Enterprise Strategy Group | **Getting to the bigger truth.™**

Technical Validation

Fortinet FortiSIEM

A Single Platform for Monitoring and Management of Security and IT

By Tony Palmer, Senior IT Validation Analyst; and Jack Poller, Senior IT Validation Analyst

June 2018

This ESG Lab Report was commissioned by Fortinet and is distributed under license from ESG.

Contents

ESG Validation Reports

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

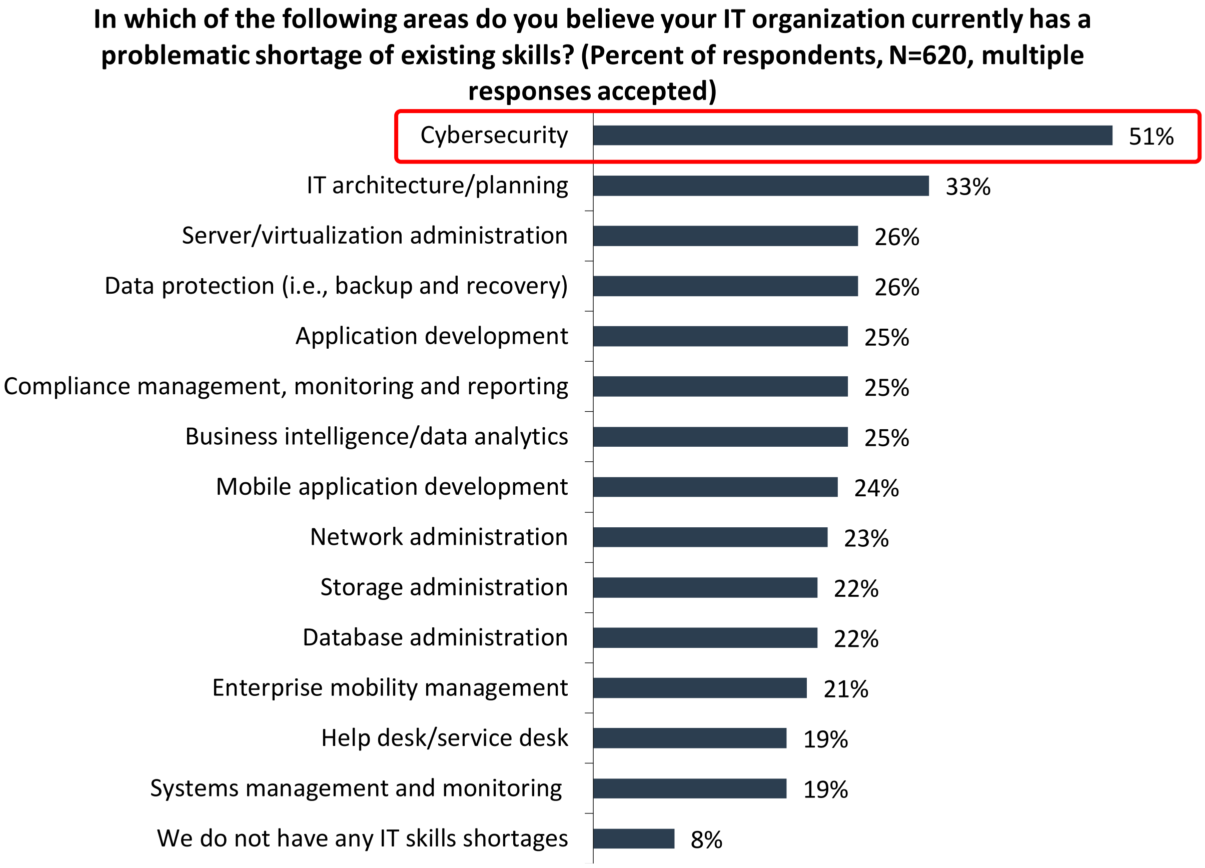
Introduction

This ESG Lab Validation details ESG's hands-on testing of the Fortinet FortiSIEM unified event correlation and risk management platform. ESG Lab focused on validating the ability of FortiSIEM to provide rapid detection and remediation of security, performance, and compliance from a single platform, performing collection and analytics with one engine. Testing was designed to explore how the solution can simplify event identification and remediation for IT teams while providing insight into performance, availability, configuration changes, and compliance.

Background

The ever-increasing volume and velocity of threats has made cybersecurity one of the top IT concerns. Indeed, according to ESG research, strengthening cybersecurity is a business initiative that 44% of respondents—the largest percentage—believe will drive the most technology spending at their organizations over the next 12 months.[1] Complicating the drive to secure their organizations is the global cybersecurity skills shortage—51% of organizations report that they have a problematic shortage of cybersecurity skills in 2018, up from 45% in 2017 (see Figure 1).[2]

Figure 1. Areas of IT Skills Shortage



Source: Enterprise Strategy Group

Because of this perennial skills shortage, organizations are seeking more efficient and effective cybersecurity tools. In the current security model, organizations often attempt to gain efficiency with a security information and event management (SIEM) solution that can provide centralized cybersecurity data collection and analysis.

[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.
[2] Ibid.

What is needed is a solution that:

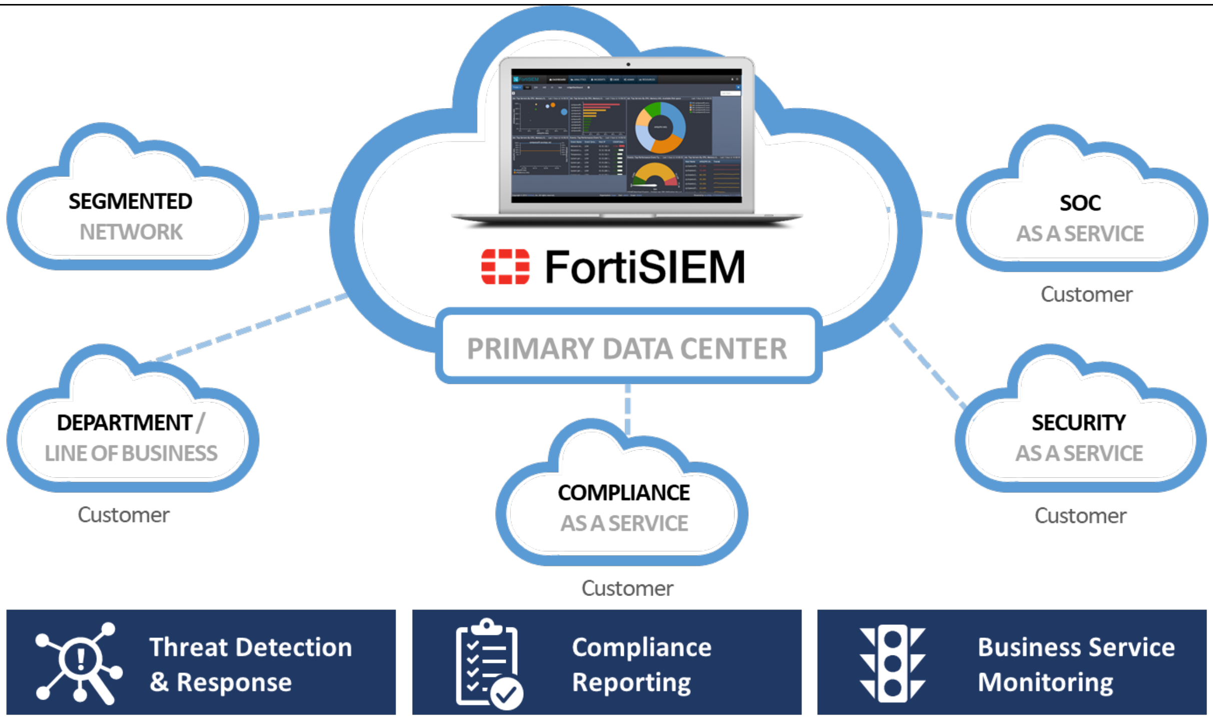
- Can leverage data from the security operations center (SOC), as well as performance, availability, change monitoring, and compliance data from network devices and hosts from the network operations center (NOC).
- Operates in a single network/security ecosystem.
- Provides organizations with the real-time, cross-correlated analytics and intelligence they need to efficiently and effectively secure and manage operations in the modern IT environment.
- Can improve visibility and device discovery to minimize and/or close security gaps from unknown devices.

ESG Lab validated that Fortinet FortiSIEM brings context to security, availability, performance, and compliance data collected across the IT environment. Physical and virtualized systems, network devices, applications, and public and private cloud data are collected and analyzed to provide advanced security and operational intelligence, rapid incident identification and response, and change and compliance monitoring and reporting.

Fortinet FortiSIEM

FortiSIEM is a platform that gives organizations a set of controls for diverse IT teams and can control what each team has access to with granular, role-based access. FortiSIEM is offered as a pre-built, 64-bit virtual appliance that runs in VMware ESX, Amazon Web Services (AWS) AMI, KVM, Microsoft Hyper-V, OpenStack, and Microsoft Azure (collector only) environments. Multiple physical appliance models with varying levels of performance are available to provide a variety of deployment options. The FortiSIEM architecture is a scale-out, enterprise- and service provider-ready, multitenant framework. Each FortiSIEM Collector can monitor more than 10,000 security events per second (EPS) and more than 1,000 devices for performance and availability.

Figure 2. Fortinet FortiSIEM



Source: Enterprise Strategy Group

Multiple appliances can be deployed for larger environments. The customer provides the storage type of their choosing, enabling them to own, manage, and control their historical reporting data. The FortiSIEM Configuration Management Database (CMDB) engine automatically discovers all the elements (devices, applications, users, IoT devices, etc.) connected to the network, and their respective interrelationships. The tool delivers a comprehensive and holistic topology map that continues to self-learn and report on any changes beyond the initial baseline. The FortiSIEM Configuration Management Database (CMDB) is a PostgreSQL database designed for secure access and high performance.

FortiSIEM collects data from thousands of varieties of systems and devices without requiring the use of agents. FortiSIEM offers an optional agent for Windows to provide enhanced functionality over Windows Management Instrumentation (WMI), which includes features such as file integrity checking and the ability to reduce chatter between Windows and FortiSIEM. The appliance-based architecture is inherently scalable to facilitate the addition of appliances or storage on the fly. Below is a brief synopsis of some of the services provided by FortiSIEM:

Statistical Anomaly Detection—FortiSIEM leverages machine-learning algorithms to profile traffic and metrics for all devices on the network, detecting anomalies while learning behaviors.

Threat Intelligence Center—The Threat Intelligence Center enables organizations to aggregate, validate, and share anonymous threat data gathered from the customer base, providing benchmark and threat detection intelligence to customers in near real time.

External Threat Feed—FortiSIEM's open API allows users to integrate public and private threat feeds into FortiSIEM and cross-correlate the data with network and security data collected internally.

File Integrity Monitoring—The optional FortiSIEM Windows agent provides file integrity monitoring and simple deployment to the entire network.

