

splunk> .conf2017

Accelerating Risk Management Through Adaptive Response Strategies

Accelerate decisions at machine-to-machine speed

Michael Woolfe | Director, Strategic Programs

September 26, 2017 | Washington, DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

Fortinet Legal Disclaimer

- ▶ This presentation is for informational purposes only and is not intended to create any contractual obligation whatsoever. Nothing in this presentation constitutes a warranty, guarantee, binding specification or other binding commitment by Fortinet, and performance and other specification information herein may be unique to certain environments. This presentation may include forward-looking statements that involve uncertainties and assumptions, such as statements regarding program, technology and functionality releases and release times. All statements other than statements of historical fact are statements that could be deemed forward-looking statements. Fortinet assumes no obligation to update any forward-looking statements, and expressly disclaims any obligation to update these forward-looking statements. Fortinet disclaims in full any guarantees and reserves its right to make technical changes and disclaims responsibility for typing or printing errors.
- ▶ Copyright © 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare®, and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners.

“Sometimes the questions are complicated and the answers are simple.”

-Dr. Seuss

Example: FortiGate Client Reputation

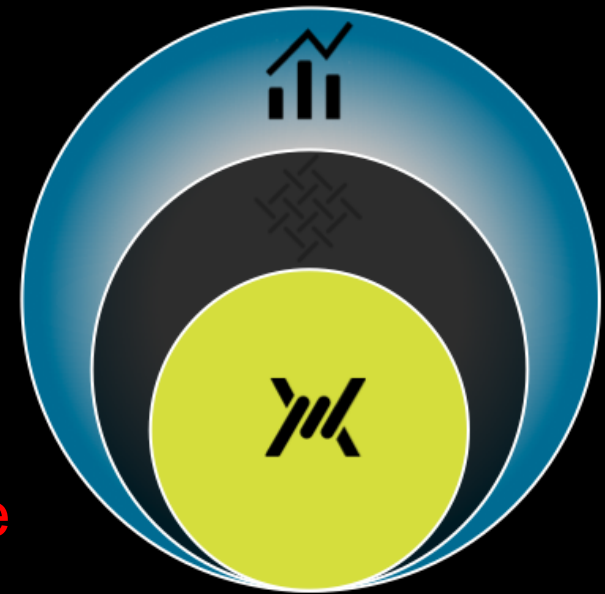
How you already rely upon a fabric

Authentication

- ▶ Credential management
- ▶ Centralized revocation
- ▶ Access auditing & tracking
- ▶ Local Passwords
- ▶ Local access records
- ▶ Individual host revocation

Network Traffic Routing

- ▶ Dynamic routing
- ▶ Domain Name Servers
- ▶ Centralized File Shares
- ▶ Static Routes
- ▶ IP addresses for each website
- ▶ Isolated storage



