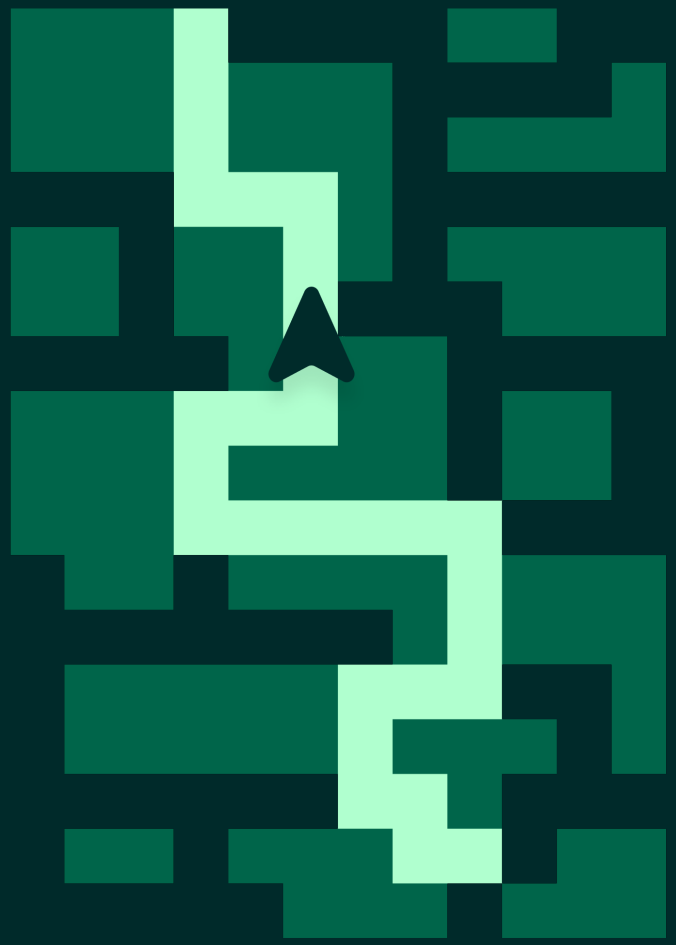
C3Plan

Cybersecurity Assessment

semios

NIST CSF Assessment and Recommendations



Created by c3plan.com

January 2025

Content

Background

Background

- Semios business: combine advanced technology with traditional agricultural wisdom, focus on crop production efficiency.
- Global Reach, operating in Canada, US, Australia, New Zealand
- Employes approximately 300 employees and works with several critical partners
- Engaged C3Plan to:
  - Provide Fractional CISO (cybersecurity support) service
  - Conduct a NIST* CSF 2.0–based IT security assessment to prioritize remediation activities and develop a roadmap
- Assessment focuses on key IT areas, endpoint management, phishing defenses, user awareness, and governance; excluding OT (Operational Technology).
- Leverage material from previous assessment (Kobalt)

GOVERN	Establish policies, processes, and oversight to manage cybersecurity risk.	DETECT	Monitor systems to identify cybersecurity events promptly.
IDENTIFY	Understand assets, risks, and threats to manage resources effectively.	RESPOND	Take action to contain and mitigate the impact of incidents.
PROTECT	Implement safeguards to secure systems, data, and operations.	RECOVER	Restore services and operations to minimize disruption.

*NIST (National Institute of Standards and Technology) CSF 2.0

Scope and Objectives

C3Plan

Scope and Objectives

- Evaluate Semios current Cybersecurity Risk Posture
  - Leverage previous assessment
  - Use standard industry framework
- Identify key risks and develop a risk register
- Identify risk-based remediation activities
- Prioritize risks based on likelihood and business impact
- Develop recommended projects and suggested timelines
- Engage fractional-CISO service to assist with remediation activities and ongoing support

Approach

C3 Plan

Approach

***Participants from Semios**:*
Dicky Leung, Kevin Johnston, Adrien Lemier

***C3Plan**:*
Omid Hamed, Felipe Sarubbi, Dinesh Kumar, Sonny Sarai

Observations

Observations (1/2)