Synthetic Transaction Monitoring—Synthetic transactions are recorded and then replayed to simulate real user input and activity. This process is designed to allow business applications to be tested and monitored the way customers will use them, and to identify problems before they occur in production.

Business Services Dashboard—FortiSIEM offers organizations the ability to associate individual components—servers, network devices, applications, databases, etc.—with the end-user experiences that they deliver, providing a contextualized view into the availability of the business.

ESG Technical Validation

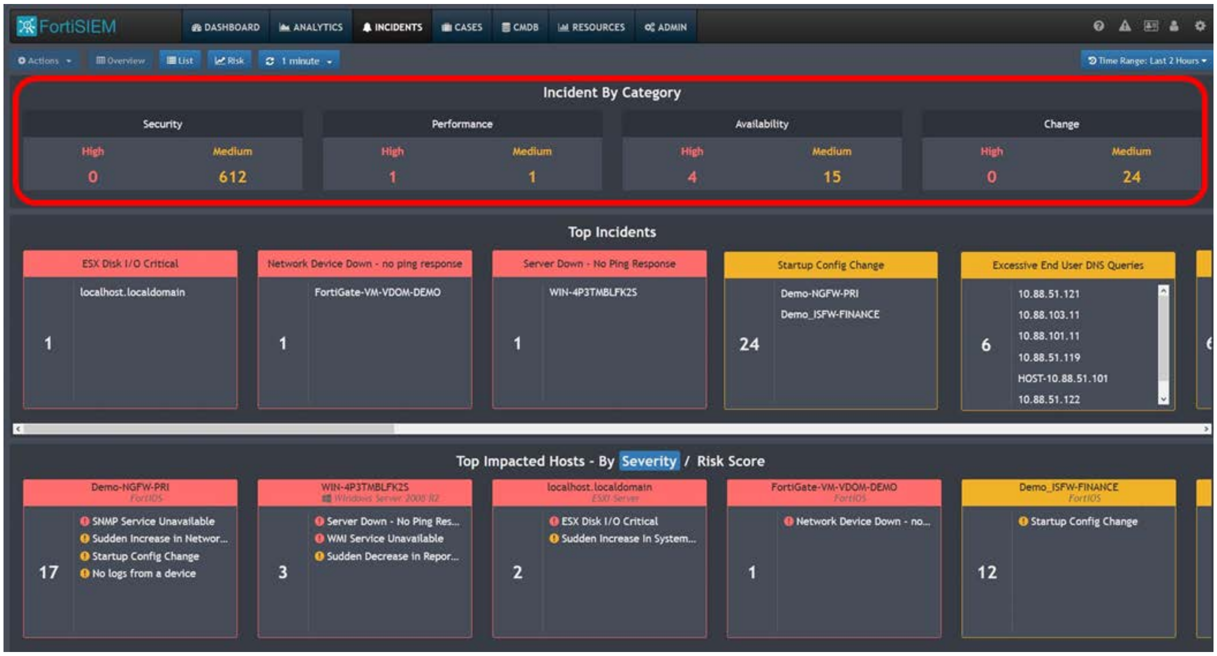
Rapid Detection and Remediation

FortiSIEM is designed to provide rapid detection and remediation of events in the context of security, performance, and compliance management in one tool that can be used by both security and IT teams. Teams access and monitor the resources and/or business services over which they have ownership. Organizations can enter specific credentials for the devices they wish to monitor, and/or scan the network to discover all devices. Once discovered, devices can be categorized and added to business services, so FortiSIEM can scan, monitor, and report incidents.

ESG Testing

ESG Lab began with a look at the FortiSIEM Incident Dashboard. As seen in Figure 3, the Incident Dashboard displays security, performance, availability, and compliance data from diverse, heterogeneous servers, network devices, and applications in one console. In this example, we see a performance alert from an ESX server, availability alerts from a server and a network device, a potential compliance issue of startup configuration changes, and a potential security incident—excessive endpoint DNS queries. Users can filter content based on any functional area from which data is being collected—security, performance, configuration changes, or others. Events and incidents can be grouped by any criteria, including incident type, source, destination, username, etc.

