Kloudynet



Why SOC Reports Matter

Good security operations are mostly invisible. The right report turns 24/7 detection and response into evidence, insight and decisions your leadership can act on.

The Visibility Problem

When a SOC does its job well, nothing dramatic happens. Attacks are stopped early, incidents stay small and the business carries on. That success is easy to overlook, and hard to justify at budget time, unless it is clearly reported.

Invisible value

Leaders can't see the threats that were stopped, so security looks like a cost rather than protection.

Tough board questions

"Are we secure?" and "Are we getting better?" need evidence, not reassurance.

Audit and regulatory pressure

Regulators and auditors expect proof that monitoring, response and reporting actually happen.

Hidden gaps

Without regular review, blind spots in coverage and recurring weaknesses go unnoticed.

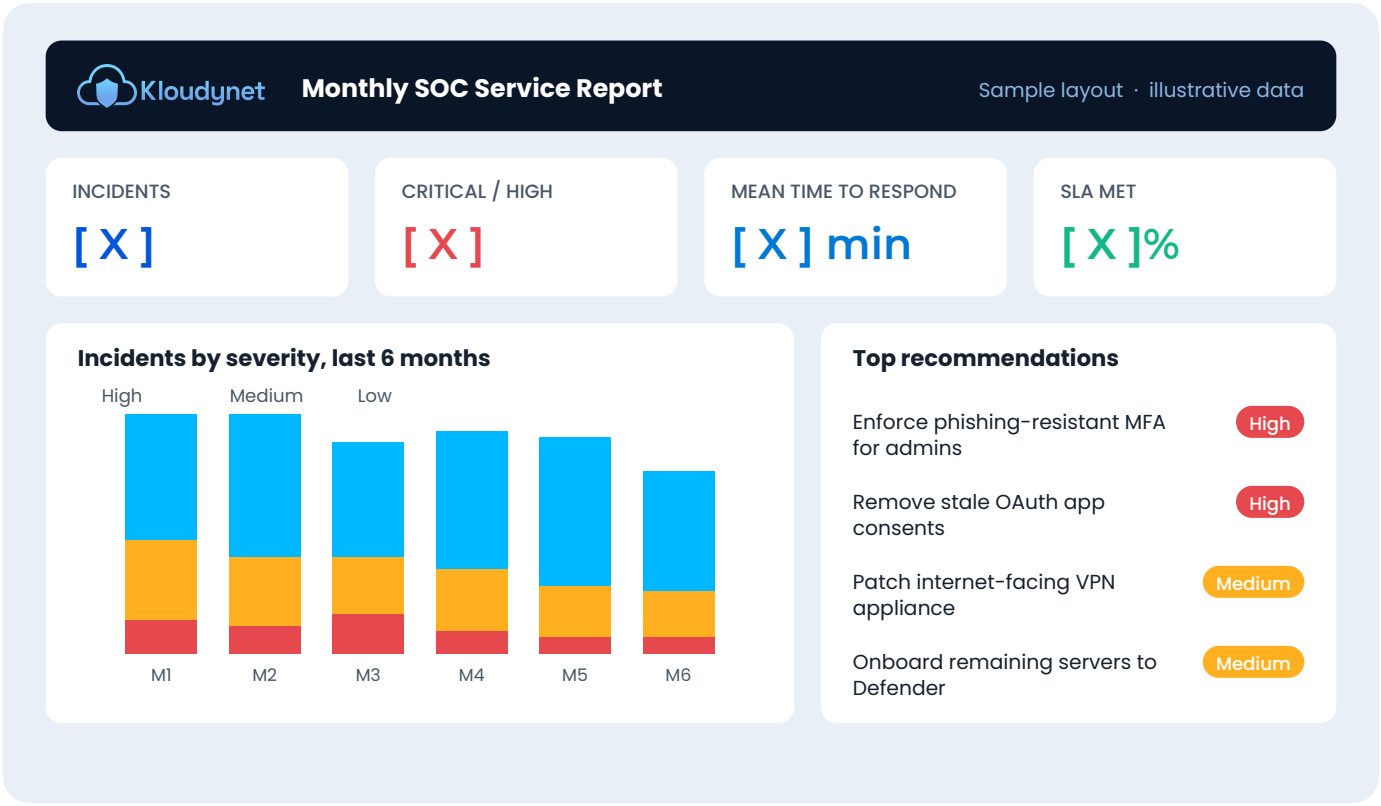
Five Questions Every SOC Report Should Answer

