Lastline and Cofense

Advanced Detection and Response

Cofense™ and Lastline® accelerate phishing incident detection and response. Lastline Analyst™ quickly integrates with your Cofense Triage™ system to provide unmatched, evidence-based malware detection of suspicious files and URLs in emails. In less than 60 seconds, you can activate Lastline's industry-leading detection technology to your Cofense Triage deployment.

The latest Verizon Data Breach Investigations Report reported that "phishing emails and malware are a potent and pervasive one-two punch" with "95% of phishing attacks that lead to a breach were followed by an installation of malware and that 66% of malware was installed via infected email attachments."[1]

Cofense Triage is the first phishing-specific incident response platform that allows security operations centers (SOC) and incident responders to automate the prioritization, analysis, and response to phishing threats that bypass your secure email gateway. It gives you the visibility and analytics you need to speed processing and response to employee reported phishing threats and decrease your risk of breach.

Speed Your Phishing Incident Detection and Response:

- Unique and comprehensive phishing-specific incident response solution
- Actionable threat intelligence from Lastline with highest levels of accuracy
- Highest accuracy and unmatched malware analysis with Lastline Deep Content Inspection
- Allows you to cluster threats based on rules that triggered them
- Mutually supported SIEM, TIP, and SOAR integrations
- Allows incident responders to share results with upstream security teams to prevent future attacks

The Power of Partnership

Cofense delivers a comprehensive human phishing defense solution focused on engaging employees to be part of the defense after a malicious email bypasses your perimeter defenses. It enables incident response teams to better identify, verify, and respond to targeted phishing attacks.

Lastline delivers unmatched malware detection. Lastline's detection engine provides complete visibility into the malicious behavior that slips past other technologies. It uses Deep Content Inspection™, a unique isolation and inspection environment that simulates an entire host (including the CPU, system memory, and all devices) to analyze malware. Deep Content Inspection interacts with the malware to observe all the actions a malicious object might take. Other malware detection technologies like virtualized sandboxes only have visibility down to the operating system level. They can inspect content and identify potentially malicious code, but they can't interact with the malware to the depth that the Lastline detection engine can. As a result, they have significantly lower detection rates and higher false positives, in addition to being easily identified and evaded by advanced malware.

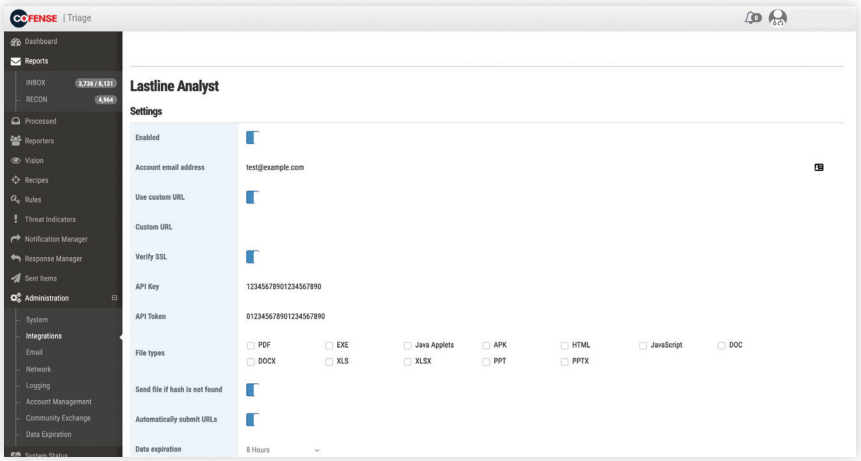
How it Works

To stay ahead of advanced email attacks, Cofense Triage can leverage the power of Lastline's advanced malware detection. Installation is fast and seamless—simply add your Lastline credentials to the Cofense Triage interface for bidirectional integration with Lastline's Global Threat Intelligence and best-in-class sandbox technology.

[1] 2017 Data Breach Investigations Report 10th Edition, Verizon

Cofense Triage provides customers out-of-the-box capabilities to analyze suspicious email at ingestion. As emails are received by Cofense Triage, they are automatically clustered together and prioritized. Cofense Triage analyzes employee-reported email based on the attributes of the email through:

- YARA rule matching
- reputation of the employee reporting
- threat intelligence
- malware analysis by Lastline



With Lastline, mutual customers can choose to configure Cofense Triage to send files hashes, URLs, and attachments to Lastline for inspection.

Together Cofense and Lastline dramatically reduce phishing susceptibility. Additionally, security teams benefit by making the most of their technologies that optimize their return on security investment.

About Lastline

Lastline provides breach protection products that are innovating the way companies defend against advanced malware-based network breaches. We deliver the visibility, context, analysis, and integrations enterprise security teams need to quickly detect and defeat sophisticated malware-based threats before a damaging and costly data breach occurs. Headquartered in Redwood City, California with offices throughout North America, Europe and Asia, Lastline's technology is used by Global 5000 enterprises, is offered directly and through resellers and security service providers, and is integrated into leading third-party security technologies worldwide. www.lastline.com.

About Cofense

Cofense™, formerly PhishMe®, is the leading provider of human-driven phishing defense solutions world-wide. Cofense delivers a collaborative approach to cybersecurity by enabling organization-wide engagement to active email threats. Our collective defense suite combines timely attack intelligence sourced from employees with best-in-class incident response technologies to stop attacks faster and stay ahead of breaches. Cofense customers include Global 1000 organizations in defense, energy, financial services, healthcare and manufacturing sectors that understand how changing user behavior will improve security, aid incident response and reduce the risk of compromise.

Experience the **Lastline Advantage**

For more information please **visit www.lastline.com**

Lastline, Inc.
1825 S. Grant Street, Suite 635
San Mateo, CA 94402

Americas: +1 877 671 3239
www.lastline.com
info@lastline.com