Threat-Informed Detection Engineering for Critical Infrastructure

Turning Intelligence into Action for Resilience

Adarsh Lal - Security Operations Lead

CISO NZ | November 2025

About Adarsh

Namaskaram! Kia Ora!

From the tranquil backwaters of Kerala, South India, to the majestic landscapes of Aotearoa, New Zealand, I am a proud Kiwi with a deep respect and love for this land.

With almost 8 years dedicated to the cybersecurity domain, my journey has encompassed critical roles:

- Senior SOC Analyst
- Global SOC Manager
- Security Operations Lead

Why Critical Infrastructure is a Unique Target

Nation-State Threats

Advanced actors targeting OT/IT convergence with sophisticated campaigns

High-Impact Scenarios

Grid disruption, sabotage, and supply chain compromise threaten national security

Detection Gap

Traditional detection methods fall short against modern adversary tactics

Threat Intel Without Action = Shelfware

The Problem

- Most intel is reactive or disconnected
- Vendor-defined detections create noise
- No clear path from intelligence to action

The Solution

Translate threats → simulations → detections → controls

Transform intelligence into actionable defense

SOC's Response

Shift from Triage to Engineering

Build Hypotheses

Create detection hypotheses from threat intelligence

Validate

Test with adversary simulation tools

Automate

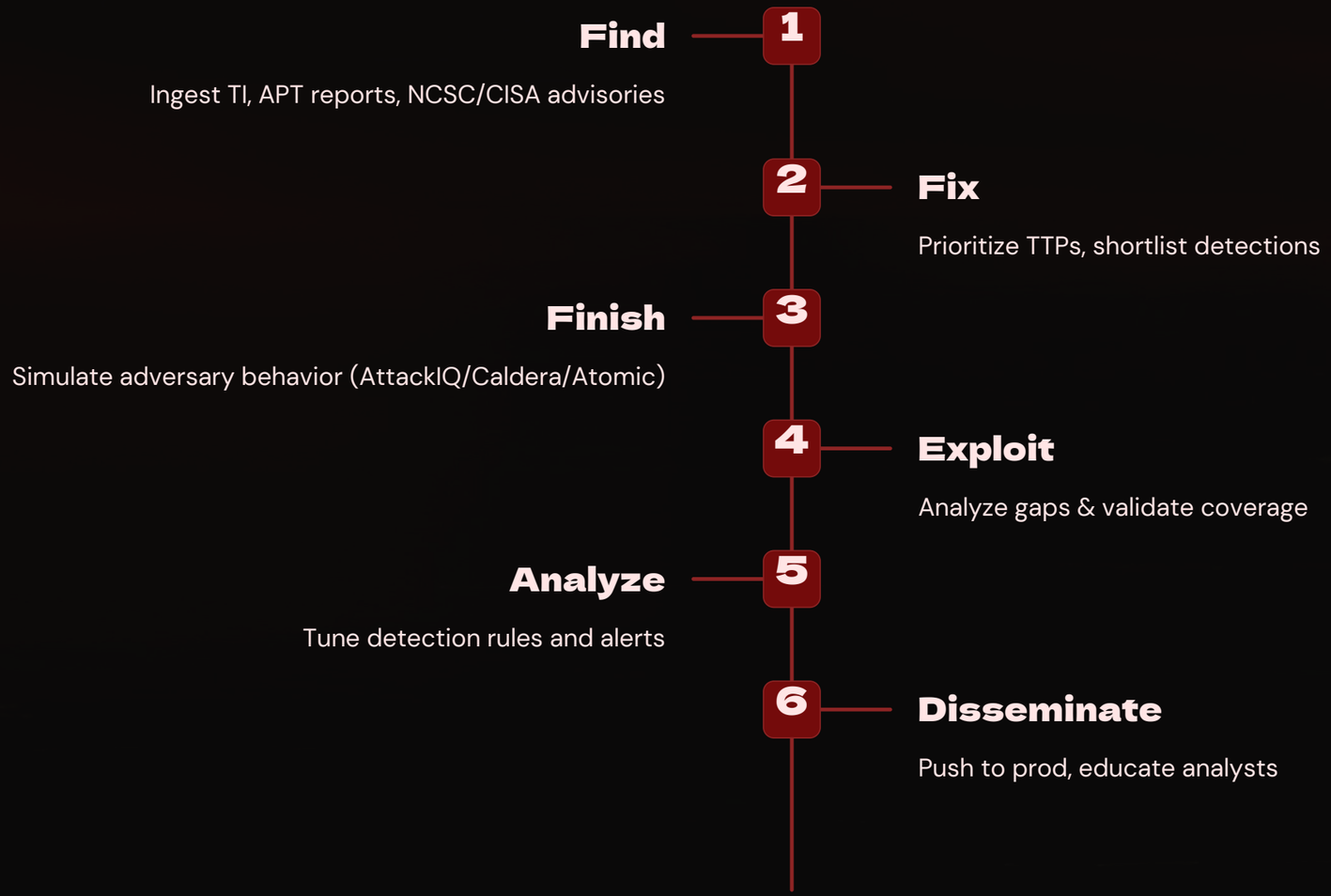
Deploy and iterate detections continuously

Align to Impact

Focus everything on CNI protection

F3EAD in Cyber Operations

Adapting Military Targeting Model to SOC



"I really recommen use F3EAD to stop reacting and start proactively engineering your visibility."