- **Overall score:** of ~1.6 is is below average and indicates the need for improvement
  - Semios is on path to foster cybersecurity mind-set culture through improved awareness
- Limited IT resources and no dedicated security personnel
- **Security in Cloud-centric environment:** Semios relies heavily on SaaS providers (e.g., Google Workspace). While these platforms offer robust built-in controls, they remain underutilized in critical areas (e.g., MFA, advanced email security).
- **Phishing as a primary threat:** Semios frequently encounters sophisticated phishing attempts, underscoring the need for stronger technical filtering and recurring user awareness efforts.
- **Endpoint management gaps:** Devices (desktops, laptops…) lack centralized oversight. MDM (mobile device management) coverage is partial, causing inconsistent encryption, patching, and remote-wipe capabilities.

Figure 1: Overall Security Score

Overall maturity is below industry average which's normally above 2.

Observations (2/2)

- Overall lack of **governance**, processes, and documentation.
    - Unstructured Incident Response. No formal plan or regular tabletop exercises, creating uncertainty about roles, responsibilities, and data restoration steps if a breach occurs.
    - Weak shadow IT and vendor management practices may introduce risks from unapproved software and weak third-party security clauses

High level considerations in this plan:

- Prioritized Incident Response and Recovery to prepare for threats and security incidents
- Conduct a baseline of technical benchmark of the current Google workspace and MS Office environment (Leverage Fractional CISO for remediation plan)
- Consider the implementation plan of the recommended projects in this assessment
- Continue with self-assessment and compare against the 2024 assessment to track progress and develop a continues improvement process

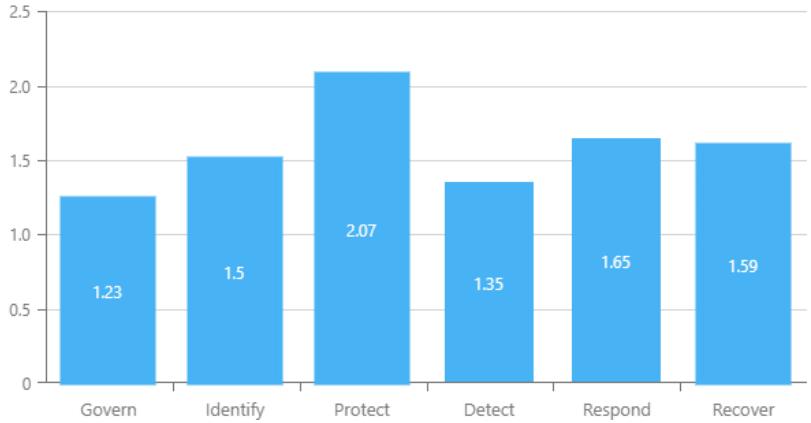


Figure 2: CSF Domain-level Maturity

Protect is slightly higher than other domains which is due to the Cloud-centric environment.

Recommendations

Recommendations

The following projects will help Semios to gradually improve cybersecurity posture within the resources and budget constraints

1. **MDM & Endpoint Hardening:** Full deployment of a unified MDM solution, plus secure baselines for device encryption, patches, and remote-wipe functions. A technical benchmark using industry standard CIS Controls will serve developing a baseline for device configuration security — Protect
2. **Phishing & Email Security Enhancements**: Upgraded email filtering, DNS/web blocking of malicious sites, and clear workflows for identifying and remediating phishing attempts. — Protect, IDENTIFY
3. **Security Awareness & Training Program**: Recurring training (including phishing simulations) to ensure employees understand evolving threats and best practices. . — Protect, Detect
4. **Incident Response & Recovery Improvements**: Documented IR plan, centralized logging or SIEM, and verified backup/restore processes for quick, organized responses to security incidents. — Respond, Recover
5. **Access Management & MFA**: Enforcing multi-factor authentication across all critical platforms and eliminating overprivileged admin accounts used for routine tasks. — Detect, Protect
6. **Governance & Vendor Management:** Establishing standardized contractual security requirements, strengthening “shadow IT” controls, and clarifying internal policies. — Govern

- Project #1, 2, 3, and 5 will further enhance Protect and Detect functions. Project #4 will improve Incident Response and Recovery processes. Project 6 will elevate the maturity in Govern function
- Each project is aligned with NIST CSF 2.0 subcategories and designed to reduce Semios’s overall risk. Detailed timelines, tasks, and budget breakdowns are provided

