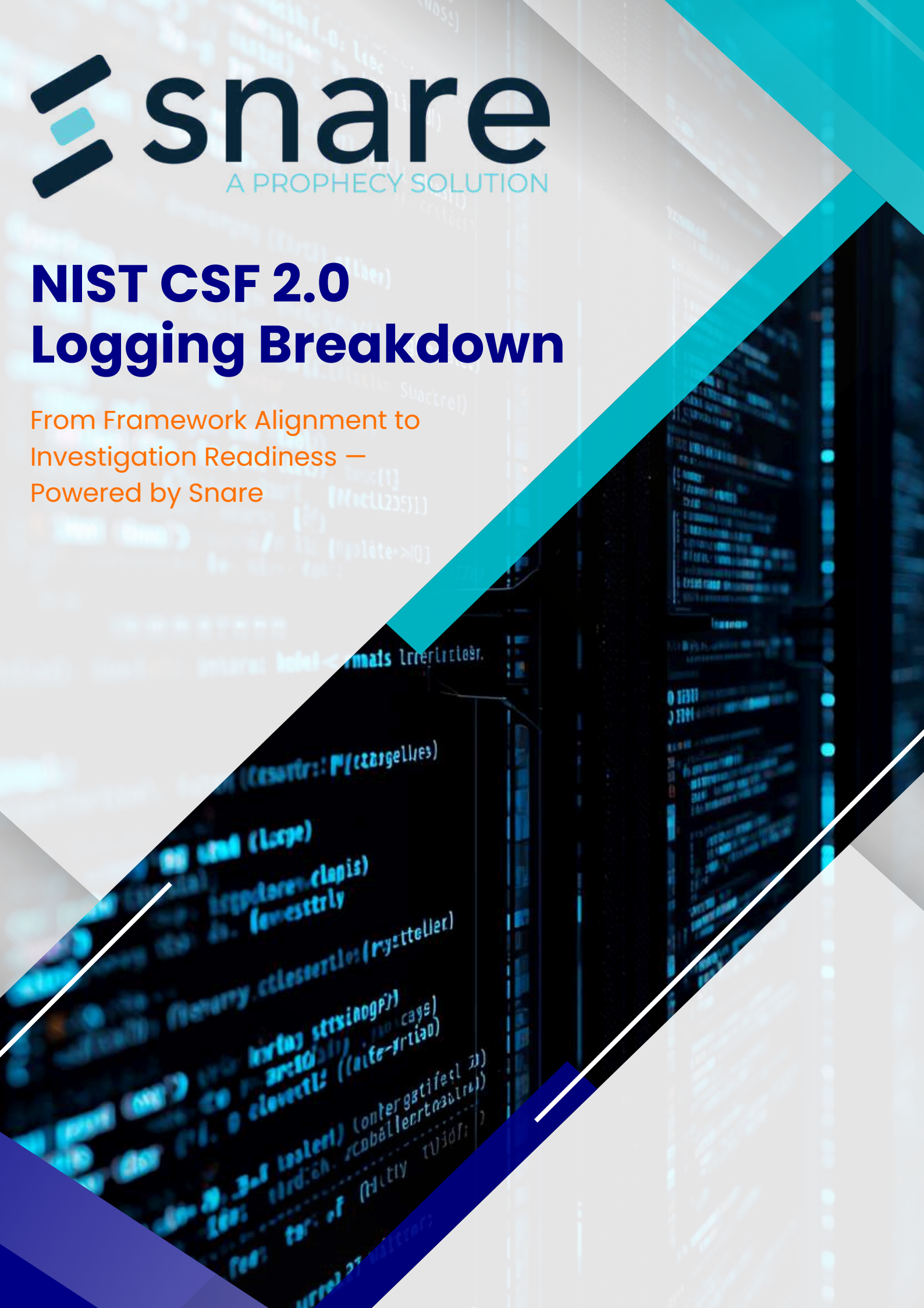
snare
A PROPHECY SOLUTION

NIST CSF 2.0 Logging Breakdown

From Framework Alignment to Investigation Readiness — Powered by Snare



Executive Summary

The **NIST Cybersecurity Framework (CSF) 2.0** represents a fundamental shift in cybersecurity.

It moves organisations beyond:

- Control implementation
- Alert generation
- Compliance reporting

With the addition of Govern, organisations are now expected to move beyond technical controls and demonstrate:

- Accountability
- Measurable risk management
- Evidence-based decision making

The Challenge

Security is no longer defined by:

- Tools deployed
- Alerts generated

It is defined by:
How well an organisation can understand, prove, and defend its security posture.

In reality:

- Logging is fragmented
- Data is incomplete
- Retention is insufficient
- Investigations are slow and inconclusive

You cannot achieve NIST CSF 2.0 alignment without a logging strategy that supports governance and investigation

snare
A PROPHECY SOLUTION

THE LOGGING GAP IN MOST ORGANISATIONS

Across industries, the same patterns appear:

1. Fragmented Collection

Logs exist — but across disconnected systems

2. Early Filtering

Data is reduced before it can be used

3. Limited Retention

Logs are not available when investigations begin

4. Lack of Correlation

Identity, activity, and impact are not connected

5. SIEM Dependency

Visibility is constrained by ingestion cost

**Security teams are not lacking data —
they are lacking usable, connected data.**

snare
A PROPHECY SOLUTION

WHAT NIST CSF 2.0 REALLY REQUIRES

SECTION 1: THE ROLE OF LOGGING IN NIST CSF 2.0

NIST CSF 2.0 consists of six core functions:

- Govern (new)
- Identify
- Protect
- Detect
- Respond
- Recover

What Has Changed in 2.0

- Stronger focus on **governance and accountability**
- Emphasis on **continuous monitoring**
- Expectation of **traceability across systems**
- Shift toward **outcome-based security**

What This Means Practically and Why Logging Now Sits at the Core

Organisations must now be able to:

- Understand who accessed systems
- Track what actions were taken
- Reconstruct incidents end-to-end
- Provide evidence for decisions and outcomes

This is not a tooling challenge.
It is a data and visibility challenge.

SECTION 2: GOVERN — ACCOUNTABILITY, RISK, AND EVIDENCE

NIST Expectation

Establish governance over cybersecurity risk, ensuring accountability and informed decision-making.

What Govern Requires in Practice

- Clear ownership of cyber risk
- Ability to measure and report on security posture
- Evidence to support decisions and controls
- Alignment between business risk and technical activity

Logging Requirements

- Audit trails of user and system activity
- Evidence of control enforcement
- Policy and configuration change tracking
- Historical records to support audits and reviews

Common Gap

Organisations:

- Define policies
- But cannot prove they are being followed

What This Looks Like (Before)

- Governance based on assumptions
- Limited auditability
- Inability to validate controls with evidence

Snare Alignment

Snare enables governance by:

- **Providing tamper-resistant, forensic-quality logs**
- **Ensuring complete audit trails across environments**
- **Supporting long-term retention for regulatory and audit needs**
- **Delivering evidence-based visibility into actual activity**

Outcome (After)

Governance moves from policy-driven → evidence-driven

snare
A PROPHECY SOLUTION

SECTION 3: IDENTIFY — VISIBILITY OF ASSETS, USERS, AND DATA

NIST Expectation

Understand assets, identities, and system usage.

Logging Requirement

- Authentication and identity logs
- Asset and system activity
- Data access tracking
- Configuration changes

Before (Typical State)

- Partial identity visibility
- Limited asset usage insight
- No linkage between users and systems

Snare Alignment

- Centralised, full-fidelity log collection
- Visibility across endpoints, infrastructure, and hybrid environments
- Foundation for linking identity to system activity

Outcome

Complete visibility of identity → system → data relationships

SECTION 4: PROTECT — CONTINUOUS VALIDATION OF ACCESS

NIST Expectation

Ensure access is controlled and continuously validated.

Logging Requirement

- Access control events
- Privileged activity logs
- Policy enforcement tracking
- Configuration changes

Before

- Access logged but not validated
- Privileged activity partially visible
- Limited auditability

Snare Alignment

- Detailed tracking of privilege usage and access events
- Policy-based control over what is collected and where it is sent
- Visibility into behaviour after authentication

Outcome

Access is continuously validated — not assumed

SECTION 5: DETECT — CONTEXTUAL MONITORING

NIST Expectation

Continuously detect anomalies across environments.

Logging Requirement

- Endpoint activity
- Network and infrastructure logs
- Cloud and SaaS audit logs
- API activity

Before

- SIEM-driven alerting
- High noise, low context
- Limited cross-system visibility

Snare Alignment

- Full-fidelity data before SIEM ingestion
- Smart filtering that preserves investigative value
- Consistent, normalized data across environments

Outcome

Detection becomes context-driven, not alert-driven

SECTION 6: RESPOND — INVESTIGATION AND RECONSTRUCTION

NIST Expectation

Investigate incidents quickly and accurately.

Logging Requirement

- Correlated logs across systems
- Session-level tracking
- Timeline reconstruction
- Forensic-quality data

Before

- Manual, fragmented investigations
- Disconnected data sources
- Incomplete timelines

Snare Alignment

- Identity → activity → impact traceability
- Replay capability for missed detections
- Centralised data for rapid investigation

Outcome

Full reconstruction of incidents with defensible evidence

SECTION 7: RECOVER — LEARNING AND RESILIENCE

NIST Expectation

Restore operations and improve resilience.

Logging Requirement

- Long-term retention
- Historical analysis
- Replay capability
- Audit-ready evidence

Before

- Short retention windows
- Limited historical visibility
- No ability to validate past events

Snare Alignment

- Cost-efficient long-term storage
- Replayable log data
- Historical insight for continuous improvement

Outcome

Recovery is driven by evidence, not assumptions

SECTION 8: HOW TO START ALIGNING YOUR ORGANISATION TO NIST CSF 2.0

Step 1: Establish Governance First (Start with "Govern")

Define:

- Who owns cyber risk
- What needs to be measured
- What evidence is required

Key Action

Align security, IT, and leadership on what must be provable

If you cannot define what evidence you need — you cannot align to NIST

Step 2: Assess Your Investigation Readiness

Ask:

- Can we reconstruct a breach end-to-end?
- Can we link identity to activity?
- Do we have sufficient retention?

Use: Investigation Readiness Checklist

Step 3: Map Your Current Logging Coverage

Identify gaps across:

- Identity
- Endpoint
- Cloud
- Network
- Applications

Key Focus
Coverage matters more than volume

Step 4: Fix the Data Foundation First

Before adding more tools:

- Centralise log collection
- Remove early filtering
- Ensure data consistency

Where Snare Fits

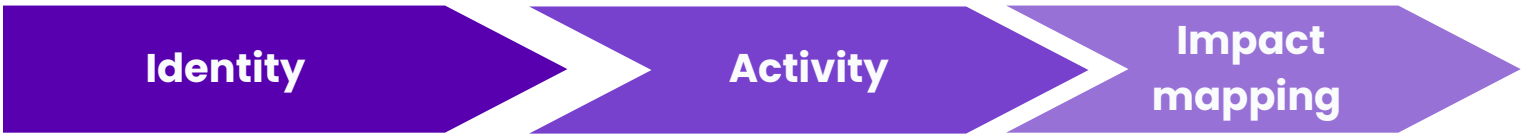
Snare operates:

- At the **first mile of data collection**
- Before SIEM ingestion
- Ensuring data completeness and integrity

Fix the data layer — everything else improves

Step 5: Enable Correlation and Traceability

Move toward:



- Link user behaviour across systems
- Enable correlation and investigation

Step 6: Extend Retention and Enable Replay

Shift from:

- Short-term detection
- Long-term investigation capability

Move to

- Retain logs beyond detection windows
- Enable reconstruction of past events

Key Capability

Ability to revisit and replay historical data

Goal
Reconstruct incidents, not just detect them

snare
A PROPHECY SOLUTION

Step 7: Optimise SIEM — Don't Depend on It

Reduce:

- Cost
- Noise
- Over- Ingestion

Enhance:

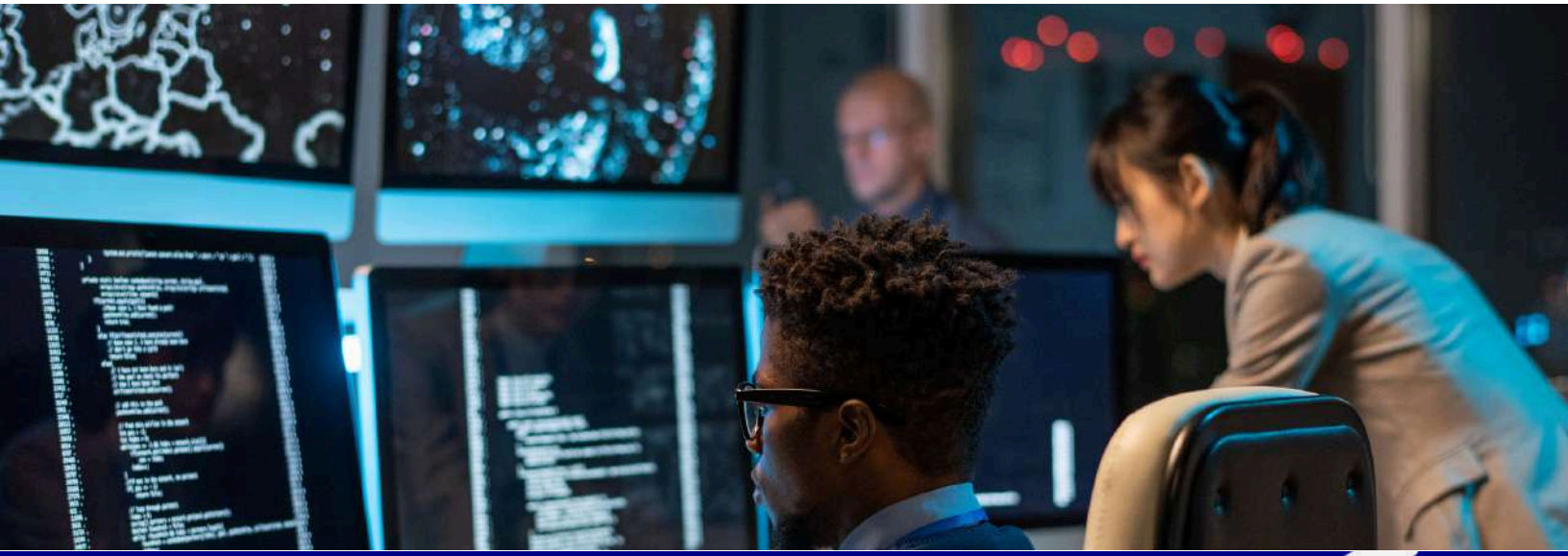
- Data quality
- Context
- Detection accuracy

Snare's Role

- Filter intelligently before SIEM
- Route logs to the right destinations
- Reduce ingestion costs without losing value

Step 8: Align to Continuous Improvement (Govern + Recover)

- Use logs to inform risk decisions
- Improve controls based on evidence



THE SNARE ADVANTAGE IN NIST ALIGNMENT

Snare is not:

- A SIEM
- A detection tool

Snare is :

