Stairwell for Financial Services

A new way to detect threats missed by others

Financial services organizations are often at the forefront of implementing the latest technology and security solutions to safeguard their systems and customer information from malicious actors. This is because they understand the information they store and process for their customers must be kept safe to ensure trust is in place, allowing customers to have confidence in the organizations they conduct financial business with. They know that as threats evolve, so too must the technology and processes used by defenders.

Stairwell understands the pressures financial services security teams face and is here to help by taking a whole new approach to detect and identify both known and unknown threats. Stairwell is helping financial services organizations assess whether their enterprise has been impacted by a threat and provides their IT/security teams with advanced analysis to take immediate action with capabilities that cannot be bypassed or evaded by attackers.

How Stairwell helps financial organizations detect & respond to threats:

- **Swift Identification:** Rapidly identify unknown threats and variants that EDR misses
- **Proactive Deployment:** Quickly deploy advanced analysis, even on systems not covered by other security tools
- **Automation:** Streamlining processes through automated tasks, such as using prebuilt YARA queries for vulnerability identification at 10x the speed
- **Timely Remediation:** Enabling prompt remediation by identifying exposed devices within seconds of an IOC / exploit notification
- **Comprehensive Analysis:** Providing advanced analysis with detailed malware file assessments and associated observations
- **Environment Assessment:** Facilitating quick and comprehensive assessments, allowing timely responses to management/regulators without retention concerns

The latest malware or 3rd-party vulnerability - Am I impacted?

Stairwell is able to swiftly identify emerging threats and active exploits, often before the security/IT team is aware of a potential exposure within their organization. Our financial services clients, as illustrated by a case involving the Citrix Bleed exploitation, have firsthand experience of Stairwell's speed and detection capabilities.

Stairwell for Financial Services

Within minutes, Stairwell can accomplish a comprehensive environment assessment — a task that traditionally consumes days or even weeks through manual audits, enabling our financial services customers to respond promptly to management and regulators regarding third-party vulnerabilities like the Log4j exploit, showcasing a rapid and effective security posture.

Continuous analysis - finding unknowns and variants

What might be known today was not known yesterday or a week ago or even months ago. Stairwell is able to continuously and automatically analyze every executable or executable-like file at the binary level for every file that has ever been ingested since becoming a customer as there are no retention limits.

Stairwell automatically identifies malware files (and their variants) within financial service organizations that were previously not identified as malicious based upon the latest threat intelligence received. The security team is now able to know exactly which file is malicious, where it was located, and provide detailed analysis on the malware identified allowing the security team to assess risk and respond accordingly.

Sharing threats across the financial services industry

The attacks pointed at financial services organizations are often different from those directed at retailers or healthcare providers. Stairwell helps financial services organizations stay abreast of the latest attacks with a private malware sharing environment that can be used among trusted financial service group members to safely and easily share not just IoC details but the actual files themselves.

With this safe and private way to share the latest threat details, your security team will be able to get immediate detailed analysis of malware in use at another financial services organization.

Summary

With unique industry requirements, Stairwell understands financial services organizations need to take extra measures to not only meet multiple regulatory requirements but they must go above and beyond to protect their customers financial information from malicious actors. Stairwell is here to help our customers take immediate action against threats or exploits and is switching up the game by taking a whole new approach to detecting threats missed by others. If you would like to learn more, please reach out as we'd be more than happy to have a chat and discuss how Stairwell can help protect your organization from the latest threats.