snare
A PROPHECY SOLUTION

From Noise to Signal: Building a Better Event Logging Strategy

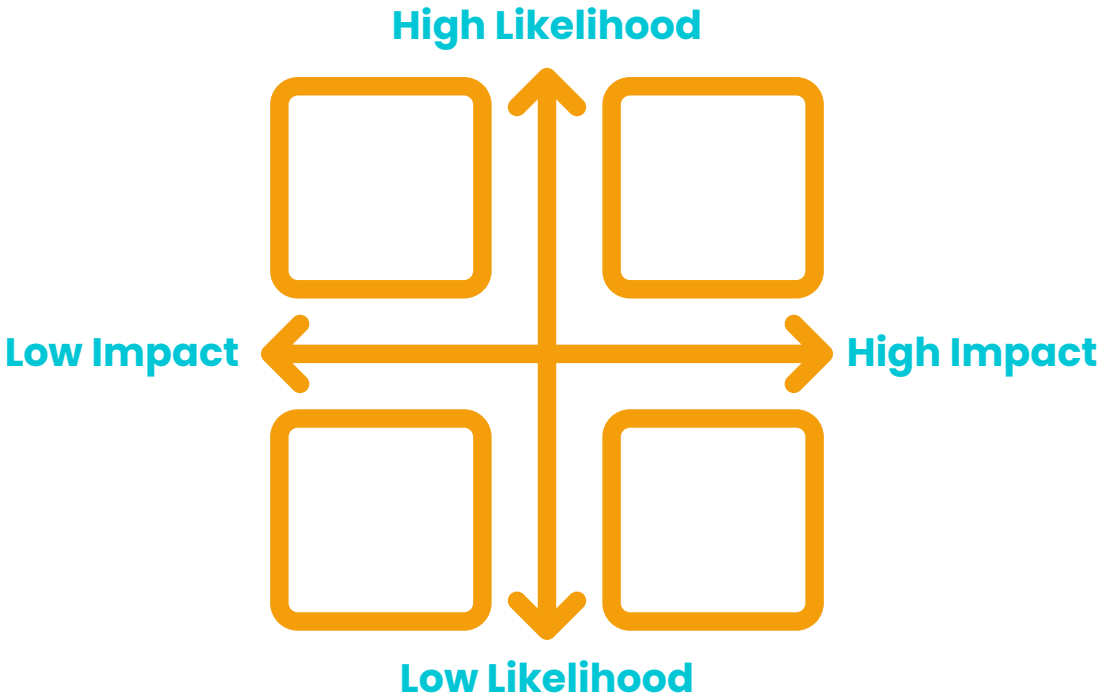
A Practical eBook for Security Leaders, SOC Teams & CISOs

Step 1: Map Your Critical Assets & Use Cases

Before you even think about which logs to collect, you need to know **what matters most** to your organisation. Not all systems or events carry the same weight, and logging everything indiscriminately leads to spiralling SIEM costs and an ocean of noise.

Best Practices:

- Identify **mission-critical systems**: authentication systems (Active Directory, Okta), privileged access platforms, cloud infrastructure APIs (AWS, Azure, GCP), and business-critical applications.
- Map **high-value use cases**: insider threat detection, privileged misuse, patch validation, regulatory audit, and incident investigation.
- Use a **logging priority matrix**: rank logs by business impact (High/Medium/Low) and likelihood of being exploited.
- Know your **compliance obligations for log collection** and retention — align your strategy with industry and regulatory requirements from day one.



