Monthly Security Report Template

Comprehensive snapshot of security posture and compliance

A monthly security report communicates the organization's cybersecurity posture, recent incidents, threat landscape and compliance status to executives and stakeholders. This template ensures that your report covers key elements in a clear and actionable way.

Key Findings Summary

- Summarize major security events, trends and notable metrics from the reporting period.
- Highlight improvements and unresolved risks that require management attention.
- Use clear language accessible to non-technical stakeholders.

Monitoring Summary

- Number of endpoints, servers and cloud services monitored versus total assets.
- Detection coverage and any unmonitored areas or blind spots.
- Patching and vulnerability management status across systems.
- Summary of alerts received and false positive rates.

[8] Bitsight recommends SOC reports include incident summaries, performance metrics, threat landscape analysis, remediation actions, compliance status and executive recommendations.

Incident Summary

- Total number of security incidents and breakdown by type (e.g., phishing, malware, unauthorized access).
- Mean time to detect and mean time to respond for each incident category.
- Details of remediation actions taken and outstanding POA&M items.
- Lessons learned and recommendations for preventing similar incidents.

Threat Landscape

- Overview of top external threats observed and emerging vulnerabilities.
- Comparison with industry threat data and relevant advisories.
- Potential impacts on your organization's mission and compliance obligations.

Remediation & Recommendations

- Actions taken to close vulnerabilities and improve security controls.
- Outstanding remediation tasks and responsible owners with due dates.
- Recommendations for additional resources, training or investment to enhance security posture.

Compliance Status

- Current CMMC Level 2/3 compliance status and recent audit findings.
- Status of DFARS 252.204-7012 incident reporting and flowdown requirements.
- Progress against NIST 800-171 controls and POA&M remediation.
- User awareness and training completion rates.

Next Steps & Planning

- Planned initiatives for the next reporting period (e.g., new controls, assessments, upgrades).
- Upcoming compliance deadlines and milestones.
- Continuous improvement activities to enhance cybersecurity maturity.