COVENANT AEGIS REVIEW OF DEFENSE TECHNOLOGY VOL. 5 · NO. 2 · 2026 · PP. 5–24

Cyber Defense for Mission Systems: Threat Modelling, Detection and Resilient Operations

A. Petrov[1], N. Haddad[2], J. Romero[1], C. Mwangi[3]

[1]*Covenant Aegis Defense Division, Cyber Operations Laboratory*

[2]*Department of Computer Security, Partner Research Network*

[3]*Critical Infrastructure Resilience Group*

Received 20 Jan 2026 · Revised 5 Mar 2026 · Accepted 13 Mar 2026 · REVIEW ARTICLE · DOI 10.48-CA/deftech.2026.0521 ·
Corresponding author: a.petrov@covenantaegis.com

ABSTRACT

Background. Mission systems—command-and-control networks, weapon platforms and critical infrastructure—are high-value targets for sophisticated, persistent adversaries. **Objective.** To review the foundations of cyber defense for such systems and to argue that resilient mission assurance matters as much as prevention. **Methods.** Structured review of threat-modelling frameworks (kill chain, MITRE ATT&CK), detection paradigms, zero-trust and cyber-resilience engineering. **Results.** Signature detection is precise but blind to novelty; machine-learning anomaly detection underperforms operationally for well-characterised reasons; zero-trust limits lateral movement; and resilient architectures let forces fight through compromise. **Conclusion.** Effective defense combines ATT&CK-mapped layered detection, zero-trust segmentation, rehearsed response and assured mission resilience—the methodology Covenant Aegis applies.

Keywords: cyber defense; intrusion detection; MITRE ATT&CK; zero trust; mission assurance; threat hunting; resilience

1. Introduction

Adversary operations against defense and critical-infrastructure systems are persistent, well-resourced and increasingly automated. Effective cyber defense requires a disciplined understanding of adversary behaviour, layered detection, and architectures that keep functioning under partial compromise [1].

2. Threat Modelling

The intrusion kill chain decomposes intrusions into stages from reconnaissance to actions on objectives, enabling defenders to break the chain at multiple points [1]. The MITRE ATT&CK knowledge base catalogues real-world adversary tactics and techniques, providing a common language for detection coverage, red-teaming and gap analysis [2]. Table 1 maps kill-chain phases to defensive opportunities.

Table 1. Kill-chain phases and corresponding defensive actions [1,2].

Phase	Adversary goal	Defensive action
Recon	Target selection	Attack-surface reduction
Initial access	Foothold	MFA, email defense
Lateral movement	Spread	Segmentation, zero trust
Exfiltration	Data theft	DLP, egress monitoring
Impact	Disruption	Resilient recovery

3. Detection

3.1 Signatures and Anomalies

Signature detection is precise for known threats but blind to novel ones; anomaly detection promises to catch the unknown but is constrained by the difficulty of defining "normal" in complex, non-stationary networks. Sommer and Paxson explain why ML anomaly detection that excels elsewhere struggles operationally: the cost of false positives, the semantic gap between anomalies and incidents, and scarce representative data [3].

3.2 Threat Hunting

Proactive, hypothesis-driven hunting guided by ATT&CK surfaces stealthy intrusions that evade alerts and feeds new detections back into the pipeline [2]. Figure 1 contrasts detection coverage across approaches.

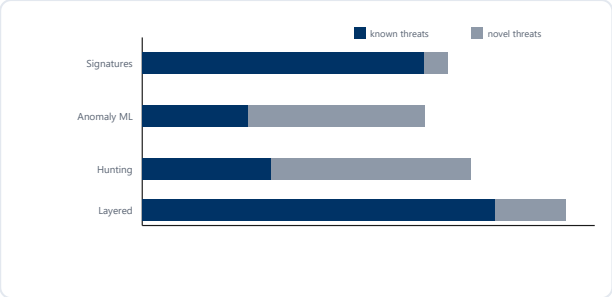


Figure 1. Schematic detection coverage: signatures excel at known threats; anomaly ML and hunting extend toward novel activity at higher analyst cost; a layered programme maximises overall coverage [2,3]. Illustrative.

4. Resilient Architecture

Zero-trust architecture replaces implicit network trust with continuous, per-request authentication and least-privilege access, limiting lateral movement after a breach [4]. Defense in depth, segmentation and assume-breach design reduce blast radius. For mission systems the goal is cyber resilience—the ability to anticipate, withstand, recover from and adapt to compromise—codified in resilience-engineering frameworks [5].

5. Response and Mission Assurance

Incident response follows a structured lifecycle of preparation, detection and analysis, containment, eradication, recovery and lessons learned [6]. For operational systems, response must preserve mission function: graceful degradation, manual fallbacks and pre-planned reconstitution allow forces to fight through an attack rather than halt.

6. The Covenant Aegis Methodology

Our methodology maps detection coverage to ATT&CK, applies zero-trust segmentation to mission networks, combines signature, behavioural and hunting layers with tuned alerting to control false positives, and validates resilience through adversary emulation and tabletop exercises. Continuous monitoring and post-incident review close the loop.

7. Discussion and Limitations

The base-rate problem and non-stationarity bound the realistic accuracy of automated detection; resilience and rehearsed response therefore carry disproportionate weight. Operational-technology and weapon-platform constraints (legacy, real-time, safety-critical) further limit standard IT controls and demand tailored engineering.

8. Conclusion

Cyber defense of mission systems rests on rigorous threat modelling, layered and realistically tuned detection, zero-trust resilient architecture and rehearsed response. Machine learning augments but does not replace these foundations; assured mission resilience is the decisive objective.