A useful report is not a data dump. It answers the questions stakeholders actually ask:

Q1 What happened?	Incidents raised, how serious they were, and which users, devices and systems were involved.
Q2 What did we stop?	Threats contained, accounts protected and attacks disrupted, with time to detect and respond.
Q3 Where are we exposed?	Coverage gaps, unpatched vulnerabilities, risky configurations and the most-targeted people.
Q4 Are we improving?	Trends over time in detection speed, false positives, coverage and open risks.
Q5 What should we do next?	Prioritised, practical recommendations with clear owners.

Inside a Kloudynet SOC Report

Each report is built around the same structure, so trends are easy to follow from one period to the next.



The Metrics That Matter

- **Mean time to detect (MTTD)**
  How quickly threats are spotted once they start.
- **Incidents by severity and type**
  Where attacks are coming from and how serious they are.
- **MITRE ATT&CK coverage**
  Which attacker techniques are detected, and which are not.
- **SLA performance**
  Whether response commitments were met, period by period.
- **Mean time to respond (MTTR)**
  How quickly threats are contained once detected.
- **True vs false positive rate**
  Whether detections are accurate or creating noise.
- **Most-targeted users and assets**
  Who and what attackers focus on, to prioritise protection.
- **Open recommendations**
  Outstanding actions, owners and progress since the last report.

KloudSecure

One Report, Every Audience

Different stakeholders need different levels of detail. Kloudynet reporting is layered so each audience gets what it needs.

Board & executives

Risk in business terms, trends and the few decisions that need their support.

IT & security leaders

Incidents, coverage, exposures and a prioritised action plan.

Auditors & regulators

Evidence of continuous monitoring, timely response and documented incidents.

Technical teams

Detailed findings, indicators and remediation steps they can act on.

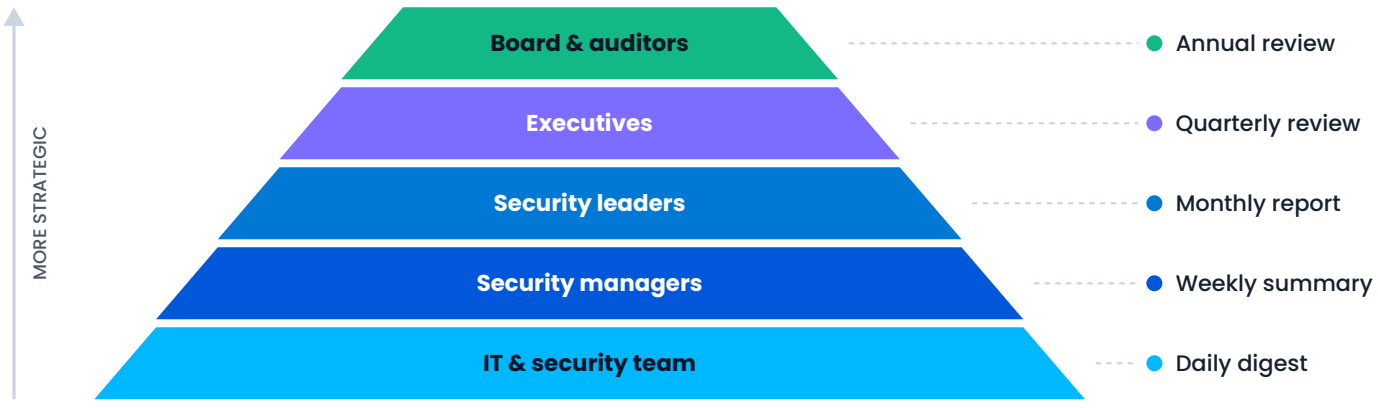
From Activity to Insight

Illustrative examples

A TYPICAL REPORT SAYS	A KLOUDYNET REPORT SAYS
1,240 alerts processed this month.	Three real incidents contained. None reached sensitive data.
Phishing detected.	Phishing aimed at finance staff: two accounts reset, sender blocked.
98% SLA met.	Critical incidents contained faster than last quarter, with the slowest one's root cause fixed.