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/product.screen?product_id=AV-CB-01" "Opera/9.80
/buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.0) Gecko/20100101 Firefox/3.6"
/buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01" "Opera/9.80
http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01" "Opera/9.80
http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01" "Opera/9.80
http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01" "Opera/9.80

```

Example: Operational Technology

FortiGate and Nozomi integration

The screenshot displays the Nozomi Networks interface for Fortinet FortiGate integration. The main window shows a connection to Fortinet FortiGate 10.101.80.81. Below this, there are fields for Host, User (admin), and Password, with a Save button. A sidebar on the right lists various system components like Network, System, Policy & Objects, Security Profiles, VPN, User & Device, and WiFi & Switch Controller. The main area shows a table of traffic logs for FortiGate VM64 FGT-Nozomi, with columns for #, Date/Time, Source, Destination, Application Name, Security Events, Result, and Policy. The logs show traffic from DESKTOP-472VGKM to 192.168.253.128 via MODBUS. A detailed view of a log entry is shown on the right, including Log Details, General information (Date, Time, Duration, Session ID, Virtual Domain), Source information (IP, Source Port, Country, Primary MAC, Source Interface, Host Name, Device Type, OS Name), Destination information (IP, Port, Country, Destination Interface), Application information (Application Name, Category, Protocol, Service), Data statistics (Received Bytes, Received Packets, Sent Bytes, Sent Packets), and Action information (Action, Threat, Policy, Policy UUID, Policy Type). A Security section shows Level, Threat Level, and Threat Score. At the bottom, there is a navigation bar with a search icon and a status bar showing page 1 of 12.

Fortinet FortiGate Integration

Connected to Fortinet FortiGate 10.101.80.81

Host: 10.101.80.81

User: admin

Save

FortiGate VM64 FGT-Nozomi

#	Date/Time	Source	Destination	Application Name	Security Events	Result	Policy
1	13:58:47	DESKTOP-472VGKM	192.168.253.128	MODBUS		9.38 kB / 5.44 kB	1 (Accepted Protocols)
2	13:54:54	DESKTOP-472VGKM	192.168.253.128	MODBUS		224 B / 184 B	1 (Accepted Protocols)
3	13:54:41	DESKTOP-472VGKM	192.168.253.128	MODBUS		11.01 kB / 6.48 kB	1 (Accepted Protocols)
4	13:52:54	DESKTOP-472VGKM	192.168.253.128	MODBUS		224 B / 184 B	1 (Accepted Protocols)
5	13:51:57	DESKTOP-472VGKM	192.168.253.128	MODBUS		11.44 kB / 6.79 kB	1 (Accepted Protocols)