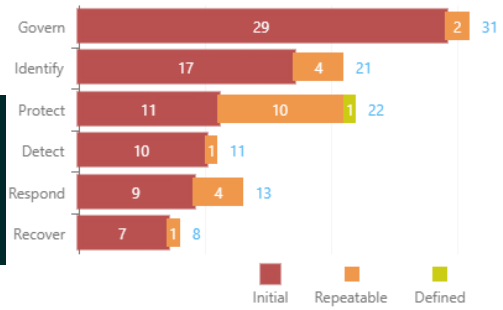


Figure 4: Cybersecurity Practices - Maturity Distribution

Concluding Statements

Concluding Statements

By implementing these recommendations in a phased approach—prioritizing MDM and phishing defenses first—Semios can:

- Secure endpoints against malware or data theft and decrease successful phishing attempts.
- Minimize downtime, data loss, and confusion during security events.
- Foster a proactive security mindset and reduce human error.
- Ensure technology decisions align with business and security goals through sustainable governance for vendors and shadow IT
- Prioritize Security projects to better align with budget and investments in risk-based security projects.

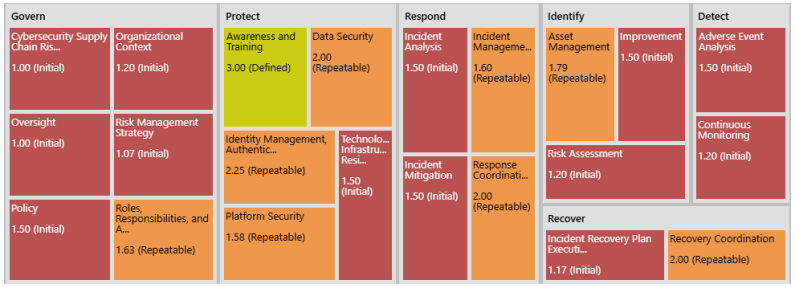


Figure 5: Capability Heatmap

All practices are in initial/repeatable maturity level save for one practice in Defined level, highlighting the overall need for improvements.

Each project is aligned with NIST CSF 2.0 subcategories and designed to reduce Semios's overall risk. Detailed timelines, tasks, and budget breakdowns are provided

C3 Plan

Thank You!

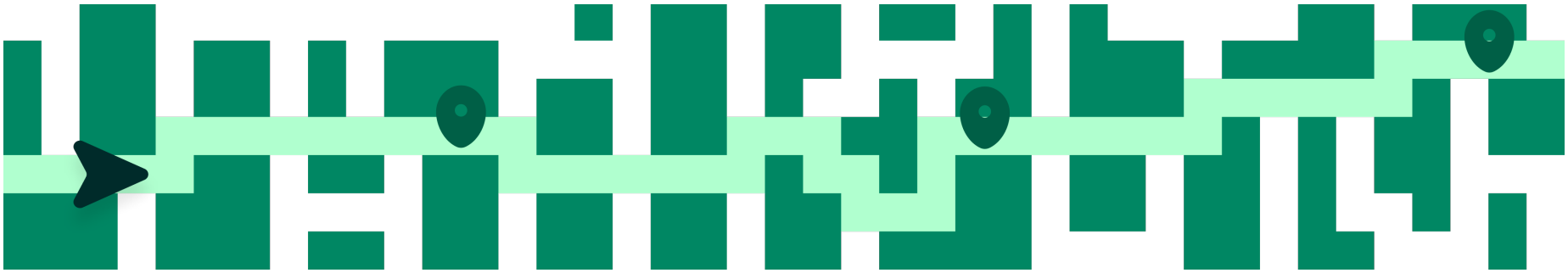
Looking forward to further discussions

January 2025

Dinesh Kumar
Dinesh@c3plan.com

Felipe Sarubbi
Felipe@c3plan.com

Omid Hamed
Omid@c3plan.com



Appendix – Detailed Analysis

NIST CSF Assessment

- Link to Detailed report, Appendix A

Semios Risk Register

- Link to Detailed report, Appendix B

Semios – Project Charters

- Link to Detailed report, Appendix C