Automated Quarantine of Under-Attack and High-Risk Network Segments to Contain the Spread of Infection and Empower Security Teams to Get Ahead of Advanced Threats

Business Problem

By exploiting vulnerabilities, attackers are compromising systems and spreading across networks to further infect assets until reaching critical systems.

Organizations struggle to prioritize high-risk assets for remediation and contain network segments that have been identified as infected.

The ability to restrict and prevent the spread of malware and quick patching of highly vulnerable systems can make the difference in the race to prevent an attack campaign from being successful.

Leveraging Frontline.Cloud for agentless real-time vulnerability risk assessment and threat scanning, and Cortex XSOAR for orchestration and automation of data enrichment and response, gives security teams the ability to take immediate steps to remediate threats before they can reach your critical data.

Solution: Overview

Digital Defense’s Frontline.Cloud platform has been purpose-built to be deployed and operate in today’s hybrid cloud enterprise environments. Frontline. Cloud is hosted on Amazon Web Services (AWS) and incorporates Digital Defense’s patented and proprietary technology that supports multiple software security systems focused on pro-actively protecting business critical assets. The Frontline.Cloud Software as a Service (SaaS) platform supports Frontline Vulnerability Manager™ (Frontline VM™), Frontline Web Application Scanning™ (Frontline WAS™), and Frontline Active Threat Sweep™ (Frontline ATS™), leveraging multiple patents that eliminate the deficiencies in similar solutions that are also traditionally based on hardware appliances. Frontline.Cloud is the only solution in the market that can scale to operate on premise, in the cloud, or in hybrid network-based implementations to fit the needs of organizations of any size, including even the largest financial, government, healthcare, retail and utility providers in the world.

Benefits

Agentless Assessment
Vulnerability and threat data of network segments during an active outbreak and/or at high-risk are ingested by Cortex XSOAR for playbook-driven data enrichment and response.

Rapid Investigation
Speed analyst investigation with threat and vulnerability context data for given assets within the infected area.

Automated Response
Automated key tasks allow for immediate quarantine and remediation of a network domain or segment to prevent further infection or new compromise of systems.

Compatibility

Frontline.cloud supports: Frontline Vulnerability Manager™ (Frontline VM™), Frontline Web Application Scanning™ (Frontline WAS™), and Frontline Active Threat Sweep™ (Frontline ATS™)
Frontline.Cloud, the industry’s only true on-demand SaaS-based vulnerability and threat assessment solution, helps security teams prioritize the most important assets to both identify active infections and pro-actively harden against an attack. Utilizing data from Frontline.Cloud and Palo Alto Networks Cortex XDR, Frontline.Cloud works with Cortex XSOAR to enable security teams to not only identify and remediate high-risk and/or compromised assets but also to provide actionable steps to prevent the spread of an infection into more sensitive areas.

Cortex XSOAR is the industry-leading Security Orchestration, Automation & Response (SOAR) technology by Palo Alto Networks that will automate up to 95% of all response actions requiring human review and allow overloaded security teams to focus on the actions that really require their attention. With Frontline.Cloud and Cortex XSOAR, Palo Alto Networks customers can now leverage on-demand vulnerability and active threat information to identify, prioritize and quarantine highly vulnerable or infected assets to allow security teams to remediate and patch systems before an infection can spread to other parts of the network.

**Solution: Summary**

- Assess a set of assets within a network segment or specific domain that are under active threat, infected, or at high risk of exploitation
- Automate the ingestion of vulnerabilities affecting your asset inventory within XSOAR for automated playbook-driven data enrichment and response.
- Leverage hundreds of Cortex XSOAR third-party product integrations to coordinate response across security tools based on insights from Frontline.Cloud
- Run 100s of commands (including for Frontline.Cloud) interactively via a ChatOps interface while collaborating with other analysts and Cortex XSOAR’s chatbot
Solution: Description

Automated, Real-time Monitoring of Assets for Infections, Active Threats, and Vulnerabilities

Digital Defense Frontline.Cloud provides an on-demand real-time assessment of vulnerable systems that can be exploited, but also actively identifies infected hosts. Along with using Frontline ATS, for active threat detection, users can also leverage our additional integration with Palo Alto Networks Cortex XDR. Frontline.Cloud is the first vulnerability management solution that can correlate threat information from Cortex XDR with operating system and web application vulnerabilities to provide security teams with additional context and better prioritize remediation of critical assets under active attack through Cortex XSOAR.

Benefit: Lightweight on-demand scanning for vulnerabilities and identification of threats generate results that trigger playbook response to speed remediation in real-time and prevent breaches.

Immediate Quarantine of High-Risk and/or Actively Infected Assets

Digital Defense Frontline.Cloud working with Cortex XSOAR provides a playbook for changing policies (at the push of a button or automatically) on Palo Alto Networks Next Generation Firewalls to temporarily quarantine or isolate network segments, or specific domains that are at high-risk or under active attack.

Benefit: Gives security teams the time needed to respond to highly vulnerable or already infected hosts, while preventing the spread of infection. This reduces response time, while also reducing impact to the rest of the network, and greatly minimizes the potential for a breach.

Learn More

To learn more about the advantages of the Digital Defense, Inc. Frontline.Cloud with Cortex XSOAR:

Sales can be reached at: sales@digitaldefense.com

Technical support questions can be directed to: integrations@digitaldefense.com

Next-Generation Firewall Remediation
About Digital Defense, Inc.
Founded in 1999, Digital Defense, Inc. is an industry recognized provider of security assessment solutions. Digital Defense provides vulnerability and threat assessment Software-as-a-Service (SaaS) solutions and services purpose-built to operate in today's hybrid cloud enterprise environments. Digital Defense's proprietary platform, Frontline.Cloud, incorporates patented technologies and offers multiple software security systems focused on pro-actively hardening business critical assets from being compromised and breached. The Frontline.Cloud platform supports Frontline Vulnerability ManagerTM (Frontline VMTM), Frontline Web Application ScanningTM (Frontline WASTM), and Frontline Active Threat SweepTM (Frontline ATSTM), that provide agentless discovery, vulnerability and threat assessment of dynamic assets, while eliminating manual processes and integrating with market-leading 3rd party security and IT offerings to eliminate gaps in visibility and enable faster remediation. Frontline.Cloud is the only solution in the market that is built to be scaled across any size organization and operate on premise, in the cloud or in hybrid network-based implementations.

For more information, visit https://www.digitaldefense.com/

About Cortex XSOAR
Cortex XSOAR, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity.

For more information, visit https://www.paloaltonetworks.com/cortex/xsoar.