The foundation that enables NIST-aligned visibility and investigation readiness

---

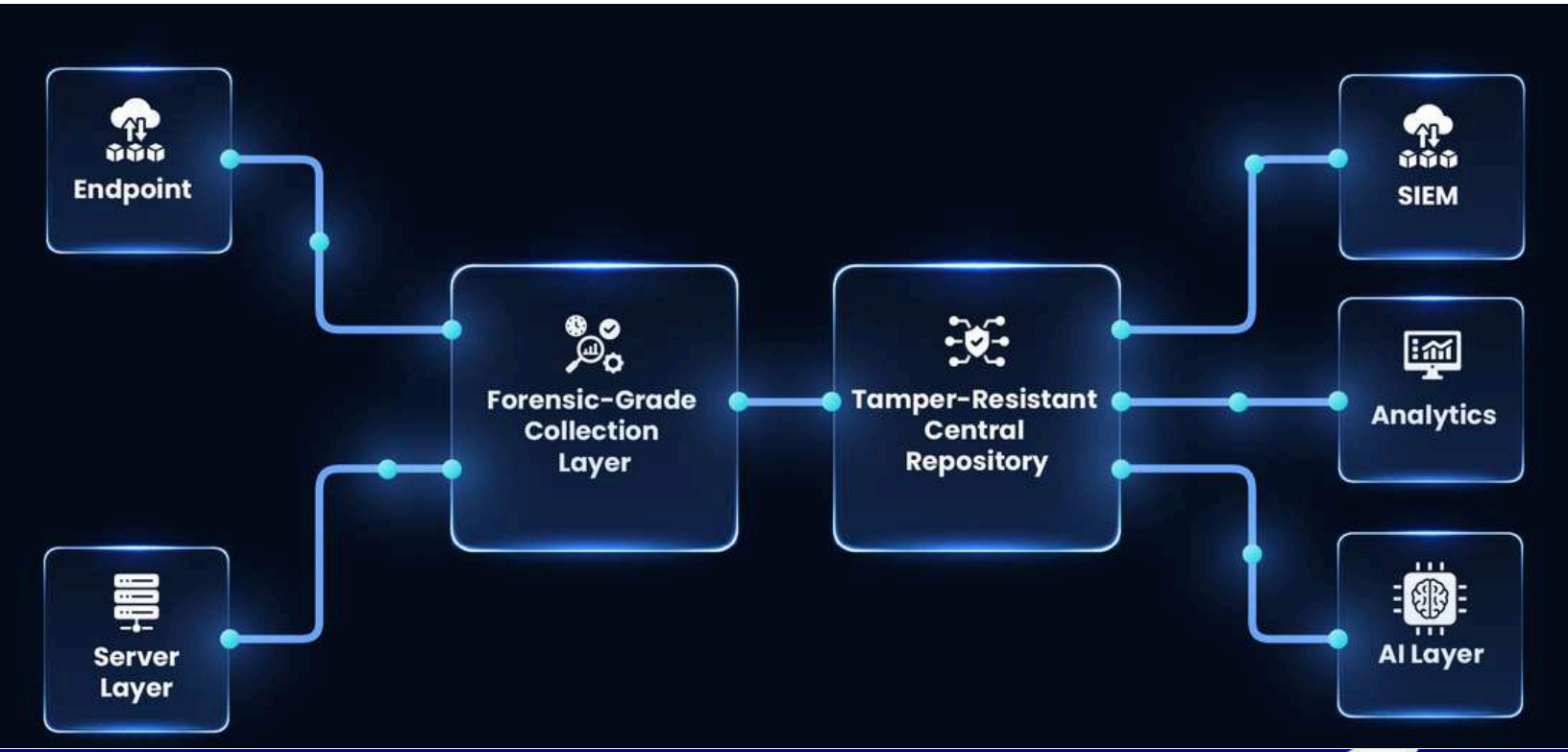
Key Capabilities

- Full-fidelity log collection
- Vendor-agnostic integration
- Long-term retention and replay
- Policy-driven routing and filtering
- Support for high-volume environments

Where is Snare Positioned

- Before SIEM
- Across environments
- At the point where data quality is defined

Without this layer, NIST alignment remains theoretical



snare
A PROPHECY SOLUTION

HOW TO BEGIN YOUR NIST CSF 2.0 ALIGNMENT JOURNEY

From Framework Understanding → Operational Execution

Most organisations understand *what* NIST requires.

The challenge is knowing **where to start — without overhauling everything at once.**

Step 1: Start With an Investigation Mindset — Not a Compliance Checklist

Before mapping controls, shift the internal question

From:
"Are we compliant?"

To:
"Can we prove what happened in our environment — end to end?"

Practical Action

Run a simple internal exercise:

Ask your team to answer:

- How did a user gain access?
- What actions did they take?
- What systems were affected?
- What data was accessed or changed?

What You'll Likely Find

- Answers are slow
- Data is incomplete
- Multiple systems are required

This gap is your true starting point — not your compliance score.

Step 2: Establish a Baseline of What You Can (and Cannot) See

Before improving anything, you need a clear picture of your current visibility.

Practical Action

Map your logging coverage across:

- Identity (IAM, Active Directory)
- Endpoints (servers, desktops)
- Cloud & SaaS
- Network & infrastructure
- Applications & APIs

Key Questions

- Where are logs being collected?
- Where are they missing entirely?
- Where are they siloed?

Critical Insight

Most organisations don't have a logging problem — they have a coverage problem.

Step 3: Fix the First Mile — Data Collection Before Detection

Most security strategies start at SIEM.

That's too late.

Practical Action

- Identify where logs are being filtered before collection
- Review what data is being dropped or reduced
- Ensure raw, high-fidelity logs are captured at source

Why This Matters

- Once data is filtered or lost:
- It cannot be recovered
- It cannot support investigation
- It limits all downstream tools

Where Snare Fits

Snare operates at this first mile:

- Collects logs before filtering removes value
- Ensures completeness and integrity
- Provides a consistent data foundation

If you fix the data layer first, every other control improves.

Step 4: Prioritise Identity → Activity → Impact Traceability

NIST CSF 2.0 implicitly requires organisations to understand cause and effect.

Practical Action

- Focus on your ability to link:
- Identity (who logged in)
- → Activity (what they did)
- → Impact (what changed)

Key Questions

- Can you trace a user session end-to-end?
- Can you detect privilege escalation during activity?
- Can you prove what data was accessed?

