2025

Aligning Get Event Log LLC with the NIST Cybersecurity Framework

GEL LLC

Information Security

Christopher Wireman

GEL LLC

6/8/2025

Table of Contents

Aligning Get Event Log LLC with the NIST Cybersecurity Framework

Executive Summary

Get Event Log LLC is a small but agile cybersecurity company specializing in Penetration Testing, Vulnerability Assessments, Red Team engagements, and Secure Software Quality Assurance (SQA). Leveraging a diverse operating environment including Windows, macOS, Linux, iOS, Android, and virtual machines secured behind a Xfinity gateway and firewall, the company seeks to align its operations with the **NIST Cybersecurity Framework (CSF)**.

This paper outlines how Get Event Log LLC implements and benefits from each of the six CSF functions—**Govern, Identify, Protect, Detect, Respond, and Recover**—across its core service offerings.

---

1. Govern

The **Govern** function establishes the foundation for cybersecurity risk management by defining policies, roles, and responsibilities.

Implementation at Get Event Log LLC:

- **Cybersecurity Policies**: Formal governance documents define procedures for client data handling, tool usage, vulnerability disclosure, and employee access control.
- **Compliance Awareness**: Mapping operations to standards like NIST SP 800-53, ISO 27001, and OWASP ensures audits and deliverables are regulation ready.
- **Ethics and Rules of Engagement**: Especially in Red Team and penetration testing, governance ensures operations stay within legal and ethical bounds.
- **Third-party Risk Management**: Assessments are conducted on tools and VM providers (e.g., Kali Linux VMs, Burp Suite Pro, Metasploit framework, NMAP, OpenVAS, and remote test environments).

---

2. Identify

The **Identify** function focuses on developing an understanding of the organization's environment to manage cybersecurity risk.

Asset Management

- **Device Inventory**: Active tracking of Windows, macOS, Linux-based PCs, and mobile devices used in client testing.
- **Software Inventory**: Logging penetration tools, hypervisors, proxy tools, mobile emulators, and QA environments.

Risk Assessment

- **Client Environment Profiling**: Before engagements, clients' assets and threat models are mapped.
- **Internal Risk Assessment**: Regular reviews assess risks associated with internal systems, such as exposed test networks or misconfigured VMs.

---

3. Protect

The **Protect** function ensures safeguards are in place to secure critical services and limit cybersecurity events.

Access Control

- Role-based access to test environments and client reports.
- MFA enforced on all endpoints and cloud accounts.

Data Security

- Encryption at rest and in transit using AES-256 and TLS 1.3.
- Segregation of client data in isolated test environments.

Secure Configuration

- Hardened VM baselines used for engagements.
- Mobile devices and testing rigs are regularly patched and monitored.

Awareness and Training

- Staff undergo continuous training in secure development, exploit chaining, mobile security, and secure code review best practices.

---

4. Detect

The **Detect** function involves identifying the occurrence of a cybersecurity event in a timely manner.

Continuous Monitoring

- VM networks and test environments are continuously logged and monitored.
- Detection rules in place to monitor unauthorized access or malware callbacks during Red Team simulations.

Threat Intelligence Integration

- TTPs aligned with MITRE ATT&CK are tracked in Red Team engagements.
- Public CVE feeds and exploit kits are integrated into vulnerability scanners and pentesting workflows.

---

5. Respond

The **Respond** function details the necessary steps to take after a cybersecurity event is detected.

Incident Response Plan

- A documented response strategy covers client-side simulations (e.g., breach simulations in Red Team ops) and internal lab incidents.
- Defined containment strategies for misfired exploits or test malware escaping a sandbox.

Communications

- Secure, encrypted communication channels (e.g., Signal, ProtonMail) are used for client reports, especially during ongoing Red Team engagements.
- Coordination with clients during time-sensitive vulnerabilities includes real-time patch guidance.

6. Recover

The **Recover** function outlines activities to maintain plans for resilience and restore capabilities or services impaired due to a cybersecurity event.

Recovery Planning

- Backups of VMs, configurations, and client documentation are stored securely and tested monthly.
- Environmental snapshots are taken before tests to allow full rollback if compromise or failure occurs.

Improvements

- Post-engagement reviews are conducted for every penetration test and Red Team project to refine methodologies.
- Lessons learned from each vulnerability assessment or QA failure are integrated into future VULN/SQA checklists.

Service Mapping Across the NIST CSF

NIST Function	**Penetration Testing**	**Vulnerability Assessment**	**Red Team Operations**	**Secure Software QA**
Govern	Rules of Engagement, NDA	Policy-driven scan rules	Legal/compliance scope	SDLC policy integration
Identify	Reconnaissance tools, asset maps	Risk-based asset prioritization	Threat model mapping	Dependency and code base inventory
Protect	Privilege separation, VM containment	Data and service hardening suggestions	OPSEC planning, secure tooling	Secure coding, static analysis tools
Detect	Payload behavior analysis	Exploit pattern detection	Alert monitoring tests	CI/CD scan triggers

NIST Function	**Penetration Testing**	**Vulnerability Assessment**	**Red Team Operations**	**Secure Software QA**
Respond	Real-time patch guidance	Risk reporting	Incident simulation	Secure bug reporting workflows
Recover	System baseline restoration	Re-assessment after remediation	Retest after breach simulation	Regression testing post-remediation