FIREEYE SECURITY ORCHESTRATOR

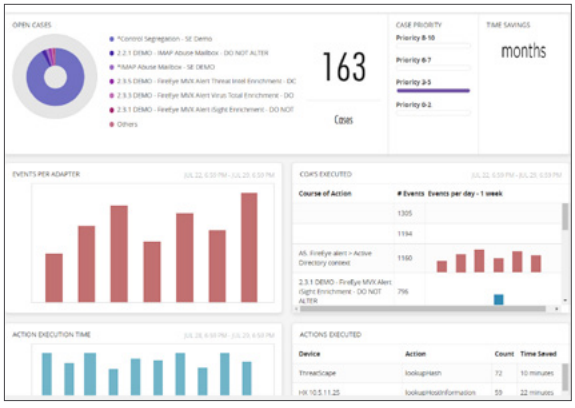
INTEGRATE AND AUTOMATE TECHNOLOGIES AND INCIDENT HANDLING PROCESSES ACROSS YOUR IT INFRASTRUCTURE

OVERVIEW

Cyber-attack volume has never been higher, and if your defenses can't keep up, you dramatically increase your risk of a breach. Attackers have the intellectual resources, the computing power, and the backbone of the fastest digital delivery networks. They can iterate on your defenses at will, changing their attack signature, morphing to new delivery methods, constantly changing how they approach the problem of infiltrating your network. They can do this all day, every day. When you factor in the volume of alerts that most SOCs contend with on a daily basis and the fact that you can't find the resources to man those SOCs, a traditional program relying on manual intervention and containment faces an asymmetric fight.

FireEye Security Orchestrator accelerates and simplifies the threat detection and response process by unifying disparate technologies and incident handling processes into a single console that delivers real-time guided responses to improve response times, reduce risk exposure, and maintain process consistency across a security program. FireEye's years of expertise battling the world's most consequential breaches has helped to hone effective processes to detect, investigate and respond to threats. FireEye Security Orchestrator enables you to overlay those best practices on to data from your FireEye deployment, SIEM and other enterprise technologies.

FireEye Security Orchestrator can affect changes at the network, host and application levels, and even to physical access-control systems. The ability to respond in seconds effectively stops the intruder in their tracks



BENEFITS

- Enhance security team capability with deployment, design and pre-built playbooks from the team with the decade-long visibility at the front lines of major cyber attack investigations
- Eliminate errors through standardized process and automation while reducing time demands on already stretched SOC teams
- Allow the SOC teams to reduce risk with quicker response times and allowing them to focus on higher priority tasks that can further improve your risk posture — like hunting
- Centralized dashboards and case management to anchor your security operations process

FireEye
SECURITY REIMAGINED

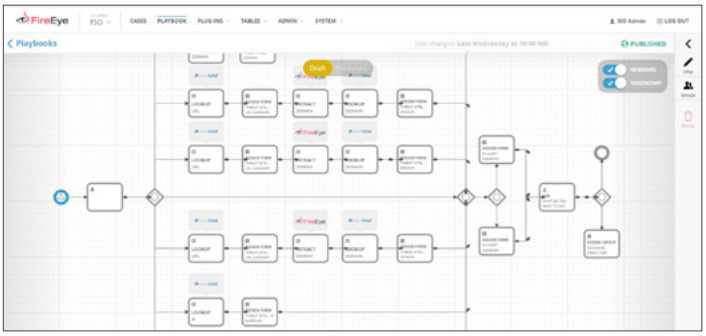
and closes the doors, limiting the damage and the risk to the organization. With FireEye Security Orchestrator, you save time and resources by unifying incident-related data and your security technologies under a single security operations platform.

Our customers signficantly reduce response times and eliminate process errors, ultimately reducing their overall risk exposure.

KEY FEATURES

Incident Response Playbooks

Incident Response Playbooks, also known as Courses of Action (CoA), codify security operations into human-led workflows and automated tasks. With your SOC processes documented, automated, and enhanced with FireEye's expertise fighting the world's most advanced attacks, your response times will decrease while maintaining process consistency across a security program.



Use the new CoA Builder to create smart, branching workflows that match how your organization's security policy and support infrastructure work. It comes with a full portfolio of pre-built plug-ins and workflows across the tools in your security operations like your SIEM, firewall, Threat Intelligence, IPS and ticketing systems. It then enables the creation of workflows that are customized to your organization's security policies and support infrastructure. With playbooks, you can deconstruct security analyst workflows into a fully or partially automated sequence of tasks, with the ability to solicit analyst feedback used to inform the direction of a given workflow.

The end result will be a smoothly operating environment with security workflows developed by and approved by your organization. These changes will be turned into automation workflows that can be initiated automatically, triggered by events in your infrastructure or executed as needed by your SOC staff.

Role-Based Access

Create role based groups and assign granular permissions to individual playbooks or specific steps within the playbook. This way each team has execution access and privileges to read the results of only the workflows that they need. You may use local users and groups, or integrate your Active Directory or Open LDAP directory and assign them to roles in the orchestrator.

Plug-Ins

Integrate, unify and control your IT architecture from a single pane of glass via the plug-in framework. Plug-ins are the connective tissue that joins your devices, applications, services and data into FireEye Security Orchestrator. They are constructed to support some of the most popular security and infrastructure technologies.

This pluggable architecture enables organizations to swap out technology or add in technology with minimal response training and integration. Plug-ins have bi-directional command and control capability to receive data and enact action.

Centralized Dashboards and Advanced Hunting

FireEye Security Orchestrator provides an investigative dashboard to search across security tools and facilitate hunting of threat actors that have targeted your organization. You can also manage cases and quickly pivot from playbooks to additional context across the existing security infrastructure.

In addition, your analysts can also view a centralized dashboard and worldwide threat maps to create an end-to-end, view of data and attacks detected by FireEye appliances within your organization. This view can provide you with both real-time and

historical insights to help drive quick detection and response. You can also conduct in-depth investigations via ultrafast, tiered and highly flexible searches across FireEye alert notification data. This allows you to quickly pivot from an alert to the larger context behind the attack. All of the search dashboards can also be saved and emailed.

Reports

You can create one-time or recurring reports that detail, correlate, and visualize related alerts. Security teams can quickly determine the sources, methodology and targets of an attack, and prevent future reoccurrence. Reports can be customized with:

- Thousands of alert parameters
- Surgical filters
- Various file formats
- Skins with organization-specific graphics
- Professional Services: Orchestration

Customized deployment services are available to design and deploy the FireEye Security Orchestrator into your security program and architecture. These services leverage FireEye expertise to design the proper playbooks based on the technology solutions in your environment and the threats your organization faces each day.

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye