COVENANT AEGIS REVIEW OF CYBERSECURITY VOL. 6 · NO. 2 · 2026 · PP. 6–25

Network Monitoring and Anomaly Detection: Telemetry, Machine Learning and Operational Reality

C. Mwangi[1], A. Petrov[1], P. Vasquez[2], N. Haddad[3]

[1]*Covenant Aegis Cybersecurity Division, Network Defense Laboratory*

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

[3]*Security Operations Research Group*

Received 17 Jan 2026 · Revised 4 Mar 2026 · Accepted 12 Mar 2026 · REVIEW ARTICLE · DOI 10.48-CA/cyber.2026.0621 ·
Corresponding author: c.mwangi@covenantaegis.com

ABSTRACT

Background. Network monitoring provides the visibility on which detection, response and forensics depend, but operational reality constrains what analytics can deliver. **Objective.** To review telemetry sources, the spectrum from signatures to ML anomaly detection, and the base-rate and encryption constraints that govern usefulness. **Methods.** Structured review of monitoring architecture and the intrusion-detection literature. **Results.** Signatures are precise but blind to novelty; ML anomaly detection underperforms operationally for well-documented reasons; and the base-rate fallacy means that even a 99%-accurate detector yields overwhelming false positives at realistic intrusion prevalence. **Conclusion.** Sustainable detection optimises positive predictive value and analyst workload, combines signatures, behaviour and hunting, and is engineered against the base-rate and encryption realities—the Covenant Aegis methodology.

Keywords: network monitoring; intrusion detection; anomaly detection; NetFlow; base-rate fallacy; SOC; encrypted traffic

1. Introduction

Defenders cannot protect what they cannot see. Network monitoring supplies the observations—who talked to whom, when, how and with what content—that underpin intrusion detection, threat hunting and investigation. Designing monitoring that yields actionable signal without overwhelming analysts is the core challenge [1].

2. Telemetry and Architecture

Monitoring draws on complementary sources: flow records (NetFlow/IPFIX) summarising connections at scale; deep packet and protocol analysis, exemplified by the Zeek/Bro framework [2]; and host, endpoint and identity logs. A modern architecture centralises and correlates these, balancing retention, cost and the privacy implications of collection.

3. Detection Approaches

3.1 Signatures

Rule- and signature-based systems such as Snort and Suricata reliably flag known patterns with low false positives but cannot detect novel behaviour [3].

3.2 Statistical and Machine Learning

Anomaly detection models a baseline of normal activity and flags deviations. Sommer and Paxson's influential critique explains why this underperforms in operational intrusion detection: the diversity and non-stationarity of normal traffic, the semantic gap between a statistical anomaly and a security incident, scarce labelled data, and the asymmetric cost of errors [4].

4. The Base-Rate Problem

Axelsson showed that because genuine intrusions are extremely rare relative to benign events, even a highly accurate detector produces overwhelming false positives—the base-rate fallacy that dominates the usefulness of intrusion detection [5]. Table 1 and Figure 1 make this concrete: at a 0.1% event rate, a detector with 99% sensitivity and 99% specificity still yields a PPV near 9%.

Table 1. PPV at sensitivity 99%, specificity 99%, by intrusion base rate (per 100,000 events).

Base rate	True+	False+	PPV
1%	990	990	50%
0.1%	99	999	9.0%
0.01%	10	1000	0.9%

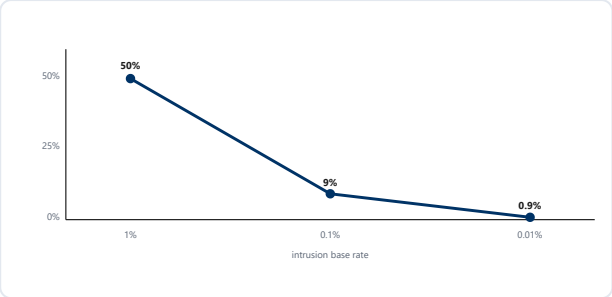


Figure 1. Positive predictive value collapses as intrusion base rate falls, at fixed 99% sensitivity/specificity—the quantitative core of alert fatigue [5]. Computed from Table 1.

5. The Encryption Trend

Pervasive transport encryption limits payload inspection, shifting detection toward metadata, flow features and TLS fingerprinting, and raising the value of host and identity telemetry. Encrypted-traffic analysis can identify malware behaviour from observable patterns without decryption, but with inherent limits [6].

6. Operational Principles

Effective monitoring favours high-fidelity, context-rich detections over volume; combines signatures, behavioural analytics and threat hunting; tunes aggressively to control false positives; and measures success by mean time to detect and respond rather than alert counts. Detection engineering mapped to adversary techniques keeps coverage aligned with real threats.

7. The Covenant Aegis Methodology

We instrument flow, protocol and host telemetry into a correlated analytics layer, prioritise precision and context to protect analyst attention, and continuously

validate detections through adversary emulation. Monitoring is treated as an engineering discipline with explicit coverage, quality and response-time objectives.

8. Discussion and Conclusion

The base-rate problem and non-stationarity bound realistic detector usefulness; machine learning is a component, not a panacea. Sustainable, high-precision detection that respects these constraints—and the encryption trend—wins in operations.