Detection Engineering Lifecycle

What Happens to a Detection Use Case in SOC

01

Backlog Entry

Threat use case enters the queue

02

Requirements Scoped

Custom detection requirements defined

03

Simulation Executed

Automated or custom simulation run

04

Coverage Reviewed

Detection effectiveness analyzed

05

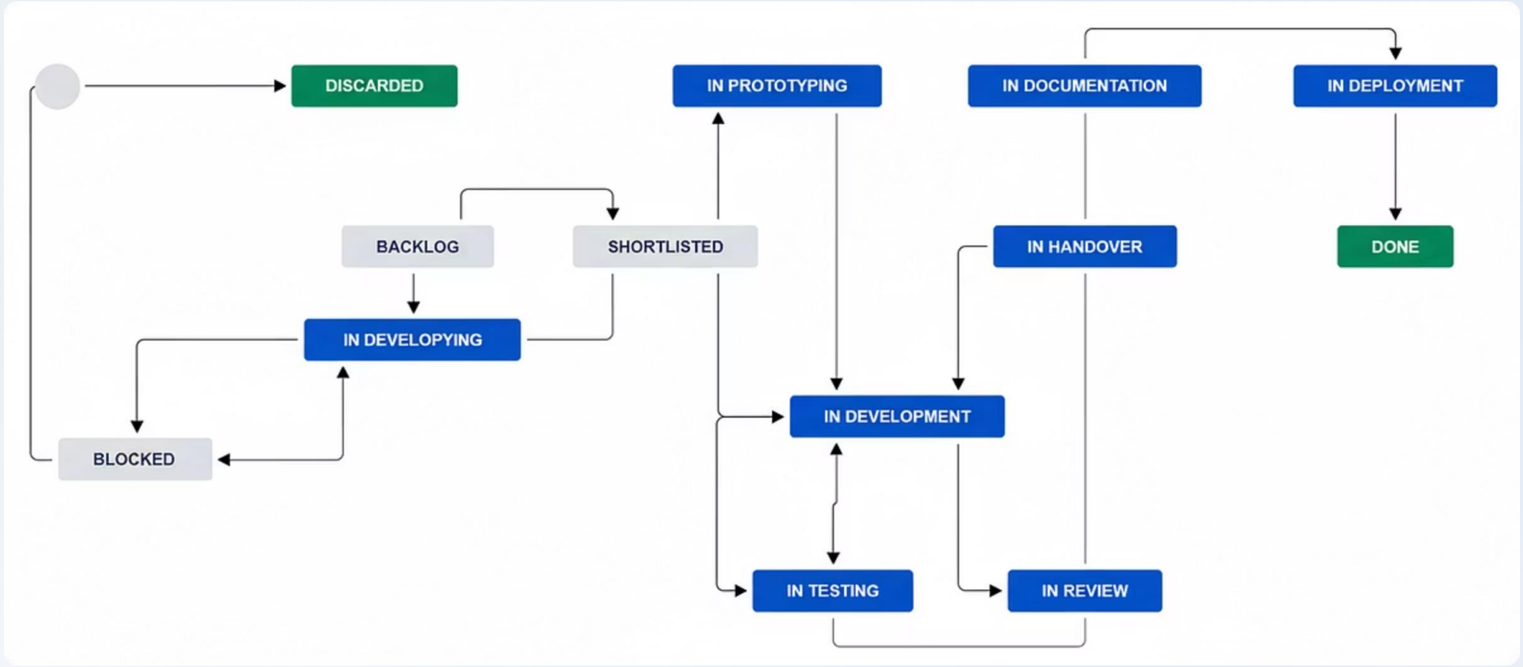
Gaps Filled

Tuning or hardening applied

06

Deployed

Rule documented and pushed to production



Workflow Snapshot

Workflow Meets Agile

Detection Engineering on your ticketing system

Status	Description
Backlog	Intake of TI or hunt ideas
Shortlisted	Prioritized & scoped
In Prototyping	Detection logic drafted
In Testing	Simulation being run
In Review	Peer or SME check
In Deployment	Rule going to production
Done	Detection deployed & monitored
Blocked	Telemetry gaps or system missing
Discarded	No business relevance

Threat Actor Techniques

Relevant to NZ Critical Infrastructure

Volt Typhoon & APT40

Chinese state-sponsored groups targeting critical infrastructure with living-off-the-land techniques