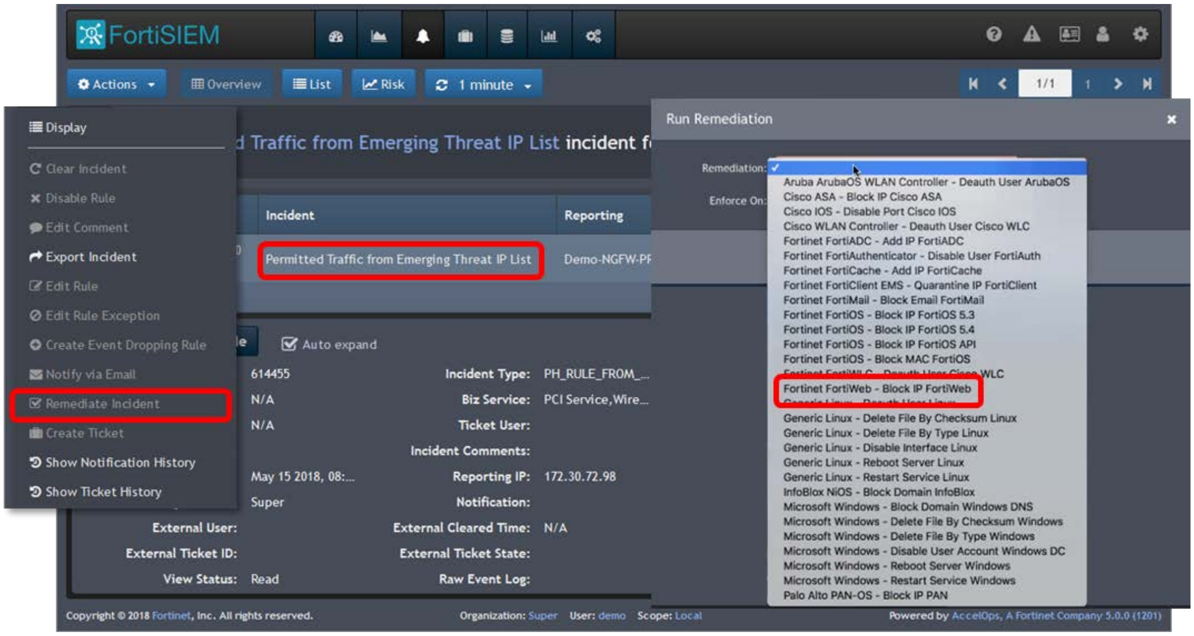
Figure 3. FortiSIEM Incident Dashboard



Source: Enterprise Strategy Group

We clicked on an incident, which took us to the incident details screen, shown in Figure 4. This incident was triggered by traffic from a known emerging threat site—which FortiSIEM identified via integration with public and premium threat feeds. From here, remediation (in this case, blocking the offending IP) was initiated with a click.

Figure 4. FortiSIEM Incident Remediation


FortiSIEM
Actions
Overview
List
Risk
1 minute
1/1
1
Display
Clear Incident
Disable Rule
Edit Comment
Export Incident
Edit Rule
Edit Rule Exception
Create Event Dropping Rule
Notify via Email
Remediate Incident
Create Ticket
Show Notification History
Show Ticket History
d Traffic from Emerging Threat IP List incident f
Incident
Reporting
Permitted Traffic from Emerging Threat IP List
Demo-NGFW-PF
Auto expand
Run Remediation
Remediation:
Enforce On:
Aruba ArubaOS WLAN Controller - Deauth User ArubaOS
Cisco ASA - Block IP Cisco ASA
Cisco IOS - Disable Port Cisco IOS
Cisco WLAN Controller - Deauth User Cisco WLC
Fortinet FortiADC - Add IP FortiADC
Fortinet FortiAuthenticator - Disable User FortiAuth
Fortinet FortiCache - Add IP FortiCache
Fortinet FortiClient EMS - Quarantine IP FortiClient
Fortinet FortiMail - Block Email FortiMail
Fortinet FortiOS - Block IP FortiOS 5.3
Fortinet FortiOS - Block IP FortiOS 5.4
Fortinet FortiOS - Block IP FortiOS API
Fortinet FortiOS - Block MAC FortiOS
Fortinet FortiWLC - Deauth User Cisco WLC
Fortinet FortiWeb - Block IP FortiWeb
Generic Linux - Deauth User Linux
Generic Linux - Delete File By Checksum Linux
Generic Linux - Delete File By Type Linux
Generic Linux - Disable Interface Linux
Generic Linux - Reboot Server Linux
Generic Linux - Restart Service Linux
InfoBlox NiOS - Block Domain InfoBlox
Microsoft Windows - Block Domain Windows DNS
Microsoft Windows - Delete File By Checksum Windows
Microsoft Windows - Delete File By Type Windows
Microsoft Windows - Disable User Account Windows DC
Microsoft Windows - Reboot Server Windows
Microsoft Windows - Restart Service Windows
Palo Alto PAN-OS - Block IP PAN

614455
N/A
N/A
May 15 2018, 08:...
Super
Incident Type: PH_RULE_FROM_...
Biz Service: PCI Service,Wire...
Ticket User:
Incident Comments:
Reporting IP: 172.30.72.98
Notification:
External User:
External Cleared Time: N/A
External Ticket ID:
External Ticket State:
View Status: Read
Raw Event Log:

Copyright © 2018 Fortinet, Inc. All rights reserved. Organization: Super User: demo Scope: Local Powered by AccelOps, A Fortinet Company 5.0.0 (1201)

Source: Enterprise Strategy Group

Why This Matters

Strengthening cybersecurity is a business initiative that 44% of respondents to ESG research—the largest percentage—believe will drive the most technology spending at their organizations over the next 12 months.[3] Organizations often attempt to leverage a SIEM solution to collect data from perimeter security and point solutions to consolidate security. Zero-day threats and compromises can evade detection with the traditional SIEM approach, which presents thousands of events per hour for manual analysis. A solution that can leverage data from security devices as well as performance, availability, change monitoring, and compliance data in a single ecosystem can provide organizations with the real-time, cross-correlated intelligence they need to secure and manage operations in the modern IT environment.

ESG confirmed that Fortinet's FortiSIEM delivers context, visibility, and rapid response by cross-correlating security, performance, and availability data from heterogeneous systems. This enables a security organization to discover, investigate, and respond to security, performance, and availability events rapidly, which provides the tools needed to address incidents completely with swift, focused, confident action. By shortening the time from detection to resolution, organizations can shave valuable time off their remediation processes, saving not just time, but effort, and money.

