, posing a significant threat to networks globally. INDUSTRIALCYBER.COAPT28 (Fancy Bear, Sofacy): A Russian state-sponsored group,
  - **APT28** has targeted healthcare sectors globally, including Australia, particularly during the COVID-19 pandemic, to steal information related to vaccine development and medical research. INDUSTRIALCYBER.COAPT29 (Cozy Bear, The Dukes): Another Russian state-sponsored group,
  - **APT29** has been involved in cyber-espionage campaigns targeting healthcare organisations to obtain COVID-19 research data.

VECTRA
A SUBSIDIARY OF ENSIGN INFOSECURITY

A Framework for Setting and Achieving Security Goals

- **Provides a structure for actionable objectives:**
  ATT&CK maps adversarial techniques, offering clarity for setting ambitious yet measurable goals. Provides a framework to quantify the concept of risk. Risk from where, from what and from who. Ensures language between red team and blue team is clearly understood allowing deeper collaboration. This is key to the MITRE ATT&CK framework – ensuring every stakeholder is talking the same language
- **Encourages ongoing progress:**
  Emulation exercises tied to OKRs ensure continuous testing, learning, and refinement.
- **Supports alignment with organisational strategy:**
  Helps define goals that bridge the gap between security improvements and business objectives.
- **Example OKR:**
- **Objective:** Improve detection of adversarial lateral movement.
  - Key Results:
    - Deploy detections for 5 MITRE ATT&CK techniques in the “Lateral Movement” category.
    - Reduce time to detect lateral movement from 1 hour to 10 minutes by Q2.

OKRs derived from ATT&CK empower leadership to track security team progress and justify investments in measurable terms.

VECTRA
A SUBSIDIARY OF ENSIGN INFOSECURITY

Case Study: Australian Hospital's Security Goals

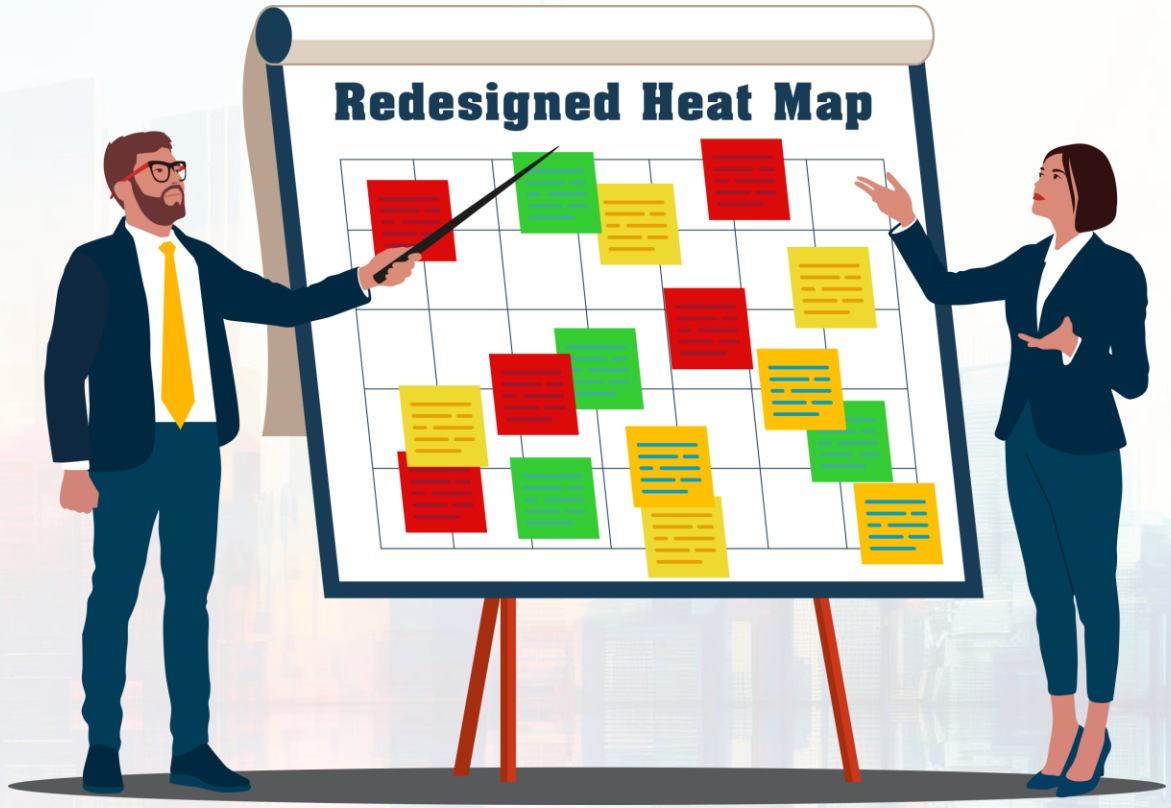
Objective: Reduce risk from legacy systems by implementing modern detection capabilities.

Key Results:

- Complete system refresh for all legacy infrastructure within six months.
- Emulate and block 10 ATT&CK-mapped techniques targeting legacy vulnerabilities.

Outcome: Progress measured through heat map updates, demonstrating reduced high-risk techniques over time.

Measurable growth visualised through heat maps demonstrated OKR progress to the board, aligning tactical improvements with broader risk reduction goals. Demonstrated ROI



VECTRA
A SUBSIDIARY OF ENSIGN INFOSECURITY

From Reactive Metrics to Proactive Goals

OKRs focus on what's possible:
Set ambitious objectives that drive improvement, rather than reflecting past performance.