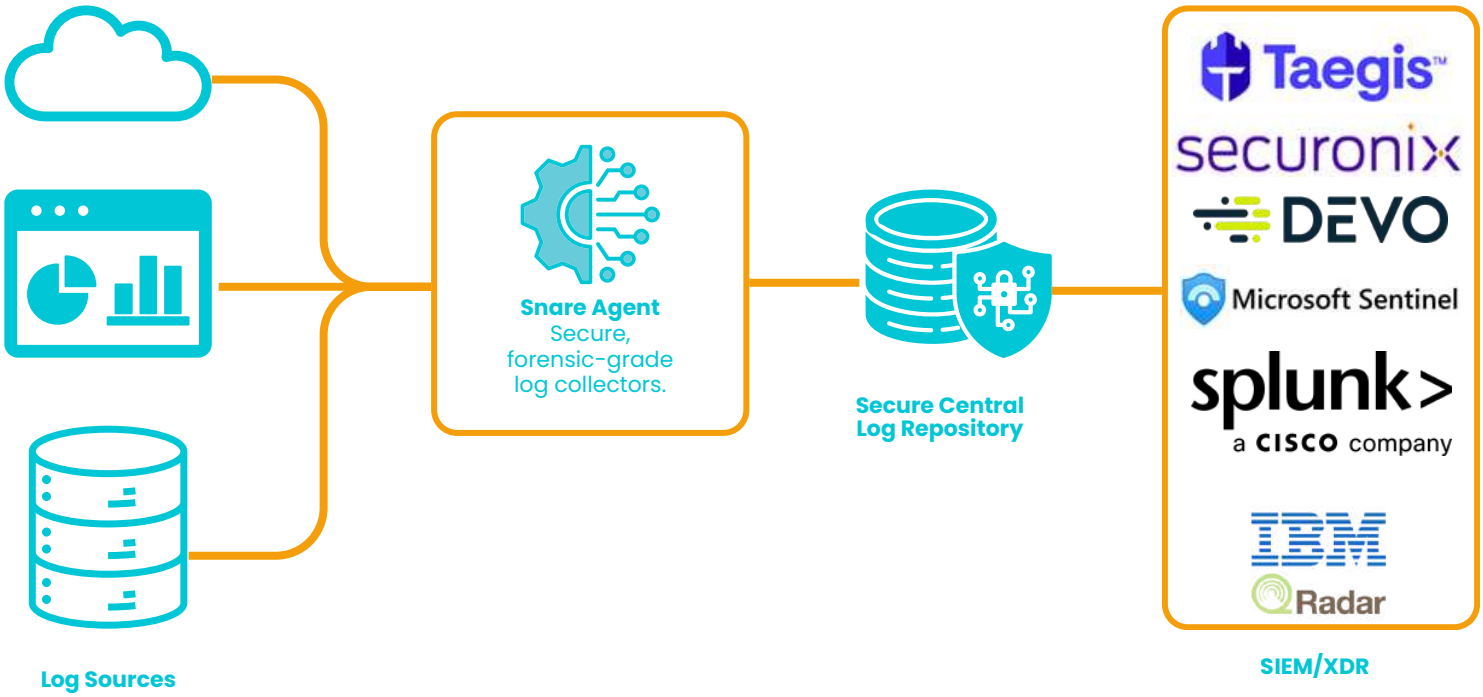
Step 2: Deploy a Trusted Collection Layer

Native OS and application logs are often too noisy, can be lost or tampered with. **A trusted collection layer** ensures your logs are forensic-grade and are delivered to the central location securely and reliably.

Best Practices:

- Use lightweight agents (like Snare) to gather a variety of log types without slowing down endpoints.
- Centralise log storage to reduce risk of loss or tempering and for easier log analysis
- Collect more than one type of logs for context and correlation
- Deploy across all OS and environments, on-prem and cloud, for best coverage

Why It Matters: Logs are only as strong as their integrity. If attackers can manipulate or delete them, your forensic record is broken.