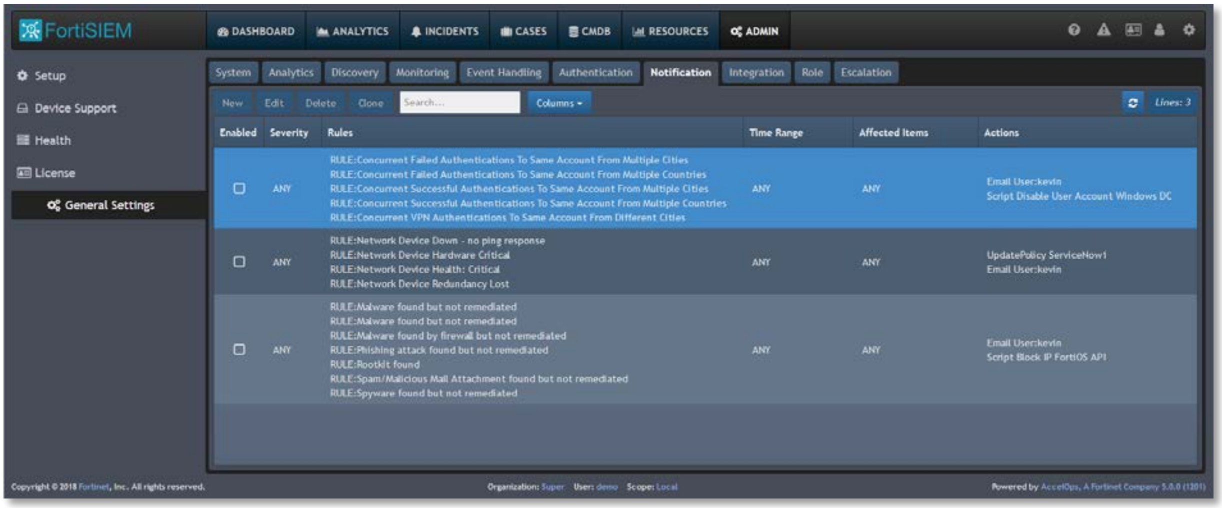
Automated Monitoring and Incident Response

FortiSIEM can automate both monitoring and response to threats to minimize impact and downtime while enabling IT and security teams to focus on more proactive activities. ESG Lab examined FortiSIEM notification policies, which provide the ability to automate detection and response to incidents across the environment.

ESG Testing

As seen in Figure 5, the notification policies can be configured to execute based on multiple criteria including severity, time range, affected elements, and rules defined in the CMDB. Thousands of rules and event types are predefined in the CMDB, and they are often consolidated to contain many events of the same category under a single rule. For example, the FailedLogin rule contains definitions for 528 different failed login types. Rules are readily extensible by the customer. For example, simply by adding a new event type in the CMDB, a new failed login type for a new device will automatically be included in the single rule FailedLogin.

Figure 5. FortiSIEM Automation with Notification Policies



Enabled	Severity	Rules	Time Range	Affected Items	Actions
□	ANY	RULE:Concurrent Failed Authentications To Same Account From Multiple Cities RULE:Concurrent Failed Authentications To Same Account From Multiple Countries RULE:Concurrent Successful Authentications To Same Account From Multiple Cities RULE:Concurrent Successful Authentications To Same Account From Multiple Countries RULE:Concurrent VPN Authentications To Same Account From Different Cities	ANY	ANY	Email User:kevin Script Disable User Account Windows DC
□	ANY	RULE:Network Device Down - no ping response RULE:Network Device Hardware Critical RULE:Network Device Health: Critical RULE:Network Device Redundancy Lost	ANY	ANY	UpdatePolicy ServiceNow1 Email User:kevin
□	ANY	RULE:Malware found but not remediated RULE:Malware found but not remediated RULE:Malware found by firewall but not remediated RULE:Phishing attack found but not remediated RULE:Rootkit found RULE:Spam/Malicious Mail Attachment found but not remediated RULE:Spyware found but not remediated	ANY	ANY	Email User:kevin Script Block IP FortiOS API

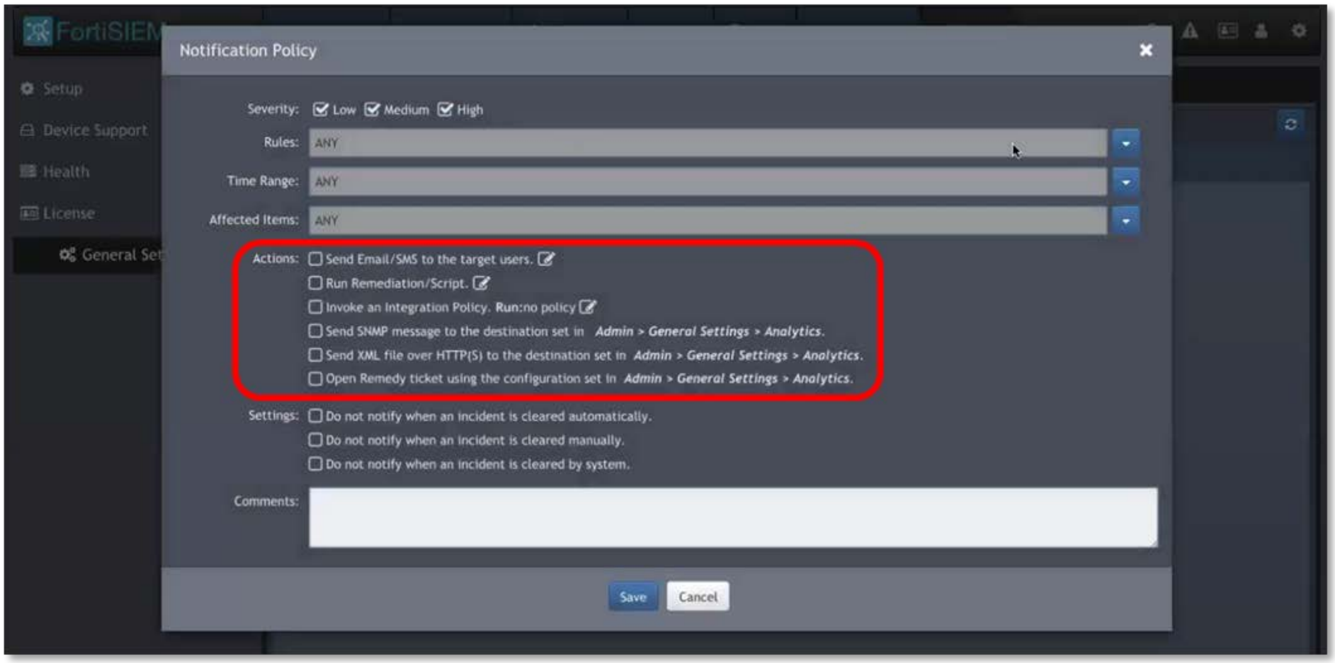
Copyright © 2018 Fortinet, Inc. All rights reserved. Organization: Super User: demo Scope: Local Powered by AccelOps, A Fortinet Company 5.0.0 (1201)