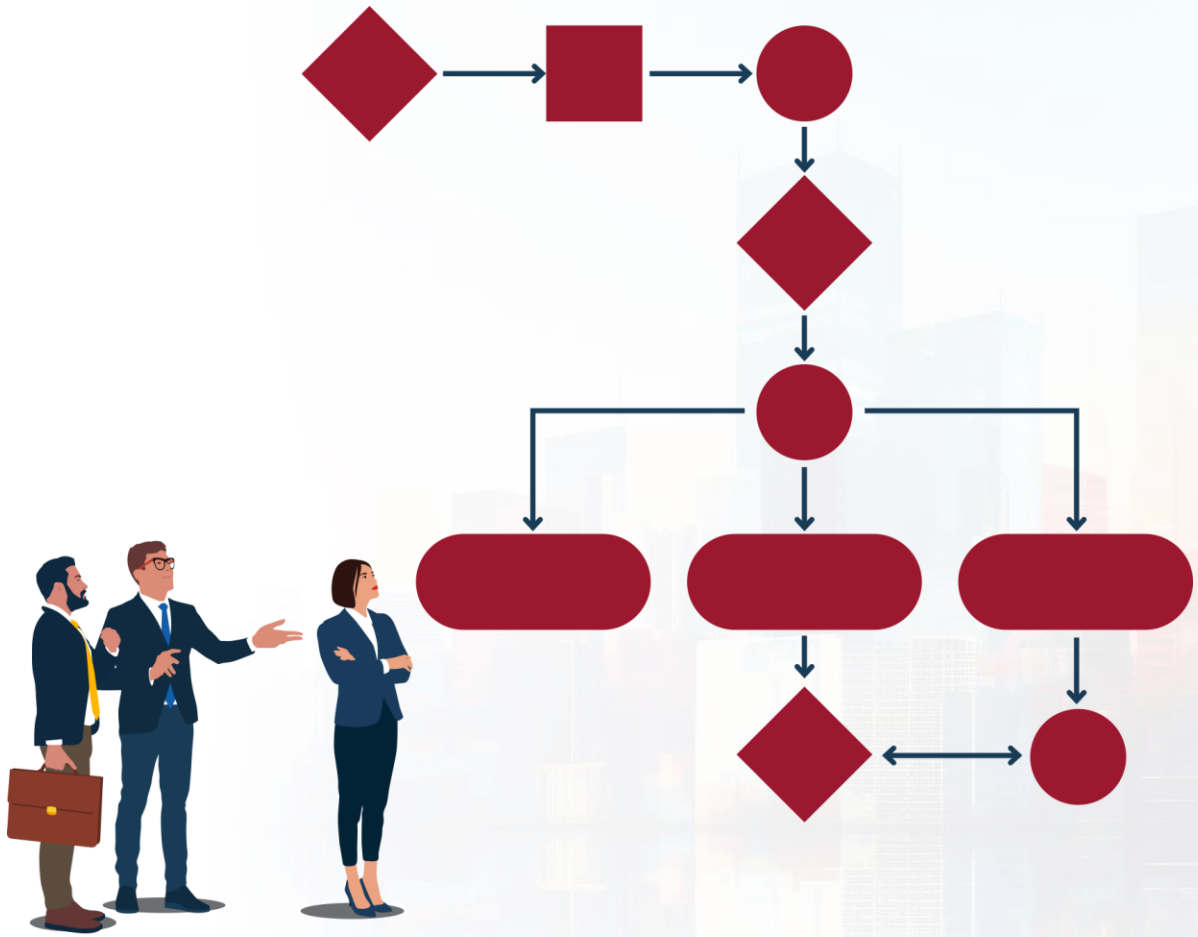
Example OKRs for Security Teams:

- **Objective:** Build resilience against initial access techniques.
- **Key Results:**
  - Simulate and detect 8 common phishing TTPs.
  - Implement 3 new email filtering controls to block malicious attachments.

Why OKRs outperform traditional KPIs:
Inspire teams to continuously improve, not settle for past benchmarks.

VECTRA
A SUBSIDIARY OF ENSIGN INFOSECURITY

Operationalising Adversarial Insights into Ambitious Goals



Leverage adversarial emulation to define OKRs: Use ATT&CK mappings to identify key areas for improvement and set meaningful objectives.

Example Objective: Improve SOC's ability to detect privilege escalation.

- **Key Results:**
  - Deploy 4 new detection rules targeting ATT&CK Privilege Escalation techniques.
  - Conduct adversarial simulations every quarter to validate detections.

Create iterative cycles for improvement: Continuously raise the bar with updated OKRs after each assessment.

VECTRA
A SUBSIDIARY OF ENSIGN INFOSECURITY

Connecting Goals to Organisational Priorities

Align security goals with business outcomes:
Set OKRs that demonstrate progress in reducing risks tied to critical business processes.

Example Objective: Strengthen resilience against ransomware.

- **Key Results:**
  - Implement multi-factor authentication across 100% of privileged accounts.
  - Block or detect 80% of ransomware TTPs emulated during red team exercises.

Demonstrate value to leadership:
Show how OKRs impact broader priorities like operational continuity and cost savings.

VECTRA
A SUBSIDIARY OF ENSIGN INFOSECURITY

Start Setting OKRs for Security Success

- **Define objectives tied to critical risks**:
  Focus on ambitious, actionable goals that align with your organisation's threat landscape.

- **Establish clear and measurable key results**:
  Example: “Detect 90% of emulated phishing campaigns within 5 minutes by Q4.”

- **Iterate and improve continually**:
  Use red team findings to reassess and update OKRs every quarter.

VECTRA
A SUBSIDIARY OF ENSIGN INFOSECURITY

VECTRA
A SUBSIDIARY OF ENSIGN INFOSECURITY

Q&A

Open for discussion on integrating OKRs into your security strategy.

VECTRA
A SUBSIDIARY OF ENSIGN INFOSECURITY

Thank you