Step 3: Filter Early

Collecting “everything” is a recipe for high SIEM bills and wasted SOC analyst hours. The smarter approach: **filter logs at the source to reduce SIEM storage/ingestions costs.**

Best Practices:

- **Filter out noise**: repetitive system events, heartbeat signals, or events with no detection value.
- **Standardise formats**: convert to standard log format supported by the destination application
- **Protect sensitive data:** mask sensitive data such as credit card numbers or secrets that may appear in the logs
- **Send what matters:** log analysis, threat detection and response tools may require different log data and formats. Apply filtering relevant to each application. Replay logs on-demand when the need arises

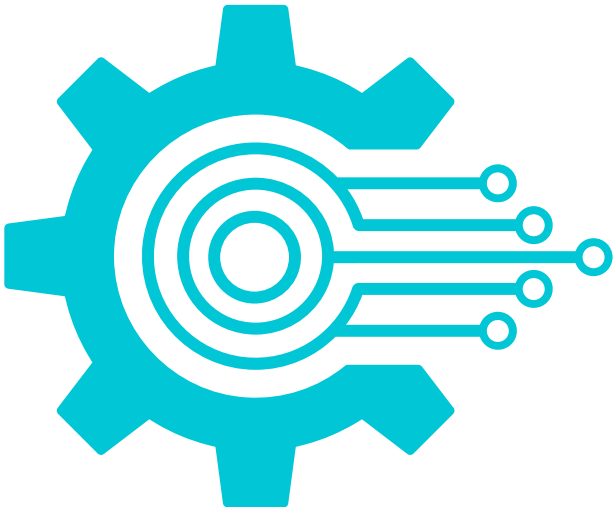
Example Impact: Organisations have reduced SIEM ingestion volumes by **50–90%** while improving detection fidelity through pre-processing.

Step 4: Optimise Storage with Smart Log Tiering

Traditional tiered storage models often push all logs into costly cloud environments — creating duplication, data sprawl, and budget headaches. Snare offers a smarter approach.

With Snare, you can store all logs centrally within your own Snare environment, where data is highly compressed, and retained at a low, predictable static cost.

From there, you only forward what's necessary to downstream systems like your SIEM, XDR, or analytics tools. This ensures you maintain full visibility and compliance without paying to re-ingest or re-analyse every log multiple times.



The result: a single source of truth for all event data, reduced cloud costs, and a far more efficient way to manage, search, and retain logs — without compromising security or compliance.

Step 5: Ensure Integrity & Retention

Logs are only valuable if they can stand up to scrutiny. Regulators, auditors, and forensic investigators all demand integrity and retention guarantees.

Best Practices:

- Apply **cryptographic checksums** or hashing to detect tampering.
- Use **write-once, read-many (WORM)** storage for critical audit logs.
- Ensure logs are backed up.
- Define retention policies based on regulation:
  - GDPR: “as long as necessary.”
  - PCI DSS: 1 year minimum.
  - Essential 8: varies by maturity level.
- Monitor access to logs — enforce least privilege and maintain audit trails.