Source: Enterprise Strategy Group

[3] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

When configuring a notification policy, multiple, diverse actions can be combined and executed in concert, as shown in Figure 6. These actions include remediation scripts—users can leverage dozens of included scripts that can perform actions appropriate to the incident against systems and devices across the IT environment or import their own. Integration policies can automate ticket creation on integrated platforms such as ServiceNow, and Remedy tickets can be generated automatically.

Figure 6. Creating a Notification Policy



Notification Policy

Severity: ☑ Low ☑ Medium ☑ High

Rules: ANY

Time Range: ANY

Affected Items: ANY

Actions:
- □ Send Email/SMS to the target users.
- □ Run Remediation/Script.
- □ Invoke an Integration Policy. Run:no policy
- □ Send SNMP message to the destination set in *Admin > General Settings > Analytics*.
- □ Send XML file over HTTP(S) to the destination set in *Admin > General Settings > Analytics*.
- □ Open Remedy ticket using the configuration set in *Admin > General Settings > Analytics*.

Settings:
- □ Do not notify when an incident is cleared automatically.
- □ Do not notify when an incident is cleared manually.
- □ Do not notify when an incident is cleared by system.

Comments:

Source: Enterprise Strategy Group

Why This Matters

In 2018, 51% of organizations report that they have a problematic shortage of cybersecurity skills, up from 45% in 2017.[4] Organizations are seeking enhanced efficiency and efficacy, and are turning toward automated, or automatable tools to alleviate the burden of manual or repetitive tasks.

FortiSIEM collects data from heterogeneous host systems, network devices, and security platforms in an organization and adds real-time context, analytics, and alerts for a more complete understanding of the environment than can be afforded with a traditional SIEM system. FortiSIEM enables rapid, efficient analysis and identification of incidents using data from multiple domains quickly and automatically with a high degree of confidence. ESG Lab has confirmed that FortiSIEM was able to capture, index, and analyze real-world network traffic consisting of hundreds of millions of daily events from thousands of devices and systems, and provide concise, real-time, actionable intelligence.

FortiSIEM can automate both monitoring and response to threats and incidents to minimize impact and downtime while enabling IT and security teams to focus on more proactive activities.

[4] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

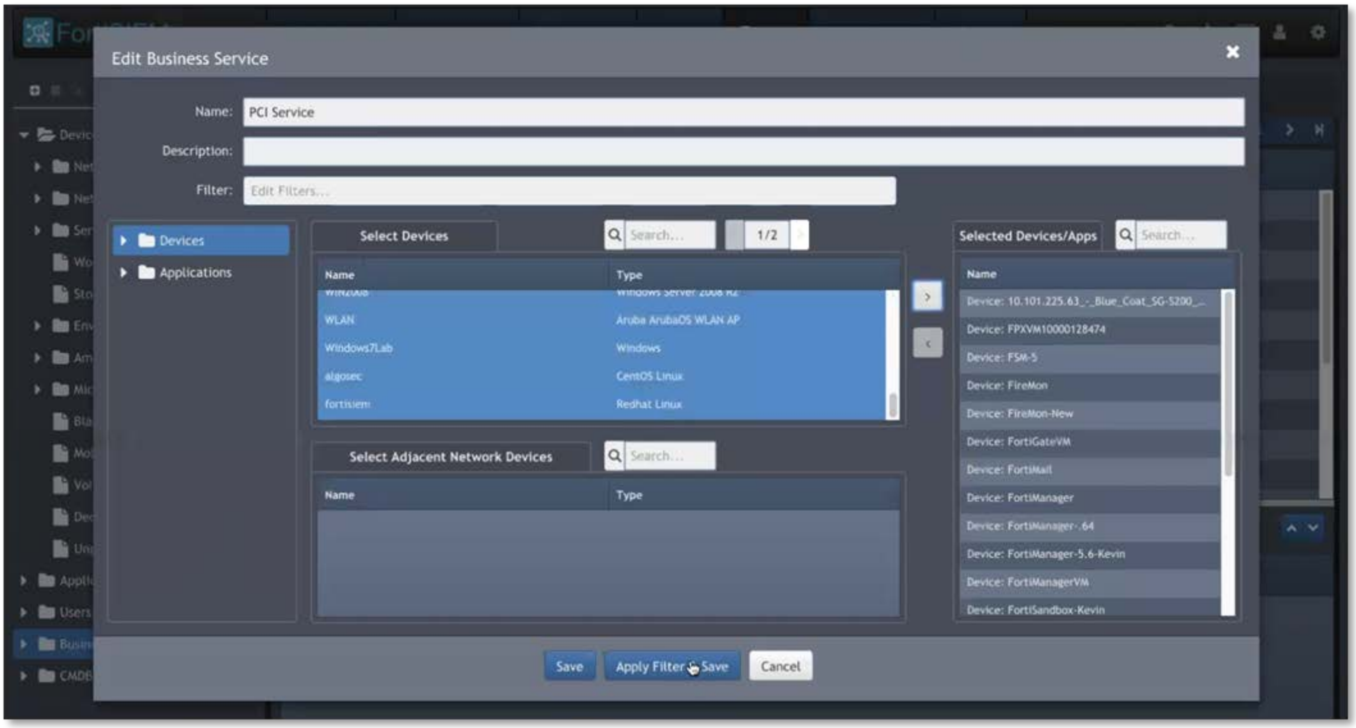
Monitoring and Managing Business Availability