From operational detail to strategic view

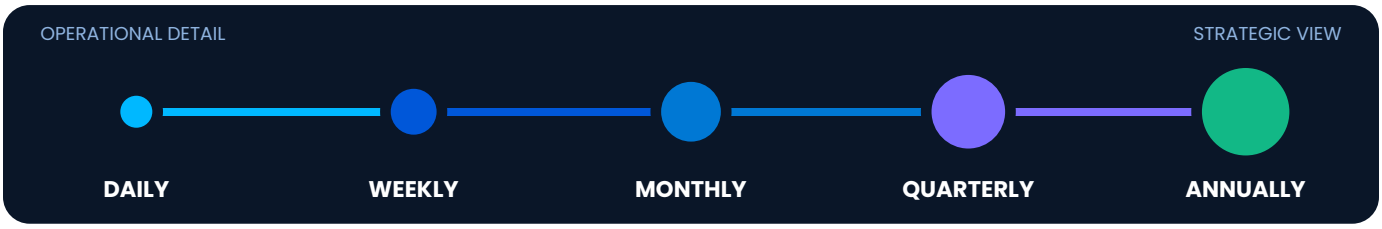
Who reads what, and how often



KloudSecure

Reporting Rhythm

Five layers of reporting, from daily operational detail to an annual strategic view, so every stakeholder gets the right picture at the right time.

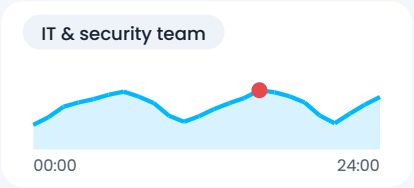


DAILY

SOC Daily Digest

Overnight activity at a glance.

- Incidents opened and closed in the last 24 hours
- Critical escalations and actions awaiting approval
- Notable blocked threats



WEEKLY

Operations Summary

What changed this week and why.

- Incident trends by severity and type
- Detection tuning and noisy rules fixed
- Open items and quick wins



MONTHLY

SOC Service Report

The full performance picture.

- MTTD, MTTR and SLA performance
- MITRE ATT&CK coverage changes
- Threat landscape and prioritised recommendations



QUARTERLY

Executive Review

Risk posture in business terms.

- Risk trend and top exposures
- Progress on recommendations
- Roadmap and investment priorities

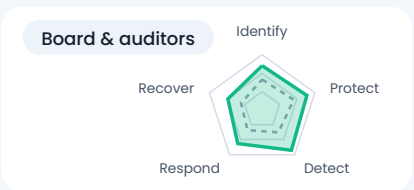


ANNUALLY

Annual Security Review

The year in review and the year ahead.

- Maturity assessment against frameworks
- Audit-ready evidence pack
- Strategy and goals for next year



Supporting Compliance

Regular, well-structured SOC reports provide the evidence trail that many frameworks and regulators look for, including:

Cyber Security Act 2024 (Malaysia)

Readiness and incident reporting expectations for national critical information infrastructure entities.

Personal Data Protection Act 2010

Demonstrating safeguards for personal data held by commercial organisations.

BNM Risk Management in Technology

Technology risk and cyber resilience expectations for financial institutions.

ISO/IEC 27001

Evidence for monitoring, incident management and continual improvement controls.

Reports support compliance evidence; they do not by themselves certify compliance with any framework.

What Sets Kloudynet Reporting Apart

Plain language first

Every report opens with a short executive summary anyone can read in minutes.

Evidence behind every number

Metrics link back to real incidents and investigations, powered by KloudSecure AI.

Actions, not just activity

Each report ends with prioritised recommendations and tracks them to closure.

See what your SOC is really doing

Ask Kloudynet for a sample SOC report and a walkthrough of our MXDR reporting.

Kloudynet