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

ESG Lab Review

Fortinet FortiSIEM: Actionable Threat and Security Intelligence

Date: July 2016 **Author:** Tony Palmer, Senior Lab Analyst

Abstract

This ESG Lab Spotlight details ESG's hands-on testing of the Fortinet FortiSIEM threat and security intelligence product. ESG Lab focused on validating the ability of FortiSIEM to manage security, performance, and compliance from a single platform, performing collection and analytics with one engine. Testing was designed to explore how the solution can speed time to threat identification and remediation while providing insight into performance, availability, configuration changes, and compliance.

The Challenges

ESG asked 633 IT professionals and managers to name their most important IT priorities, and information security was cited by 37% of respondents, making it the most-often cited response by a wide margin.[1] Business intelligence and data analytics initiatives ranked second, cited by 24% of respondents. In addition, when asked to identify their most important justifications for IT investments, while 39% of organizations named improved security, 32% called out business process improvement and 27% indicated a reduction in operational expenditures, which suggests that while information security is certainly at the top of mind, operational improvement is not far behind.

The current security model often attempts to consolidate security by leveraging a SIEM solution to collect log, syslog, and netflow data from perimeter security and point solutions. However, experience tells us that zero-day threats and security compromises can evade detection when their network activity is "lost in the noise" of a traditional SIEM solution, which can present thousands of events to a security analyst per hour for manual analysis. What is needed is a holistic approach that can leverage data from security solutions in 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) in a single network/security ecosystem, providing organizations with the real-time, cross-correlated analytics and intelligence they need to secure and manage operations in the modern IT environment.

The Solution: FortiSIEM

ESG Lab validated how Fortinet FortiSIEM brings context to security, availability, and performance 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, along with change and compliance monitoring and reporting.

FortiSIEM is offered as a prebuilt 64-bit virtual appliance that runs in ESX, AWS, KVM, or Hyper-V environments. The FortiSIEM architecture is a scale-out, enterprise and service provider-ready multitenant framework. Each virtual appliance can monitor over 10,000 security events per second (EPS) and more than 1,000 devices for performance and availability. 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 etc.) connected to the network, and their respective interrelationships. The tool delivers the user with a comprehensive & holistic topology mapping that continues to self-learn and report on any changes beyond the initial baseline.

[1] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.

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 WMI (Windows Management Instrumentation), which includes features like 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. Here 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.

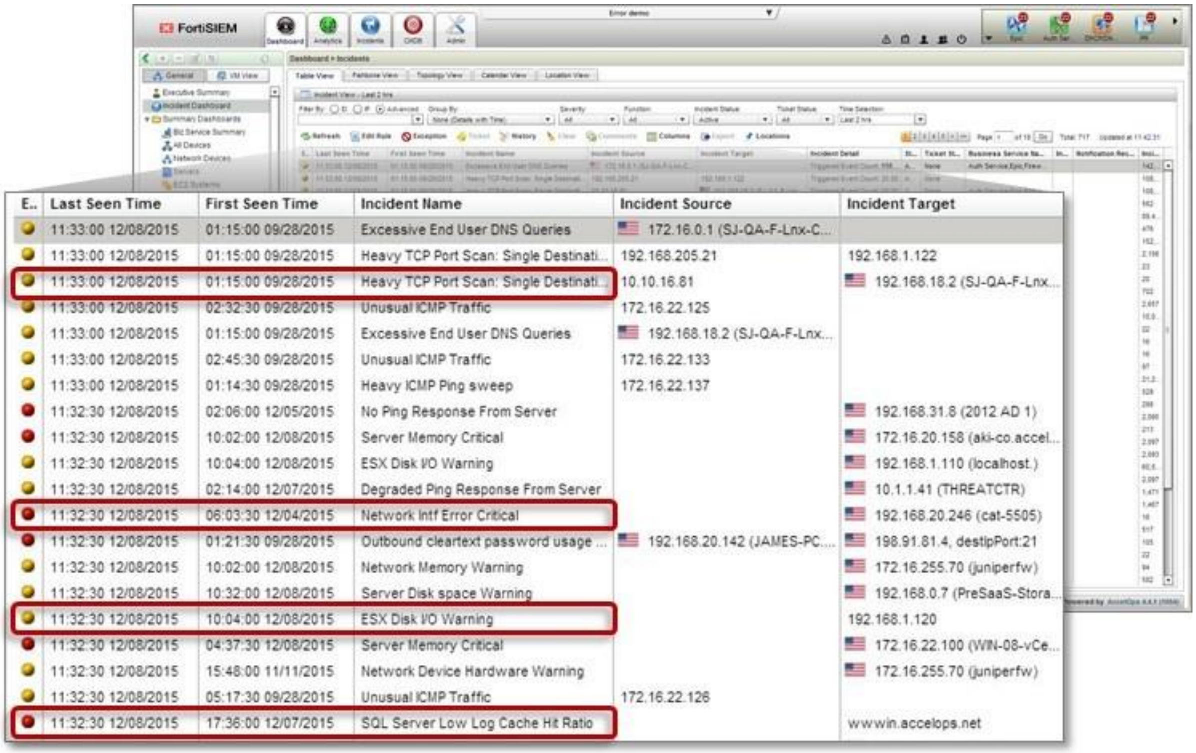
File Integrity Monitoring—The optional FortiSIEM Windows agent provides file integrity monitoring and simple deployment to the entire network.

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.

ESG Lab Tested

ESG Lab began with a look at the FortiSIEM Incident Dashboard. As seen in Figure 1, the Incident Dashboard displays security, performance, and availability data from diverse, heterogeneous servers, network devices, and applications in one console. In the example shown in Figure 1, we see data from Windows and Linux servers, network switches and firewalls, an ESX Cluster, and an application—SQL Server. Users can filter content based on any functional area that data is being collected from—security, performance, configuration changes, or others. Events and incidents can be grouped by any criteria, including incident type, source, destination, username, et al.

Figure 1. FortiSIEM Incident Dashboard



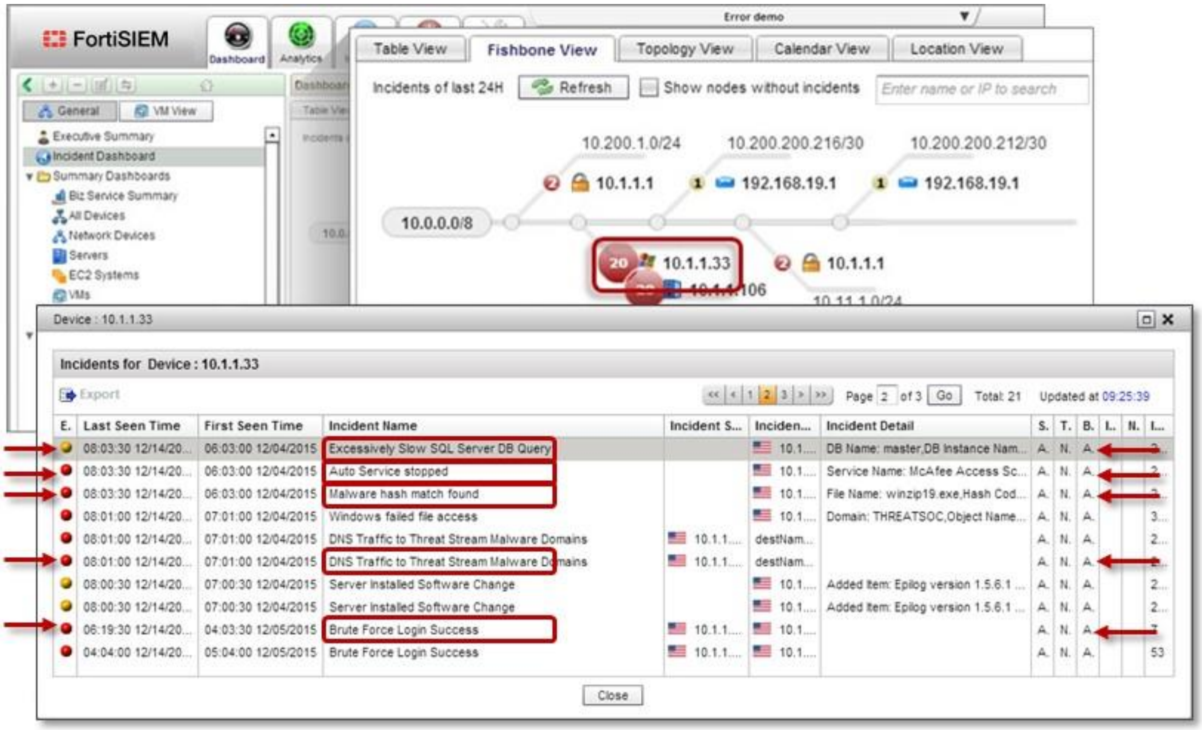
E..	Last Seen Time	First Seen Time	Incident Name	Incident Source	Incident Target
●	11:33:00 12/08/2015	01:15:00 09/28/2015	Excessive End User DNS Queries	172.16.0.1 (SJ-QA-F-Lnx-C...	
●	11:33:00 12/08/2015	01:15:00 09/28/2015	Heavy TCP Port Scan: Single Destinati...	192.168.205.21	192.168.1.122
●	11:33:00 12/08/2015	01:15:00 09/28/2015	Heavy TCP Port Scan: Single Destinati...	10.10.16.81	192.168.18.2 (SJ-QA-F-Lnx...
●	11:33:00 12/08/2015	02:32:30 09/28/2015	Unusual ICMP Traffic	172.16.22.125	
●	11:33:00 12/08/2015	01:15:00 09/28/2015	Excessive End User DNS Queries	192.168.18.2 (SJ-QA-F-Lnx...	
●	11:33:00 12/08/2015	02:45:30 09/28/2015	Unusual ICMP Traffic	172.16.22.133	
●	11:33:00 12/08/2015	01:14:30 09/28/2015	Heavy ICMP Ping sweep	172.16.22.137	
●	11:32:30 12/08/2015	02:06:00 12/05/2015	No Ping Response From Server		192.168.31.8 (2012 AD 1)
●	11:32:30 12/08/2015	10:02:00 12/08/2015	Server Memory Critical		172.16.20.158 (aki-co.accel...
●	11:32:30 12/08/2015	10:04:00 12/08/2015	ESX Disk I/O Warning		192.168.1.110 (localhost.)
●	11:32:30 12/08/2015	02:14:00 12/07/2015	Degraded Ping Response From Server		10.1.1.41 (THREATCTR)
●	11:32:30 12/08/2015	06:03:30 12/04/2015	Network Intf Error Critical		192.168.20.246 (cat-5505)
●	11:32:30 12/08/2015	01:21:30 09/28/2015	Outbound cleartext password usage ...	192.168.20.142 (JAMES-PC....	198.91.81.4, destIpPort:21
●	11:32:30 12/08/2015	10:02:00 12/08/2015	Network Memory Warning		172.16.255.70 (juniperfw)
●	11:32:30 12/08/2015	10:32:00 12/08/2015	Server Disk space Warning		192.168.0.7 (PreSaaS-Stora...
●	11:32:30 12/08/2015	10:04:00 12/08/2015	ESX Disk I/O Warning		192.168.1.120
●	11:32:30 12/08/2015	04:37:30 12/08/2015	Server Memory Critical		172.16.22.100 (WIN-08-vCe...
●	11:32:30 12/08/2015	15:48:00 11/11/2015	Network Device Hardware Warning		172.16.255.70 (juniperfw)
●	11:32:30 12/08/2015	05:17:30 09/28/2015	Unusual ICMP Traffic	172.16.22.126	
●	11:32:30 12/08/2015	17:36:00 12/07/2015	SQL Server Low Log Cache Hit Ratio		www.win.accelops.net

Speeding Threat Identification and Incident Response

ESG Lab examined the FortiSIEM fishbone view, which provides a visual representation of the devices and systems on the networks in the environment. Each device has a number indicating how many incidents are associated with the device, and clicking on the number brings up a list of the incidents associated with that one device.

As seen in Figure 2, the Windows server selected shows a number of incidents associated with it, which were collected from a variety of sources and reported based on 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 2. Incidents for a Specific Server



Device : 10.1.1.33

Incidents for Device : 10.1.1.33

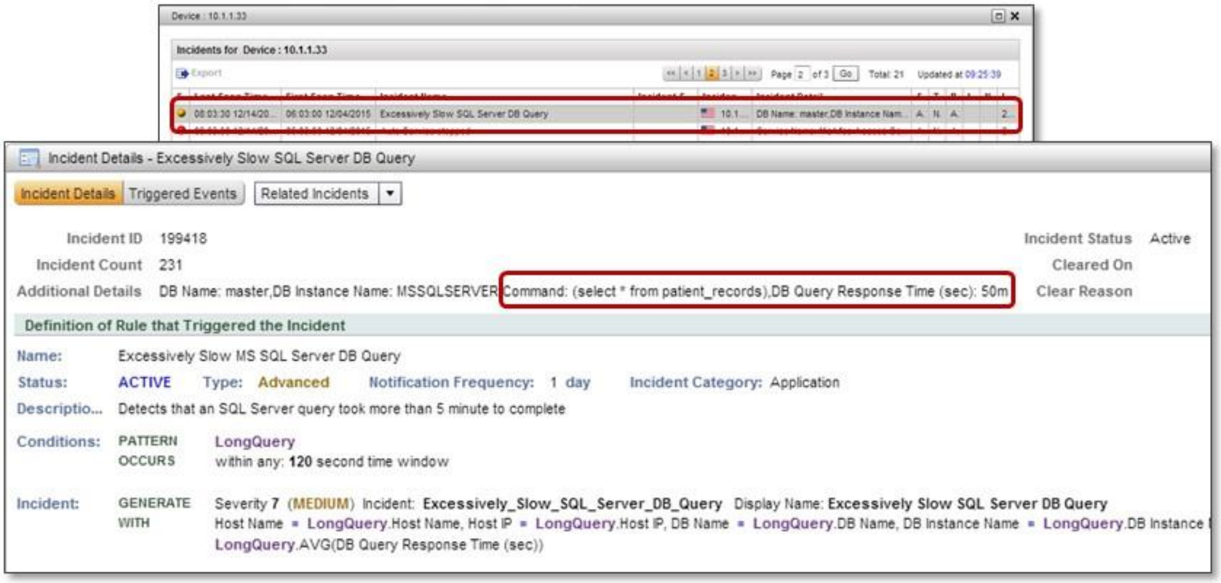
Export | << < 1 2 3 > >> Page 2 of 3 Go | Total: 21 | Updated at 09:25:39

E.	Last Seen Time	First Seen Time	Incident Name	Incident S...	Inciden...	Incident Detail	S.	T.	B.	I..	N.	I...
●	08:03:30 12/14/20...	06:03:00 12/04/2015	Excessively Slow SQL Server DB Query		10.1....	DB Name: master,DB Instance Nam...	A.	N.	A.			2...
●	08:03:30 12/14/20...	06:03:00 12/04/2015	Auto Service stopped		10.1....	Service Name: McAfee Access Sc...	A.	N.	A.			2...
●	08:03:30 12/14/20...	06:03:00 12/04/2015	Malware hash match found		10.1....	File Name: winzip19.exe,Hash Cod...	A.	N.	A.			2...
●	08:01:00 12/14/20...	07:01:00 12/04/2015	Windows failed file access		10.1....	Domain: THREATSOC,Object Name...	A.	N.	A.			3...
●	08:01:00 12/14/20...	07:01:00 12/04/2015	DNS Traffic to Threat Stream Malware Domains	10.1.1....	destNam...		A.	N.	A.			2...
●	08:01:00 12/14/20...	07:01:00 12/04/2015	DNS Traffic to Threat Stream Malware Domains	10.1.1....	destNam...		A.	N.	A.			2...
●	08:00:30 12/14/20...	07:00:30 12/04/2015	Server Installed Software Change		10.1....	Added Item: Epilog version 1.5.6.1 ...	A.	N.	A.			2...
●	08:00:30 12/14/20...	07:00:30 12/04/2015	Server Installed Software Change		10.1....	Added Item: Epilog version 1.5.6.1 ...	A.	N.	A.			2...
●	06:19:30 12/14/20...	04:03:30 12/05/2015	Brute Force Login Success	10.1.1....	10.1....		A.	N.	A.			7
●	04:04:00 12/14/20...	05:04:00 12/05/2015	Brute Force Login Success	10.1.1....	10.1....		A.	N.	A.			53

Close

While all of these events represent useful insight gained from analytics on the data streams ingested by FortiSIEM, one event in this view was of particular interest: The *Excessively Slow SQL Server DB Query*. ESG Lab highlighted the incident and selected *Show Incident Details* from the drop-down menu. As Figure 3 shows, the incident details reveal that the actual executed query was "select * from patient-records," which, when taken along with all the other suspicious activity on the host, would indicate data exfiltration is taking place. This example highlights that serious security threats can be identified through monitoring performance, availability, change, and configuration analytics, traditionally monitored in the NOC, and cross-correlating that data with SIEM analytics, that are traditionally monitored in the SOC.

Figure 3. SQL Performance Issue


Device : 10.1.1.33
Incidents for Device : 10.1.1.33
Export
Page 2 of 3 Go
Total: 21
Updated at 09:25:39
08:03:30 12/14/20... 06:03:00 12/04/2015 Excessively Slow SQL Server DB Query 10.1... DB Name: master,DB Instance Nam... A. N. A. 2...
Incident Details
Triggered Events
Related Incidents

Incident Details - Excessively Slow SQL Server DB Query

Incident ID 199418
Incident Count 231
Additional Details DB Name: master,DB Instance Name: MSSQLSERVER,Command: (select * from patient_records),DB Query Response Time (sec): 50m
Incident Status Active
Cleared On
Clear Reason

Definition of Rule that Triggered the Incident

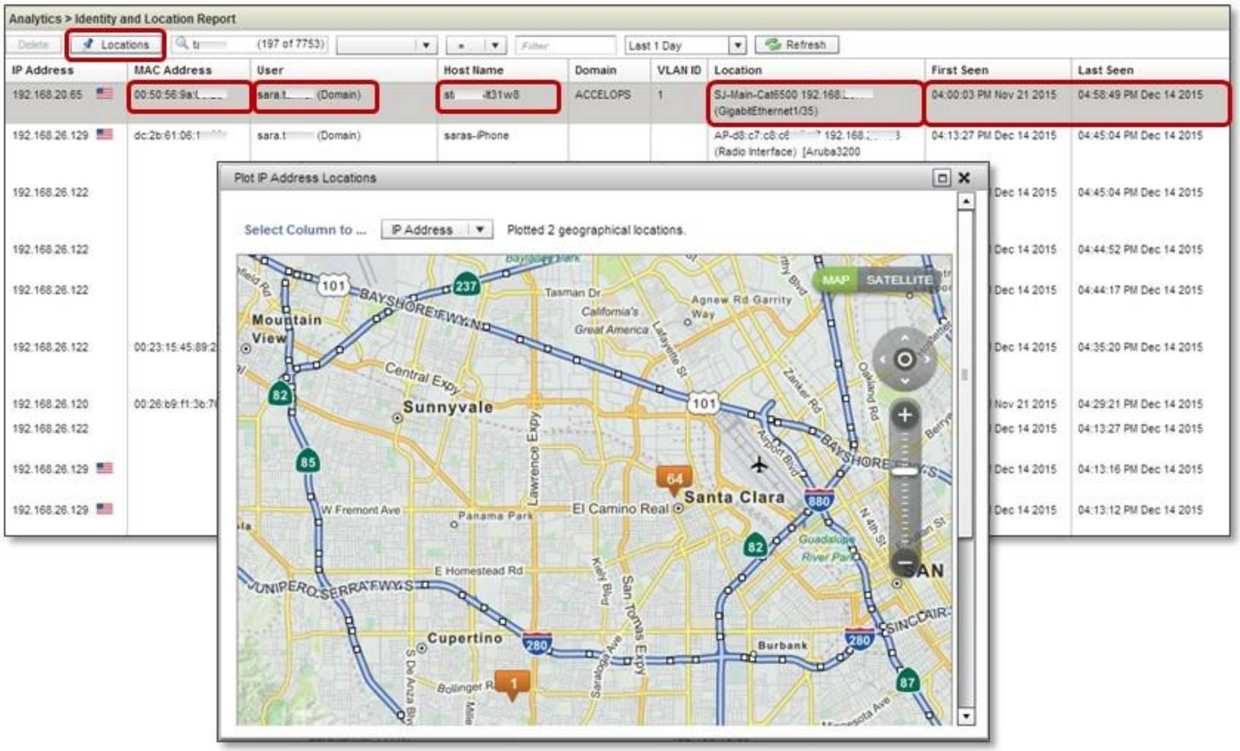
Name: Excessively Slow MS SQL Server DB Query
Status: ACTIVE Type: Advanced Notification Frequency: 1 day Incident Category: Application
Descriptio... Detects that an SQL Server query took more than 5 minute to complete
Conditions: PATTERN LongQuery
OCCURS within any: 120 second time window
Incident: GENERATE WITH Severity 7 (MEDIUM) Incident: Excessively_Slow_SQL_Server_DB_Query Display Name: Excessively Slow SQL Server DB Query
Host Name = LongQuery.Host Name, Host IP = LongQuery.Host IP, DB Name = LongQuery.DB Name, DB Instance Name = LongQuery.DB Instance
LongQuery.AVG(DB Query Response Time (sec))

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 security information and event management (SIEM) system. FortiSIEM enabled 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.

Providing Cross-correlated Context

ESG Lab also looked at how FortiSIEM IT operations analytics can provide cross-correlated context not only for threat detection, but also to identify baseline access, usage, and utilization patterns to enable organizations to more quickly identify anomalous activity. FortiSIEM provides dozens of preconfigured reports that apply advanced analytics to collected data and provide insight into performance, availability, and security across every discipline of IT. ESG Lab ran the identity and location report and selected a specific user by searching on her last name. As seen in Figure 4, each access of the network was listed with detail gleaned from multiple diverse sources. While the firewall and routers provided the IP address, the Active Directory servers provided the username and hostname of the machine used to log in as well as the time and duration of each log in. The location was provided by the device that the user connected to, even down to the switch blade and port. This provides a complete picture that can alert IT managers when a user's apparent behavior strays from normal patterns.

Figure 4. Analytics—Identity and Location Report



IP Address	MAC Address	User	Host Name	Domain	VLAN ID	Location	First Seen	Last Seen
192.168.20.65	00:50:56:9a:[redacted]	sara.t[redacted] (Domain)	st[redacted]-lt31w8	ACCELOPS	1	SJ-Main-Cat6500 192.168.[redacted] (GigabitEthernet1/35)	04:00:03 PM Nov 21 2015	04:58:49 PM Dec 14 2015
192.168.26.129	dc:2b:61:06:1[redacted]	sara.t[redacted] (Domain)	saras-iPhone			AP-d8:c7:c8:c6[redacted]7 192.168.2[redacted]3 (Radio Interface) [Aruba3200	04:13:27 PM Dec 14 2015	04:45:04 PM Dec 14 2015
192.168.26.122							Dec 14 2015	04:45:04 PM Dec 14 2015
192.168.26.122							Dec 14 2015	04:44:52 PM Dec 14 2015
192.168.26.122							Dec 14 2015	04:44:17 PM Dec 14 2015
192.168.26.122	00:23:15:45:89:2						Dec 14 2015	04:35:20 PM Dec 14 2015
192.168.26.120	00:26:b9:f1:3b:7						Nov 21 2015	04:29:21 PM Dec 14 2015
192.168.26.122							Dec 14 2015	04:13:27 PM Dec 14 2015
192.168.26.129							Dec 14 2015	04:13:16 PM Dec 14 2015
192.168.26.129							Dec 14 2015	04:13:12 PM Dec 14 2015

Select Column to ... IP Address ▾ Plotted 2 geographical locations.

FortiSIEM demonstrated the capability to deliver cross-correlated, context-aware visibility and situational awareness, along with the ability to drill down to specific events in any domain. This enables an organization to discover, investigate, and manage responses to events from a single console, which provides the tools needed to address security, performance, and availability incidents completely, taking swift, focused action. By shortening the time from detection to analysis and response, organizations can gain the opportunity and ability to address issues and stop threats before they become critical issues.

Why This Matters

Information security, along with business intelligence and data analytics initiatives were the top two most-cited IT priorities in a recent ESG survey.[2] The current security model often attempts to leverage a SIEM solution to collect log, syslog, and netflow data from perimeter security and point solutions to consolidate security. Zero-day threats and security compromises can evade detection with the traditional SIEM approach, which can present thousands of events to a security analyst per hour for manual analysis.

A solution that can leverage data from security solutions in 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) in a single network/security ecosystem can provide organizations with the real-time, cross-correlated analytics and intelligence they need to secure and manage operations in the modern IT environment.

ESG confirmed the ability of Fortinet's FortiSIEM to deliver context-aware visibility and situational awareness by cross-correlating data from security, performance, and availability data from diverse, heterogeneous servers, network devices, and applications. This enables a security organization to discover, investigate, and manage responses to not only security, but performance and availability events from a single interface, which provides the tools needed to address incidents completely, taking swift, focused, confident action. By shortening the time from detection to resolution, organizations can shave valuable time off of their remediation processes, saving time, effort, and money.

The Bigger Truth

Organizations have been leveraging virtualization to provide flexible IT services to users, whether from traditional data centers or the cloud—private or public. Information security was the most-often cited most important IT priority in an ESG survey, with regulatory compliance not far behind.[3] In addition to improved security, business process improvement and reducing operational expenditures were called out as important justifications for IT investments in the same survey.

The consequences of security breaches can be devastating to operations, company reputations, and finances and the costs may include not just resuming operations and addressing security gaps, but legal liability and regulatory fines that can be an onerous burden.

FortiSIEM was designed to capture and analyze massive amounts of cross-domain contextual data in real time. Effective operations management and incident response in protecting an organization's security and performance requires delivering fast response to both simple and complex queries, across the entire IT ecosystem. The ability to provide both real-time and historical analytics is key to optimizing both immediate incident investigation and forensics. ESG Lab tested the FortiSIEM management console and found it easy to use to gain insight into the overall health of the IT ecosystem as well as the health and security of users and devices across the entire network. ESG Lab also explored real-time cross-correlation and analytics to isolate specific incidents with specific criteria and actionable context.

In the opinion of ESG Lab, FortiSIEM's unique capabilities in IT operations analytics provides the real-time and historical analytics—with correlated context—needed for organizations to confidently detect and resolve anomalous activity and incidents. 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 investigation and remediation. The ability to ingest custom data from any source without requiring agents enables organizations to gain useful visibility into any threat to their environment.

[2] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.

Organizations are experiencing increasing security challenges in protecting their business information assets. For the many businesses that must adhere to compliance regulations, cloud-based services and application mobility provide even greater security and availability challenges. A multi-layered security approach with visibility into all aspects of operations is a necessity.

What's needed is a solution that increases IT productivity and efficiency. FortiSIEM is designed to solve this problem in a unique way by providing an integrated monitoring application that automatically discovers servers, devices, and applications in the environment; baselines activities and traffic patterns; and uses prebuilt rules to provide proactive alerts on security, performance, and availability events in real time, with options to customize based on unique needs. FortiSIEM helps organizations quickly identify and rectify problems by appending events with contextual intelligence such as user identity, device type, and geo-location information.

ESG Lab validated that Fortinet's FortiSIEM provides a next-generation SIEM with the critical functions of continuous monitoring, cross-domain analytics, and rapid incident identification and response, combined with performance and availability monitoring management and intuitive ease of use. ESG Lab believes organizations that can cross-correlate performance, availability, change configuration, security, and compliance will have an unfair advantage against today's increasingly dangerous threats.

[3] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

The goal of ESG Lab reports is to educate IT professionals about data center technology products for companies of all types and sizes. ESG Lab 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 objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab'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.