UNC3846

North Korean actors focusing on supply chain compromise and financial gain

Lapsus$

Global cybercriminal group using social engineering and extortion tactics

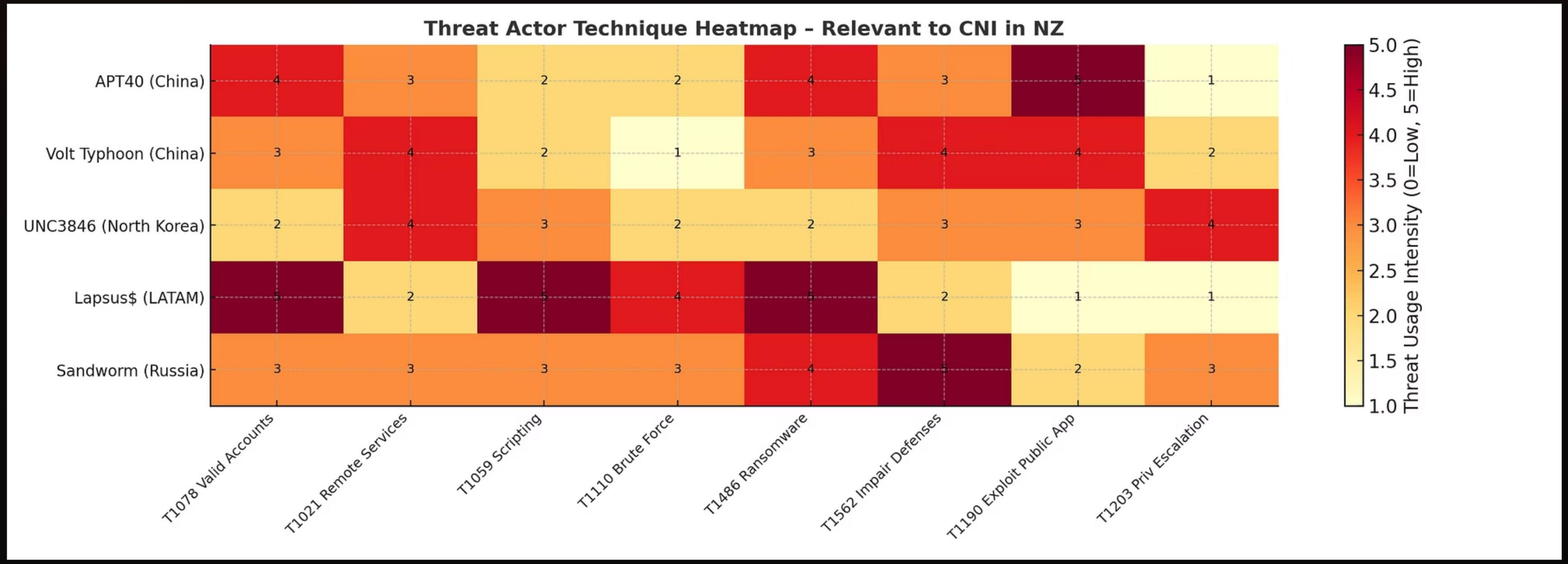
Sandworm

Russian military unit known for destructive attacks on infrastructure

Common Techniques: Valid Accounts, Remote Services, Brute Force, Ransomware, Impair Defenses

Threat Actor Technique Heatmap

Visualizing the most prevalent techniques against New Zealand's Critical Infrastructure.



High-Priority Logs Across IT and OT

Early Wins Without Full Telemetry

IT Logs

- Active Directory (authentication + privilege changes)
- Sysmon (execution visibility)
- Citrix & Jump Host access logs
- EDR Telemetry

OT Logs

- Historian events
- SCADA protocol traffic
- Authentication attempts on HMI
- Engineering Workstations

Focus on high-risk nodes and work inward. You don't need everything to start.

6-Month Governance & Refresh Cycle

Keeping Detection Strategy in Sync With Reality

Reassess Threats

Update top threats and actor TTPs

Stakeholder Review

Include OT engineering and IR teams

Update Coverage

Refresh heatmap and ATT&CK matrix

Audit Sources

Review log sources vs. detection coverage

Prioritize Backlog

Rank items based on real risk

"This keeps SOC grounded in the actual threat landscape - not stale assumptions."

Metrics That Matter

From Noise to Signal to Confidence

85%

Actor Coverage

High-priority actors covered by custom rules

14d

Deployment Time

Average detection-to-deployment cycle

2.3%

False Positive Rate

Per sprint across all detections

Additional Metrics: Rules per attack stage (Initial Access, Execution, Exfiltration) and OT vs. IT rule distribution

Lessons Learned

Over-Reliance on Vendors

Depended too heavily on vendor-provided detections instead of custom engineering

Poor Coverage Tracking

Lacked systematic approach to measure detection effectiveness across threat landscape

No Feedback Loop

Simulation results weren't feeding back into production detection improvements

The Fix

Detection Engineering Lifecycle + F3EAD enforcement created accountability and continuous improvement

Threat intelligence isn't just read

It's executed, simulated, and turned into resilient defense

Key Takeaways

1 **Use F3EAD Framework**

Transform threat intelligence into actionable decisions with military-proven methodology

2 **Let TTPs Guide Collection**

Adversary tactics determine which logs to collect, not vendor recommendations

3 **Simulate and Validate**

Test detections through adversary emulation-never assume they work

4 **Measure Resilience**

Focus on metrics that improve defense posture, not just alert volume

Q&A

Happy to Share Insights, Mistakes & Lessons

Thank you :)