PALO ALTO NETWORKS AND LIBRAESVA

Email Security IoC Feed Integration

Benefits of the Integration

- Share IoC feeds from Libra ESVA with Palo Alto Networks Next-Generation Firewall via MineMeld.
- Simplify workflows for blocking IoCs without spending additional resources to manage block lists, including automated timeout of expired indicators.

The number of new malware variants grows daily, and cybercriminals constantly find new ways to infiltrate systems. With so many attack vectors, security products must work together to stop advanced threats. Through sharing and collaboration between enterprise security tools, organizations can build a better understanding of their attack surface as well as take advantage of information and intelligence collected by the security products to improve overall protection against cyberthreats.

Libraesva

Libraesva's award-winning technology – its email security virtual appliance, Libra ESVA – uses a simple, pragmatic approach to stop email-borne threats. The Libra ESVA suite provides security, continuity and compliance offerings that include:

- **Email Security Gateway** – filters out email traffic that contains malicious links or attachments.
- **Email Load Balancer** – optimizes and balances the performance and efficiency of email traffic.
- **Email archiving** – saves and protects data contained in email messages to enable fast retrieval and ensure compliance is met.
- **Threat intelligence** – correlates threat intelligence, including sandboxing analysis results and dangerous URLs, from all Libra ESVA appliances globally and can compare the statistics as well as performance of the appliances.

Palo Alto Networks

The Palo Alto Networks® Security Operating Platform prevents successful cyberattacks by harnessing analytics to automate routine tasks and enforcement. Tight integration across the platform and with partners simplifies security so you can secure users, applications and data. The platform empowers you to confidently automate threat identification and enforcement across cloud, network and endpoints using a data-driven approach and precise analytics. It blocks exploits, ransomware, malware and fileless attacks to minimize infections of endpoints and servers. The platform also lets you easily adopt best practices and take a Zero Trust approach to reducing opportunities for attack.

Palo Alto Networks and Libraesva

Libraesva extends the market-leading capabilities of the Security Operating Platform by delivering a rich email security threat feed to improve the blocking of malicious domains, attachments and anti-spoofing-based attacks.

The Libraesva and Palo Alto Networks integration provides:

- Highly accurate and corroborated threat detection by continuously providing Palo Alto Networks next-generation firewalls with indicators of compromise, or IoCs, captured by the Libra ESVA email security appliance. Many of these IoCs are unknown to any other sources.
- Identification of malicious activity, such as data exfiltration attempts, compromised user accounts and rogue processes.
- Automated, streamlined incident response to reduce organizational risk and stop threats by capturing malicious domains and adding them to a Palo Alto Networks Next-Generation Firewall policy.

Use Case No. 1: Detect and Block Zero-Day Phishing

Challenge

It's widely known that the preferred vector for infections is email. Zero-day phishing makes no exception. Newly compromised websites hosting zero-day phishing pages are spread to users via malspam campaigns that can reach users' email inboxes.

Answer

The Libra ESVA URLSand Sandbox rewrites email links and collects a fresh, real-time feed of newly compromised websites delivered through email. Integrating this feed with Palo Alto Networks Next-Generation Firewall policy blocks network access to these websites. Additionally, an organization can send files and URLs to Palo Alto Networks WildFire® malware prevention service to complement the Libra ESVA Malware Feed.

Benefit

Protection against zero-day phishing with the Libra ESVA Phishing Feed increases detection of zero-day compromised website URLs delivered via email.

Use Case No. 2: Block Network Access to Zero-Day Malware

Challenge

One of the most common techniques used to deliver zero-day malware is forcing users to download content from a compromised website. More than 90 percent of these advanced threats start with an email that slips through most filters because it appears to originate from a legitimate sender.

Answer

By rewriting all email links and pointing them to the Libra ESVA Cloud Sandbox, URLSand collects real-time IoCs of droppers used to download malware. Integrating these IoCs with Palo Alto Networks next-generation firewalls, through Palo Alto Networks MineMeld™ threat intelligence syndication engine, prevents network access to these websites. Additionally, organizations can send files and URLs to WildFire to complement the Libra ESVA Malware Feed.

Benefit

Protection against zero-day malware with the Libra ESVA Malware Feed and WildFire increases detection of zero-day compromised website URLs delivered via email and the network.

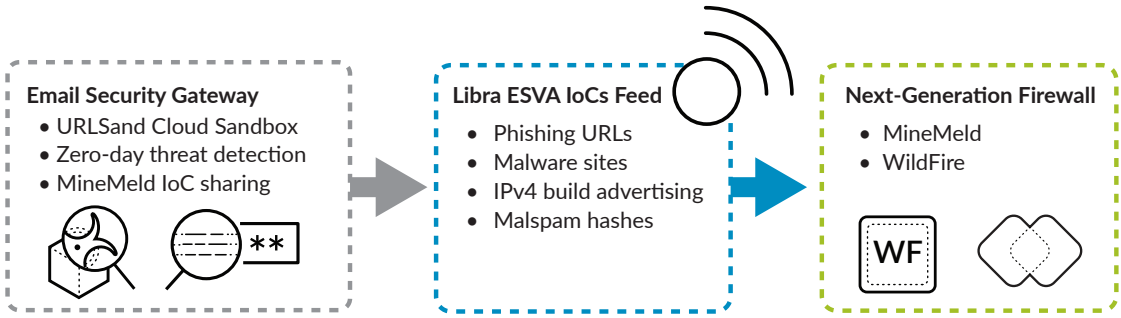

Figure 1: Palo Alto Networks and Libraesva integration

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com