References

1. Hutchins EM, Cloppert MJ, Amin RM. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*. 2011.
2. Strom BE, et al. MITRE ATT&CK: Design and Philosophy. MITRE Technical Report; 2018 (updated 2020).
3. Sommer R, Paxson V. Outside the closed world: on using machine learning for network intrusion detection. *IEEE S&P*. 2010:305–316.
4. Rose S, Borchert O, Mitchell S, Connelly S. Zero Trust Architecture. NIST Special Publication 800-207; 2020.
5. Ross R, Pillitteri V, Graubart R, et al. Developing Cyber-Resilient Systems. NIST SP 800-160 Vol. 2 Rev. 1; 2021.
6. Cichonski P, Millar T, Grance T, Scarfone K. Computer Security Incident Handling Guide. NIST SP 800-61 Rev. 2; 2012.

9. ATT&CK-Driven Detection Engineering

The MITRE ATT&CK knowledge base structures detection engineering by enumerating adversary tactics and techniques observed in the wild [A1]. Defenders map their telemetry and analytics to techniques, measure coverage, and prioritise gaps by adversary prevalence and impact. ATT&CK also underpins adversary emulation and purple-teaming, in which red and blue teams jointly exercise and improve detections. Table A1 lists representative tactics and corresponding data sources.

Table A1. Selected ATT&CK tactics and high-value telemetry [A1].

Tactic	Example technique	Telemetry
Initial access	Phishing	Email, proxy
Execution	Scripting	Process, EDR
Persistence	Scheduled task	Registry, audit
Lateral movement	Remote services	Auth, netflow
Exfiltration	C2 channel	DNS, egress

10. Zero-Trust Architecture

Zero trust replaces perimeter trust with continuous verification: every request is authenticated, authorised and encrypted on the basis of identity, device posture and context, enforced at a policy decision/enforcement point [A2]. For mission systems this contains lateral movement and limits blast radius after a foothold. Microsegmentation, strong identity, device attestation and least privilege are the core mechanisms. Figure A1 contrasts attacker lateral reach under perimeter versus zero-trust models.

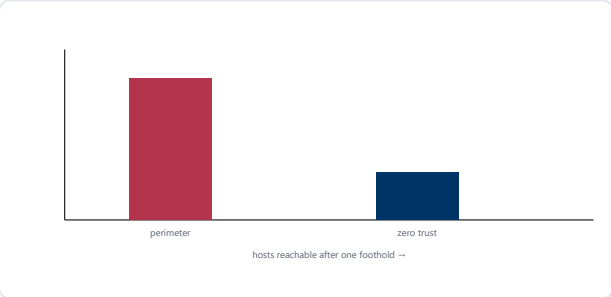


Figure A1. Schematic: zero-trust segmentation sharply reduces the number of systems an attacker can reach from a single compromised host [A2]. Conceptual.

11. Cyber Resilience Engineering

Resilience is the capacity to anticipate, withstand, recover from and adapt to adverse cyber events. NIST SP 800-160 Vol. 2 codifies resilience techniques—segmentation, redundancy, diversity, deception, non-persistence and analytic monitoring—as engineering controls [A3]. For mission systems the design goal is to fight through compromise: graceful degradation, manual fallbacks and pre-planned reconstitution preserve essential function even when parts of the system are denied.

12. Operational Technology and Weapon Platforms

Mission and infrastructure systems often include operational-technology (OT) and embedded components with real-time and safety constraints that preclude standard IT controls. The Purdue model and OT-specific guidance inform segmentation between enterprise IT and control networks [A4]. Legacy, long-lifecycle and safety-critical platforms require tailored monitoring, rigorous change control and supply-chain assurance rather than wholesale adoption of enterprise tooling.

13. Incident Response and Recovery

Structured incident response follows preparation, detection and analysis, containment, eradication, recovery, and post-incident review [A5]. For operational systems, response plans must protect mission continuity, defining degraded-mode operations and reconstitution sequences in advance. Rehearsal through tabletop and live exercises converts plans into capability, ensuring decisions under attack are made by plan rather than improvisation.

14. Threat Intelligence and Supply Chain

Cyber threat intelligence contextualises detection with adversary tradecraft and indicators, while software-supply-chain

security—provenance, signing and bill-of-materials—addresses a vector exploited in high-profile compromises. Defending mission systems requires assurance not only of the system but of the tools, dependencies and update channels that build and maintain it.

15. Future Directions

Priorities include automation of detection engineering against an evolving ATT&CK corpus, robust analytics that respect the base-rate constraint, resilience metrics tied to mission outcomes, and assured autonomy for response. The decisive measure is sustained mission function under active, capable adversaries.

Extended References

7. Strom BE, et al. MITRE ATT&CK: Design and Philosophy. MITRE; 2018 (updated 2020).
8. Rose S, et al. Zero Trust Architecture. NIST SP 800-207; 2020.
9. Ross R, et al. Developing Cyber-Resilient Systems. NIST SP 800-160 Vol. 2 Rev. 1; 2021.
10. Stouffer K, et al. Guide to Operational Technology (OT) Security. NIST SP 800-82 Rev. 3; 2023.
11. Cichonski P, et al. Computer Security Incident Handling Guide. NIST SP 800-61 Rev. 2; 2012.

Author contributions: AP and NH structured the review; JR and CM analysed detection and resilience; all authors revised. **Funding:** Covenant Aegis Defense Division. **Competing interests:** Authors are affiliated with Covenant Aegis.

© 2026 Covenant Aegis Defense Division. This review synthesises publicly available literature and NIST/MITRE frameworks for defensive cybersecurity; figures are illustrative. For professional and educational use.