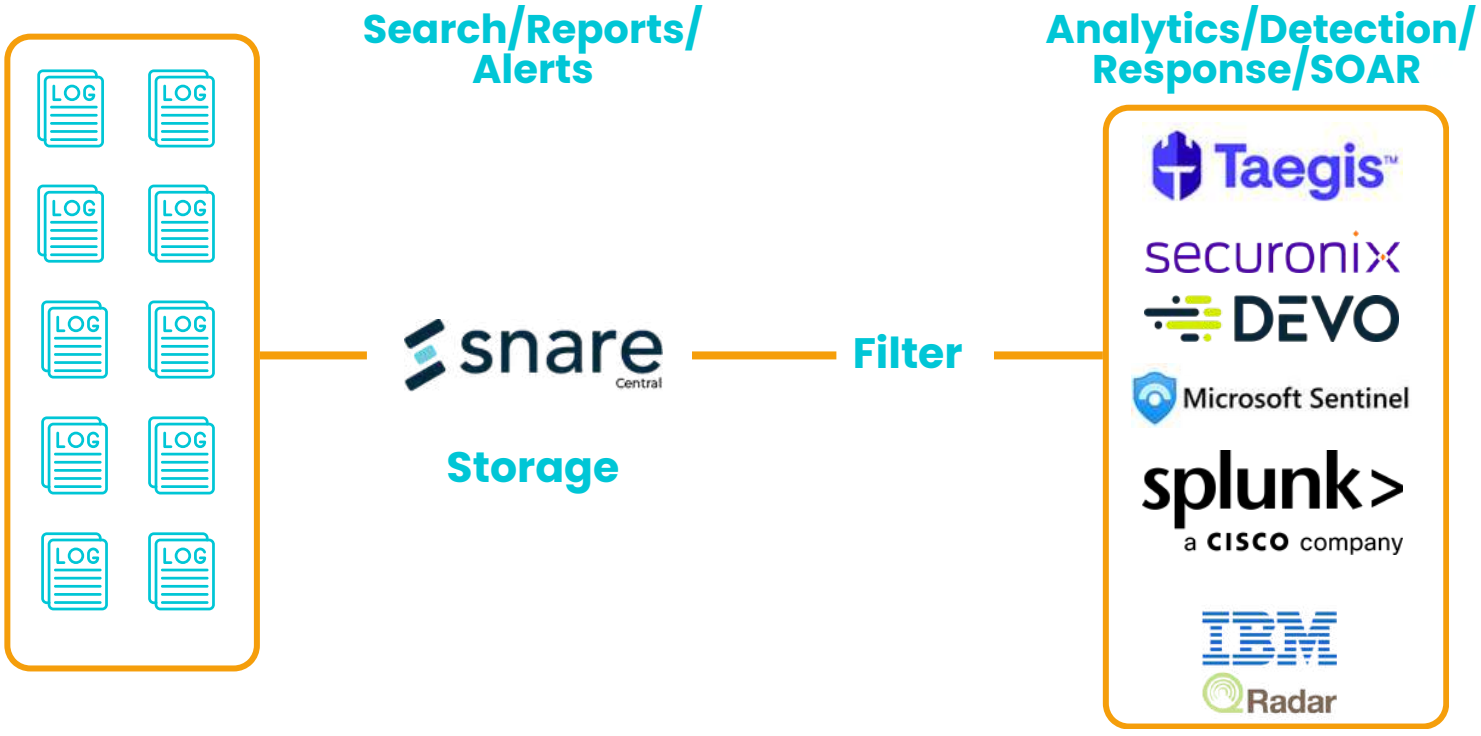
Step 6: Correlate, Alert, and Act

The true value of logging isn't just collecting — it's what you do with the data. Feeding enriched, filtered logs into SIEM and XDR makes detection sharper and response faster.

Best Practices:

- Prioritise correlation rules that combine multiple log sources (e.g., failed MFA + privilege escalation attempt).
- Reduce false positives with cleaner, more contextualised logs.
- Integrate with SOAR platforms to automate incident response.
- Share enriched logs with threat intelligence feeds to strengthen detection.

Example Impact: SOC teams often report **20–30% faster mean time to detect (MTTD)** when logs are clean and normalised when required.



Step 7: Review, Refine, Repeat

Logging is not a “set and forget” discipline. Threats evolve, compliance changes, and new systems enter your environment. Continuous review is essential.

Best Practices:

- Schedule **quarterly logging health checks**:
  - Are you still collecting the right data? What’s changed?
- Review SIEM costs regularly and adjust filtering rules.
- Align logging coverage with evolving regulatory requirements.
- Test log usability with mock forensic investigations.

Conclusion: Event Logging as a Business Enabler

Event logging done right is not just “security plumbing.”

It reduces risk, ensures compliance, cuts costs, and enables smarter detection and response.

With a structured strategy, logging shifts from being a burden to becoming a business advantage.

snare
A PROPHECY SOLUTION

Book a Free Logging Health Check

Explore Snare's Suite of Solutions

www.snaresolutions.com

Toll Free US: 1(800) 834 1060
Asia/Pacific: +61 8 8213 1200
UK/Europe: +44 (800) 368 7423

AMERsales@prophecyinternational.com
APACsales@prophecyinternational.com
EMEAsales@prophecyinternational.com