FireEye
SECURITY REIMAGINED

FireEye Threat Analytics Platform (TAP) and Lieberman

Enables Automated Intrusion Detection and Response

SOLUTION BRIEF

SECURITY REIMAGINED

INTEGRATED SOLUTION HIGHLIGHTS

- **Proactive Protection:** Ensures a constant, evolving defense against attackers, limiting their ability to gain and maintain anonymous access to critical systems.
- **Limits Cyber Intrusions:** Guarantees that threats don't spread to dependent systems and mitigates the scope of damage that can occur.
- **Real-Time Threat Response:** Eliminates the need for IT to intervene when FireEye Threat Analytics Platform (TAP) detects threats by providing automated, real-time credential rotation.

OVERVIEW

Despite compelling evidence that IT networks are under increasing danger from persistent and sophisticated threats, many IT security managers continue to gamble with their organization's data network security.

A recent survey by Lieberman Software Corporation revealed that 92 percent of IT security professionals believe that cyber security drills are a good way to prepare for cyber attacks. However, 63 percent of those surveyed admitted that their organizations never run such drills, or only do so annually.

This posture is insufficient to assure network security and to keep pace with evolving threats. In today's threat landscape, organizations are attacked continuously. Organizations that fail to maintain a vigilant posture will most certainly suffer the devastating consequences of preventable security breaches.

LIEBERMANSOFTWARE™

The same survey reveals that what we see in the press is just a glimpse of reality. A full 87 percent of IT professionals stated that they believe large financial hacks are happening more often than reported, and right under the nose of security auditors.

THE CHALLENGE

Unprotected datacenters could be home to thousands of vulnerable privileged accounts, including:

- Stale, shared, and misconfigured administrative logins.
- Hardware and application instances with unchanged default logins.
- Poorly secured and easily cracked privileged credentials in service accounts, VM hypervisors, and network appliances.

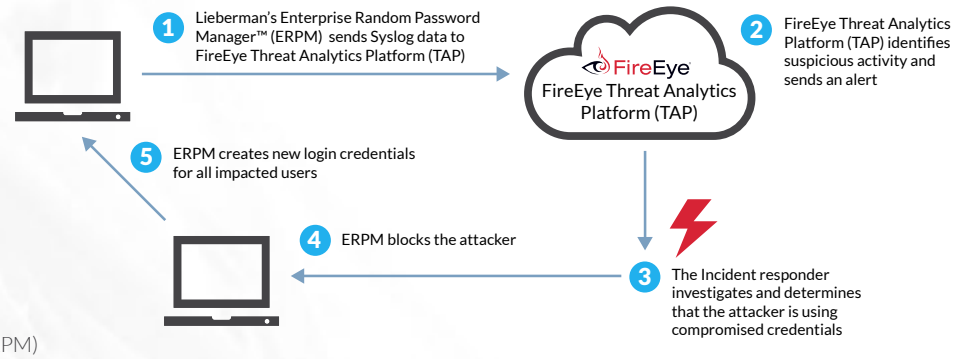
These may lead to security holes that leave the network vulnerable to cyber attacks and insider threats.

The challenge for IT security professionals is to identify these potential security holes and close them. If a breach does occur, the additional challenge is to identify it quickly and prevent further damage until they can fix the vulnerability.

A process of manual identification and remediation is inadequate to address today's threats. A constant, vigilant, and automated process is required.

THE INTEGRATED SOLUTION

Lieberman Software and FireEye have collaborated to deliver a market first: A uniquely new integrated, automated capability designed to significantly improve data breach remediation response time and lower cybersecurity risk for enterprises.



FIREEYE PRODUCT AND VERSION

FireEye Threat Analytics Platform (TAP)

LIEBERMAN PRODUCT AND VERSION

Enterprise Random Password Manager™ (ERPM)

For the first time, Lieberman Software and FireEye enable a sophisticated new level of automated defense against "land & expand" cybersecurity attacks. This protection is accomplished via real-time monitoring of FireEye's Threat Analytics Platform (TAP) data feed, which can trigger automated, rapid rotation of the "privileged attack surface" credentials during an actual breach incident. Real-time, rapid rotation provides isolation and containment of hackers and malware in the affected domain, geographical region, or IT asset class. What used to take days can now be done in minutes.

HOW THE JOINT SOLUTION WORKS TOGETHER

The FireEye Threat Analytics Platform (TAP) consumes Lieberman Enterprise Random Password Manager (ERPM) Syslog output in JSON format, adding this critical privileged identity and access management context to the FireEye Threat Analytics Platform (TAP) analytical view for analysis and correlation.

The Lieberman Enterprise Random Password Manager (ERPM) continuously polls the feed from FireEye Threat Analytics Platform (TAP) to monitor the environment for data breach confirmation.

Specifically, when a threat is detected and reported by FireEye Threat Analytics Platform (TAP), Lieberman Enterprise Random Password Manager (ERPM):

- Immediately changes credentials to stop a breach in progress when FireEye Threat Analytics Platform (TAP) detects an intrusion. This detection effectively moves the 'attack surface' and provides immediate isolation and containment of the data breach threat.
- Delivers real-time automated credential management to accelerate responses to threats.
- Maintains an active defense by automatically rotating credentials on a schedule.
- Adds and continually tracks all systems found within the environment to eliminate blind spots, manage, monitor, report, and control the privileged access that SIEM systems can't detect on their own.
- Addresses threats across dependent systems and accounts to ensure threats don't spread.

THE VALUE OF THIS PARTNERSHIP

By natively integrating with FireEye's widely-accepted Threat Analytics Platform (TAP), Lieberman's Enterprise Random Password Manager (ERPM) delivers automated, 'closed loop' integration and enables automated intrusion response for joint customers. When combined, these cyber security partners deliver a new and uniquely integrated, automated capability designed to significantly improve data breach remediation response time and lower cybersecurity risk for enterprises.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. FireEye has over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000.

ABOUT LIEBERMAN

Lieberman Software proactively mitigates cyber attacks that bypass conventional enterprise defenses and penetrate the network perimeter. By delivering an adaptive identity threat response in real-time, the company continuously secures customer environments, countering malicious attacks from the outside, and within. Many of the largest businesses and governments across the globe trust Lieberman Software to secure their assets, protect their finances, and guard their reputation.

For more information contact CSC@fireeye.com.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**