References

1. Bejtlich R. *The Practice of Network Security Monitoring*. No Starch Press; 2013.
2. Paxson V. Bro: a system for detecting network intruders in real-time. *Comput Netw*. 1999;31(23–24):2435–2463.
3. Roesch M. Snort: lightweight intrusion detection for networks. *USENIX LISA*. 1999:229–238.
4. Sommer R, Paxson V. Outside the closed world: on using machine learning for network intrusion detection. *IEEE S&P*. 2010:305–316.
5. Axelsson S. The base-rate fallacy and the difficulty of intrusion detection. *ACM Trans Inf Syst Secur*. 2000;3(3):186–205.
6. Anderson B, McGrew D. Identifying encrypted malware traffic with contextual flow data. *ACM AISec*. 2016:35–46.

9. Telemetry Sources in Depth

Effective monitoring layers complementary data. Flow records (NetFlow/IPFIX) scale to high-volume backbones and reveal communication structure; full packet capture provides content and protocol detail at high storage cost; protocol-aware analysis frameworks such as Zeek produce rich, structured transaction logs [A1]. Endpoint detection and response (EDR) and identity logs are increasingly decisive as encryption limits network payload visibility. Table A1 compares sources by fidelity, cost and scalability.

Table A1. Monitoring telemetry sources.

Source	Fidelity	Cost/scale
Flow (NetFlow)	Low (metadata)	Excellent
Packet capture	High	Expensive
Zeek logs	Medium-high	Good
EDR / host	High (host)	Good

10. Why ML Anomaly Detection Is Hard Operationally

Sommer and Paxson's analysis remains the definitive account: intrusion detection differs from domains where ML excels because the cost of errors is highly asymmetric, "normal" traffic is enormously diverse and non-stationary, labelled attack data are scarce, and the gap between a statistical anomaly and a security-relevant event is large [A2]. The consequence is that anomaly detectors that look strong on static benchmarks often produce unmanageable false positives in production. Realistic deployment uses anomaly detection narrowly, for well-characterised behaviours, with heavy contextual enrichment.

11. The Base-Rate Problem, Quantified

Axelsson formalised why intrusion detection is dominated by the base-rate

fallacy: at realistic intrusion prevalence, even very high accuracy yields low positive predictive value, so analysts drown in false positives [A3]. Figure A1 plots required specificity to maintain a target PPV as base rate falls—an exacting constraint that explains the centrality of precision and alert triage over raw detection rate.

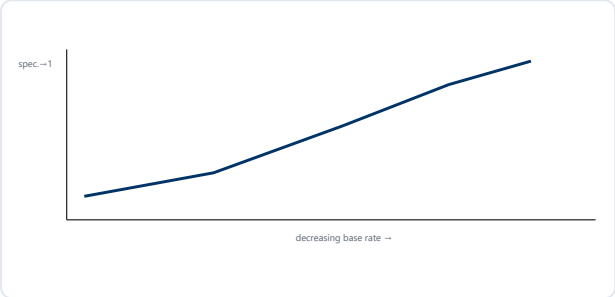


Figure A1. Schematic: as intrusion base rate falls, the specificity required to maintain a usable PPV approaches 1, an exacting operational constraint [A3]. Conceptual.

12. Encrypted-Traffic Analysis

With most traffic encrypted, detection shifts to metadata: flow features, packet-size and timing sequences, TLS handshake fingerprints (e.g., JA3-style) and certificate characteristics. Research shows malware family and behaviour can often be inferred from such observable features without decryption [A4]. Limits are real—benign and malicious encrypted flows overlap—so encrypted-traffic analysis augments host and identity telemetry rather than replacing it. Wholesale TLS interception carries security and privacy costs that must be weighed.

13. SOC Operations and Detection Engineering

Sustainable monitoring is an engineering and human-process discipline. Detections are written, tested and version-controlled, mapped to ATT&CK for coverage measurement, and tuned to control false positives. Alerts are enriched with asset and identity context and triaged by severity. Key metrics are mean time to detect and respond and detection coverage —not alert volume. Analyst cognitive load is a first-order design constraint [A5].

14. Privacy, Legal and Governance Considerations

Network monitoring collects potentially sensitive data, raising legal and privacy obligations that vary by jurisdiction and sector. Governance defines retention, access control, minimisation and audit, and balances visibility against intrusion. In regulated and multinational environments these constraints materially shape what telemetry may be collected and retained.

15. Future Directions

Priorities include privacy-preserving analytics over encrypted traffic, robust detection that respects the base-rate constraint, automated detection-engineering pipelines, and tighter fusion of network, host and identity telemetry. Sustainable, high-precision detection

aligned to adversary behaviour—not maximal alerting—remains the goal.

Extended References

7. Paxson V. Bro: a system for detecting network intruders in real-time. *Comput Netw*. 1999;31(23–24):2435–2463.
8. Sommer R, Paxson V. Outside the closed world: on using ML for network intrusion detection. *IEEE S&P*. 2010:305–316.
9. Axelsson S. The base-rate fallacy and the difficulty of intrusion detection. *ACM TISSEC*. 2000;3(3):186–205.
10. Anderson B, McGrew D. Identifying encrypted malware traffic with contextual flow data. *ACM AISec*. 2016:35–46.
11. Hassan WU, et al. Reducing alert fatigue via provenance-based triage. (NDSS / related SOC research). 2019.

Author contributions: CM led the review; AP and PV analysed detection methods; NH contributed SOC operations. All authors revised. **Funding:** Covenant Aegis Cybersecurity Division. **Competing interests:** Authors are affiliated with Covenant Aegis.

© 2026 Covenant Aegis Cybersecurity Division. This review synthesises publicly available peer-reviewed literature; figures computed from stated assumptions. For professional and educational use.