The FortiSIEM platform is engineered to help organizations better monitor and manage the availability of their businesses. Unlike traditional SIEMs, FortiSIEM associates the individual elements that make up business services. Servers, network devices, databases, and applications are monitored as parts of a complete organism to provide deeper visibility into the status of the business. FortiSIEM provides dozens of preconfigured reports that apply advanced analytics to collected data and provide insight into performance, availability, and security of business services across every discipline of IT.

ESG Testing

ESG Lab defined a Business Service in FortiSIEM based on a Payment Card Industry (PCI) security standards-compliant payment processing environment. PCI security standards set the technical and operational requirements for organizations that accept or process payment transactions. PCI standards also cover software developers and manufacturers of applications and devices that are used in those transactions. In this scenario, we emulated a business that conducts e-commerce via an online webstore.

Figure 7. Defining a PCI-compliant Business Service



Edit Business Service

Name: PCI Service

Description:

Filter: Edit Filters...

Select Devices

Name	Type
WIN2008	Windows Server 2008 R2
WLAN	Aruba ArubaOS WLAN AP
Windows7Lab	Windows
algosec	CentOS Linux
fortisiem	Redhat Linux

Select Adjacent Network Devices

Name	Type

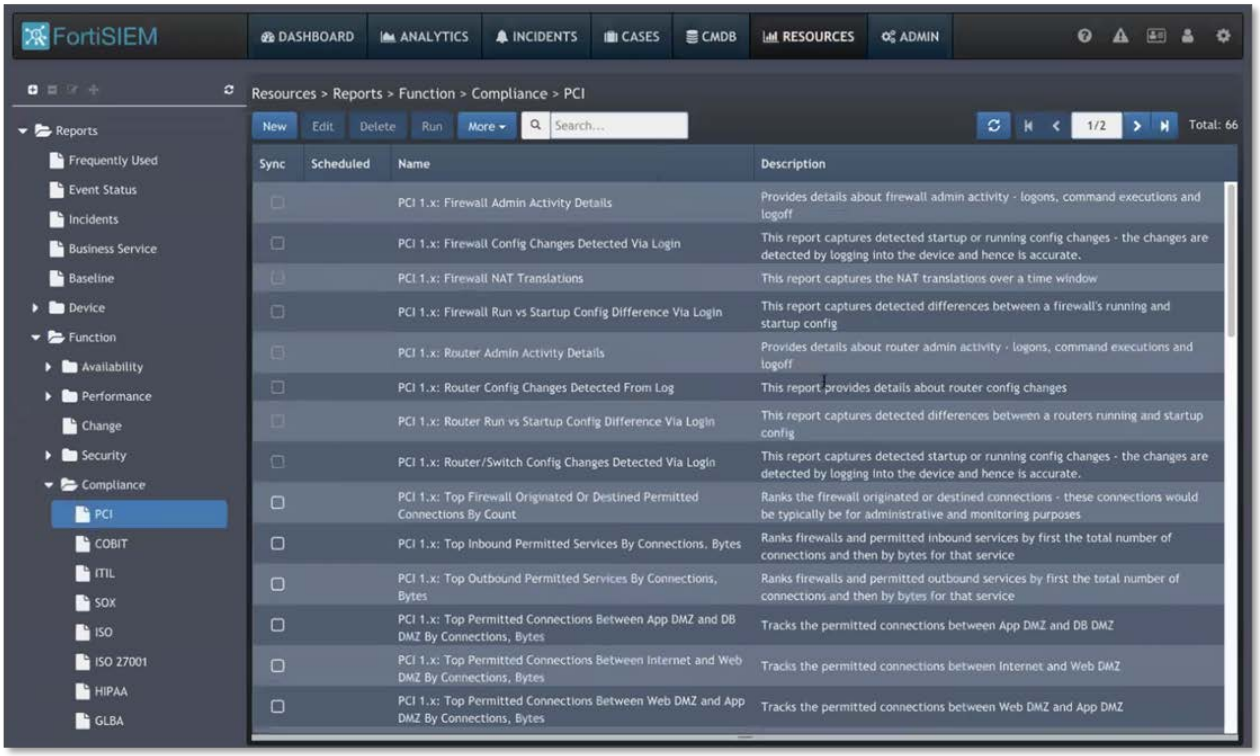
Selected Devices/Apps

Name
Device: 10.101.225.63_-_Blue_Coat_SG-5200_...
Device: FPXVM10000128474
Device: FSM-5
Device: FireMon
Device: FireMon-New
Device: FortiGateVM
Device: FortiMail
Device: FortiManager
Device: FortiManager-.64
Device: FortiManager-5.6-Kevin
Device: FortiManagerVM
Device: FortiSandbox-Kevin

Source: Enterprise Strategy Group

A typical PCI-compliant environment will include many different types of devices and applications, from back-end storage, databases, and analytics, to web applications, network and security devices, and services, including gateways, firewalls, and load balancers. All these devices and apps must adhere to the PCI standards. FortiSIEM made it easy to select all the devices and applications associated with the PCI environment and add them to the *PCI Service* business service in one click.