Common Reality

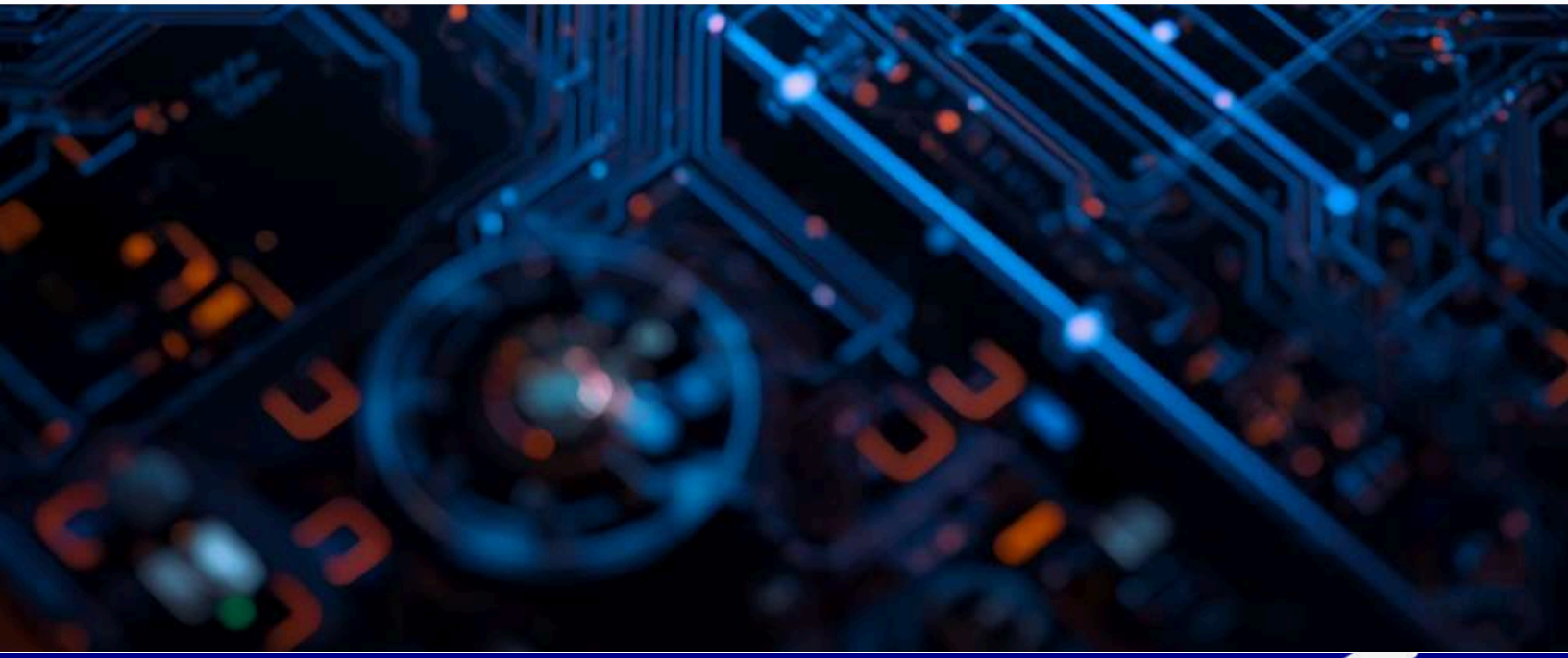
Most organisations:

- Can see identity
- Can see events
- But cannot connect them

Where Snare Fits

- Provides the data continuity required for correlation
- Enables consistent log structure across environments
- Supports investigation-ready traceability

This is the difference between detection and understanding.



Step 5: Extend Retention to Match Real Investigation Timelines

Detection does not always happen in real time.

Practical Action

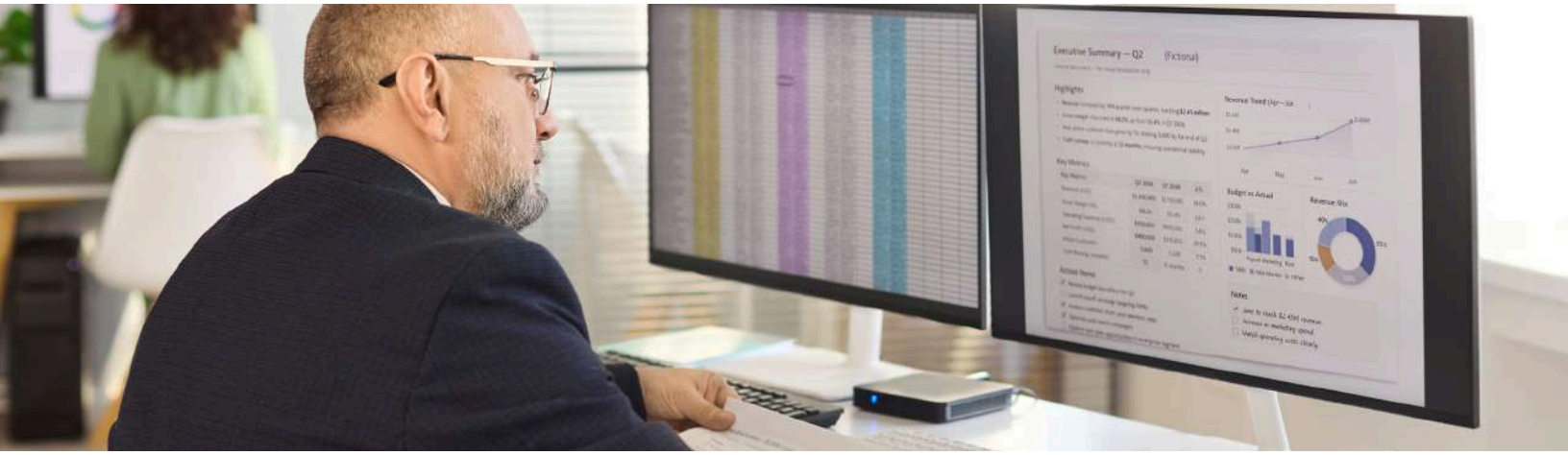
- Assess your current log retention periods
- Compare them to realistic breach discovery timelines (weeks to months)
- Extend retention for high-value log sources

Key Risk

If logs are gone before an investigation begins — the investigation is already compromised.

Where Snare Fits

- Enables cost-efficient long-term storage
- Reduces dependency on expensive SIEM retention
- Supports historical analysis and replay



Step 6: Enable Replay and Reconstruction Capabilities

Modern investigations require more than search.

They require reconstruction

Practical Action

- Ensure logs can be accessed historically without delay
- Enable replay of log data into analysis tools
- Validate that timelines can be rebuilt accurately

Key Outcome

**You move from "what triggered an alert" →
to "what actually happened."**

Where Snare Fits

- Replay capability for missed detections
- Reconstruction of full timelines
- Support for forensic-level investigations

Step 7: Optimise SIEM — Reduce Noise, Increase Value

SIEM is critical — but often overloaded.

Practical Action

- Identify unnecessary ingestion
- Reduce low-value data sent to SIEM
- Prioritise high-context, high-value logs

Key Shift

From:

- "Send everything to SIEM"

To:

- "Send what matters — retain everything else intelligently"

Where Snare Fits

- Smart filtering and routing
- Reduces ingestion costs
- Preserves full data outside SIEM

Better data → better detection → lower cost

Step 8: Align Teams Around Investigation Outcomes

NIST CSF 2.0 is not just a technical framework — it is operational.

Practical Action

- Align:
- Security teams
- IT operations
- MSSPs (if applicable)

Around one shared goal:

Investigation readiness

What This Looks Like

- Faster incident response
- Clear ownership of data visibility
- Shared understanding of risk

FINAL GUIDANCE: START SMALL, BUT START WITH IMPACT

Organisations often delay NIST alignment because it feels too large.

It doesn't need to be.

Start With These Three Moves

1. **Assess investigation readiness**
2. **Fix logging coverage and collection**
3. **Extend retention and enable traceability**

You don't need to transform everything.
You need to fix the parts that prevent you from seeing the truth.

CLOSING INSIGHT

NIST CSF 2.0 is not prescriptive about tools.

But it is very clear about outcomes:

- Visibility
- Traceability
- Accountability

The organisations that succeed will not be those with the most controls — but those with the clearest understanding of what is happening in their environment.

Start Your NIST Alignment Journey Today

- Assess your current maturity
- Identify logging gaps
- Build an investigation-ready architecture

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

snare
A PROPHECY SOLUTION