WHITE PAPER: Mycelium RF Analysis Framework

Extending Security and Compliance Automation to the RF Spectrum

1. Executive Summary

Adlumin's platform provides unparalleled value through its focus on security and compliance automation. However, a critical piece of the compliance puzzle remains a manual, point-in-time effort: the security of wireless devices. The Cyber Grove has developed Mycelium, a scriptable RF analysis engine that can extend Adlumin's automation capabilities to the RF spectrum. By integrating Mycelium, Adlumin can offer a revolutionary new feature: the ability to automatically test and validate the security of wireless controls, providing continuous compliance for a threat surface that has, until now, been a complete black box for automated platforms.

2. The Challenge: The Manual Gap in Automated Compliance

Automated compliance is the goal, but the reality is that many controls still require manual, periodic testing. This is especially true for wireless systems.

- **The Compliance Blind Spot:** Compliance frameworks like PCI-DSS, HIPAA, and NERC CIP have strict requirements for physical and network access controls. Yet, the wireless physical access systems, medical telemetry devices, and industrial controls that fall under these frameworks are often invisible to automated scanning platforms.
- **The Inability to Automate Wireless Tests:** How do you automatically verify that a building's wireless door locks are not vulnerable to a simple replay attack? Or that data from a patient's wireless medical device is properly encrypted? This is typically a costly, manual test performed by specialists, which is the antithesis of the continuous compliance model.
- **Lack of Verifiable Evidence:** Compliance hinges on evidence. Without a way to automatically test and document vulnerabilities in the RF layer, organizations have a significant, unverified gap in their compliance posture and audit records.

3. The Solution: Mycelium as a Compliance Automation Engine

Mycelium is designed to be a powerful **RF automation engine** that can be driven by a platform like Adlumin's. By integrating Mycelium, Adlumin can translate compliance requirements into automated, scriptable tests that run continuously.

- **From Manual to Automated:** Convert manual RF security and compliance checks into "compliance playbooks." These are simple Mycelium scripts that can be executed on-demand by the Adlumin platform to test specific controls.
- **Continuous Compliance for Wireless:** Enable customers to move from expensive, point-in-time wireless penetration tests to a model of continuous, automated validation of their wireless security posture.

- **Generate Actionable Evidence:** When a test fails, Mycelium can automatically log the failure and provide the specific data (e.g., the captured unencrypted packet, the replayed signal) as concrete evidence. This data can be streamed directly into the Adlumin dashboard, creating an undeniable, actionable finding.
- **Expand Your Platform's Reach:** Offer a unique, compelling feature that no other compliance automation platform has: the ability to reach beyond the network and into the RF spectrum.

4. Use Case: Automated PCI Compliance Check for Physical Access

A financial services client uses Adlumin for automated PCI-DSS compliance monitoring.

1. **The Playbook:** The Adlumin platform, as part of a scheduled PCI compliance audit, triggers a Mycelium sensor deployed near the client's data center. The platform instructs Mycelium to run the "PCI-Req-9.1.1-Physical-Access-Test" playbook.
2. **The Test:** The Mycelium script automatically targets the wireless frequencies used by the data center's door access card readers. It attempts a series of common attacks, including a replay attack.
3. **The Finding:** Mycelium successfully captures and replays a signal to unlock a door. It immediately logs this failure.
4. **The Evidence:** Mycelium sends a structured "Compliance Failure: PCI DSS Req 9.1.1" alert to the Adlumin dashboard. The alert includes the timestamp, the targeted asset (Door Reader #4), the vulnerability (Replay Attack Successful), and a copy of the captured signal data as evidence. The SOC team now has an automated, verifiable, and actionable compliance failure to address.

5. About The Cyber Grove

The Cyber Grove is a Maryland-based small business focused on creating powerful automation technologies for cybersecurity and compliance leaders.

6. Partnership Proposal

We believe that integrating Mycelium's RF automation engine will provide Adlumin with a powerful and unique competitive differentiator. This partnership would allow you to offer the industry's first automated compliance validation for the wireless spectrum.

We propose a technical discussion with your product and engineering leadership to explore how Mycelium's capabilities can be integrated into your platform.

Contact: brent.wood@thecybergrove.com **Website:** https://www.thecybergrove.com