Figure 8. Business Service Reporting



Resources > Reports > Function > Compliance > PCI

Sync	Scheduled	Name	Description
☐		PCI 1.x: Firewall Admin Activity Details	Provides details about firewall admin activity - logons, command executions and logoff
☐		PCI 1.x: Firewall Config Changes Detected Via Login	This report captures detected startup or running config changes - the changes are detected by logging into the device and hence is accurate.
☐		PCI 1.x: Firewall NAT Translations	This report captures the NAT translations over a time window
☐		PCI 1.x: Firewall Run vs Startup Config Difference Via Login	This report captures detected differences between a firewall's running and startup config
☐		PCI 1.x: Router Admin Activity Details	Provides details about router admin activity - logons, command executions and logoff
☐		PCI 1.x: Router Config Changes Detected From Log	This report provides details about router config changes
☐		PCI 1.x: Router Run vs Startup Config Difference Via Login	This report captures detected differences between a routers running and startup config
☐		PCI 1.x: Router/Switch Config Changes Detected Via Login	This report captures detected startup or running config changes - the changes are detected by logging into the device and hence is accurate.
☐		PCI 1.x: Top Firewall Originated Or Destined Permitted Connections By Count	Ranks the firewall originated or destined connections - these connections would be typically be for administrative and monitoring purposes
☐		PCI 1.x: Top Inbound Permitted Services By Connections, Bytes	Ranks firewalls and permitted inbound services by first the total number of connections and then by bytes for that service
☐		PCI 1.x: Top Outbound Permitted Services By Connections, Bytes	Ranks firewalls and permitted outbound services by first the total number of connections and then by bytes for that service
☐		PCI 1.x: Top Permitted Connections Between App DMZ and DB DMZ By Connections, Bytes	Tracks the permitted connections between App DMZ and DB DMZ
☐		PCI 1.x: Top Permitted Connections Between Internet and Web DMZ By Connections, Bytes	Tracks the permitted connections between Internet and Web DMZ
☐		PCI 1.x: Top Permitted Connections Between Web DMZ and App DMZ By Connections, Bytes	Tracks the permitted connections between Web DMZ and App DMZ

Source: Enterprise Strategy Group

FortiSIEM provides the ability to run detailed reports on all business services. Figure 7 shows just a few of the built-in reports for PCI compliance. These reports would automatically run against all devices and applications in the *PCI Services* group.

Why This Matters

The complexity of IT infrastructure is increasing—more than two-thirds of surveyed organizations said that their IT environment has gotten more complex in the last two years.[5] Data growth and the rapid proliferation of virtualized applications are increasing the cost and complexity of securing and protecting business-critical applications and the hardware and software assets that power them.

A solution that can combine independent, heterogenous elements into logical groupings that reflect the customer-facing services that are at the core of an organization's business and enable organizations to monitor those services holistically, can significantly improve business availability while reducing time and effort.

ESG was able to create a business service that reflected a complex payment card application that required PCI compliance in just a few clicks, then monitor that application, and all the individual components that made it up, validating the availability of the service in the multiple contexts of security, performance, availability, and compliance.

[5] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

The Bigger Truth

Many factors are driving the focus on improving cybersecurity, from the previously cited cybersecurity skills shortage and increasing volume and velocity of threats to the increasing complexity of IT infrastructure—more than two-thirds of surveyed organizations said that their IT environment has gotten more complex in the last two years. Thus, organizations are seeking enhanced efficiency and efficacy, and, according to ESG research, 36% of organizations cited improved security/risk management as their most important IT investment justification, the most-often cited survey response.[6]

At the same time, the cost of downtime is enormous; depending on the industry, organizations lose hundreds of thousands to millions of dollars for every hour of downtime from lost productivity and revenue, missed opportunities, and loss of reputation and customers.

Fortinet designed FortiSIEM to be an effective and efficient IT, network, and cybersecurity operations management platform, providing both real-time and historical analytics with fast, automated responses to both simple and complex cross-domain incidents covering business services across the entire IT ecosystem. Cross-domain experience can be used by organizations to improve response and remediation times while reducing costs.

ESG Lab tested FortiSIEM and found that the user interface was easy to use, and FortiSIEM's rapid correlation of events enables quick and decisive identification of important events, leveraging insight across the entire IT spectrum for automated investigation and remediation. FortiSIEM takes this one step further with the concept of business services, collections of interdependent devices, services, and applications that together comprise a core business function. FortiSIEM provides the context IT teams need to be able to monitor a business service as a holistic entity, and address issues within individual components that may threaten business availability.

In the opinion of ESG Lab, FortiSIEM's unique capabilities in cybersecurity and IT operations management provide the real-time and historical analytics—with correlated context—needed for organizations to confidently detect and resolve anomalous activity and incidents and preserve business continuity.

[6] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.