6	13:46:52	DESKTOP-472VGKM	192.168.253.128	MODBUS		224 B / 184 B	1 (Accepted Protocols)
7	13:46:36	DESKTOP-472VGKM	192.168.253.128	MODBUS		11.88 kB / 7.11 kB	1 (Accepted Protocols)
8	13:44:33	DESKTOP-472VGKM	192.168.253.128	MODBUS		224 B / 184 B	1 (Accepted Protocols)
9	13:43:33	DESKTOP-472VGKM	192.168.253.128	MODBUS		12.02 kB / 7.21 kB	1 (Accepted Protocols)
10	13:39:35	DESKTOP-472VGKM	192.168.253.128	MODBUS		224 B / 184 B	1 (Accepted Protocols)
11	13:34:56	DESKTOP-472VGKM	192.168.253.128	MODBUS		10.72 kB / 6.27 kB	1 (Accepted Protocols)
12	13:32:32	DESKTOP-472VGKM	192.168.253.128	MODBUS		673.24 kB / 417.14 kB	1 (Accepted Protocols)

Log Details

General

Date: 05/26/2017
Time: 13:58:47
Duration: 12s
Session ID: 2726081
Virtual Domain: root

Source

IP: 192.168.254.11
Source Port: 62173
Country: Reserved
Primary MAC: 00:50:56:b9:74:47
Source Interface: port2
Host Name: DESKTOP-472VGKM
Device Type: Windows PC
OS Name: Windows 10 / 2016

Destination

IP: 192.168.253.128
Port: 502
Country: Reserved
Destination Interface: port3

Application

Application Name: MODBUS
Category: unscanned
Protocol: tcp
Service: Modbus

Data

Received Bytes: 5 kB
Received Packets: 103
Sent Bytes: 9 kB
Sent Packets: 204

Action

Action: Accept: session timeout
Threat: 262144
Policy: 1
Policy UUID: 32dfb20c-18b5-51e7-7f54-50387c77ff6
Policy Type: policy

Security

Level: ■■■■■■■■■■
Threat Level: low
Threat Score: 5

Alerts

Page 1 of 1, 5 entries

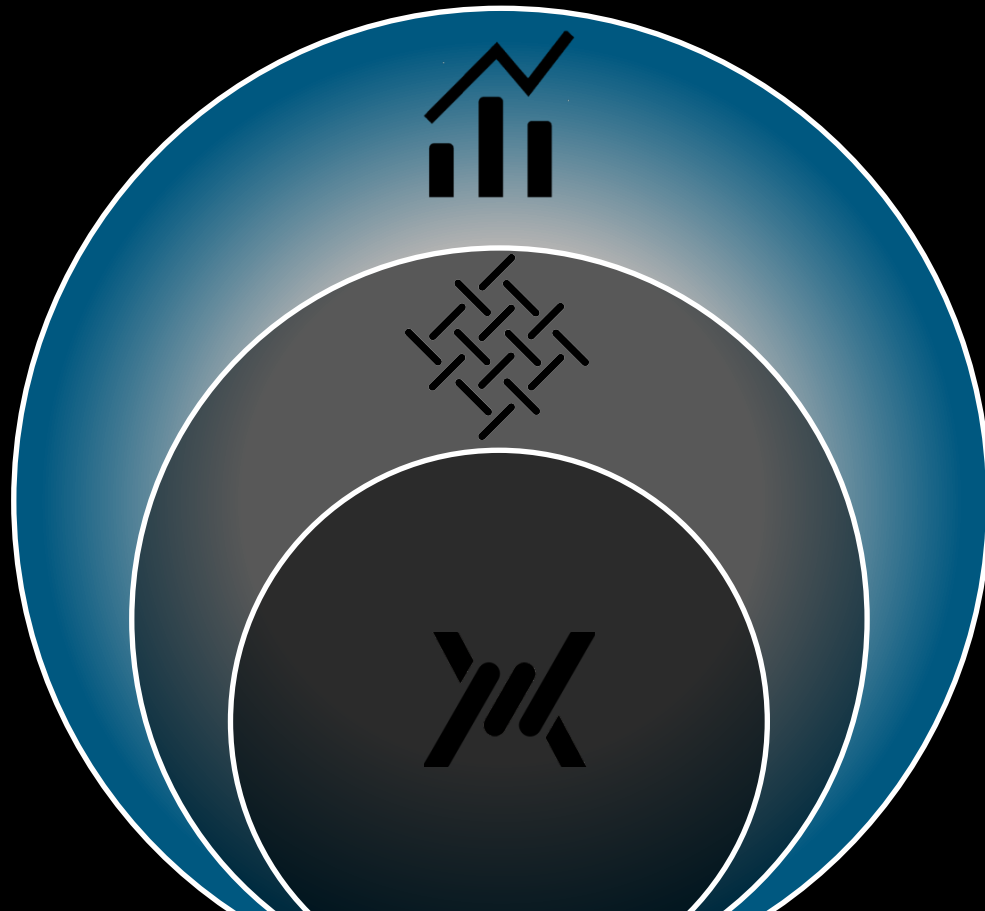
Actions	Time	ID	Type ID	Status	Name
<input checked="" type="checkbox"/>	13:58:59.189	17d178de	INCIDENT:ANOMALOUS-PACKETS	open	Anomalous packets
<input checked="" type="checkbox"/>	13:58:46.433	0b264656	VI:NEW-FUNC-CODE	open	New SCADA function code det
<input checked="" type="checkbox"/>	13:58:46.433	03af3b66	VI:PROC-NEW-VALUE	open	New SCADA variable value
<input checked="" type="checkbox"/>	13:58:46.433	a1033abe	VI:PROC-NEW-VAR	open	New SCADA variable appear
<input checked="" type="checkbox"/>	13:57:44.440	1c5e1642	VI:NEW-NODE	open	New node appeared

Ask me anything

[Total: 12]

HITL: Human in the Loop

Operations Management & Analytics



- ▶ Red Button
- ▶ What we cannot push to the team or wire
- ▶ Integrating larger context & authorization
- ▶ Training the model

Example: Splunk Adaptive Response

“I like the concept of a security fabric because it **simplifies security**, and it enables network and security professionals to **respond** to cyber attacks **faster**, **minimizing** the impact of a **breach**.”

Simplification for faster, better response

Undeniable fabric value

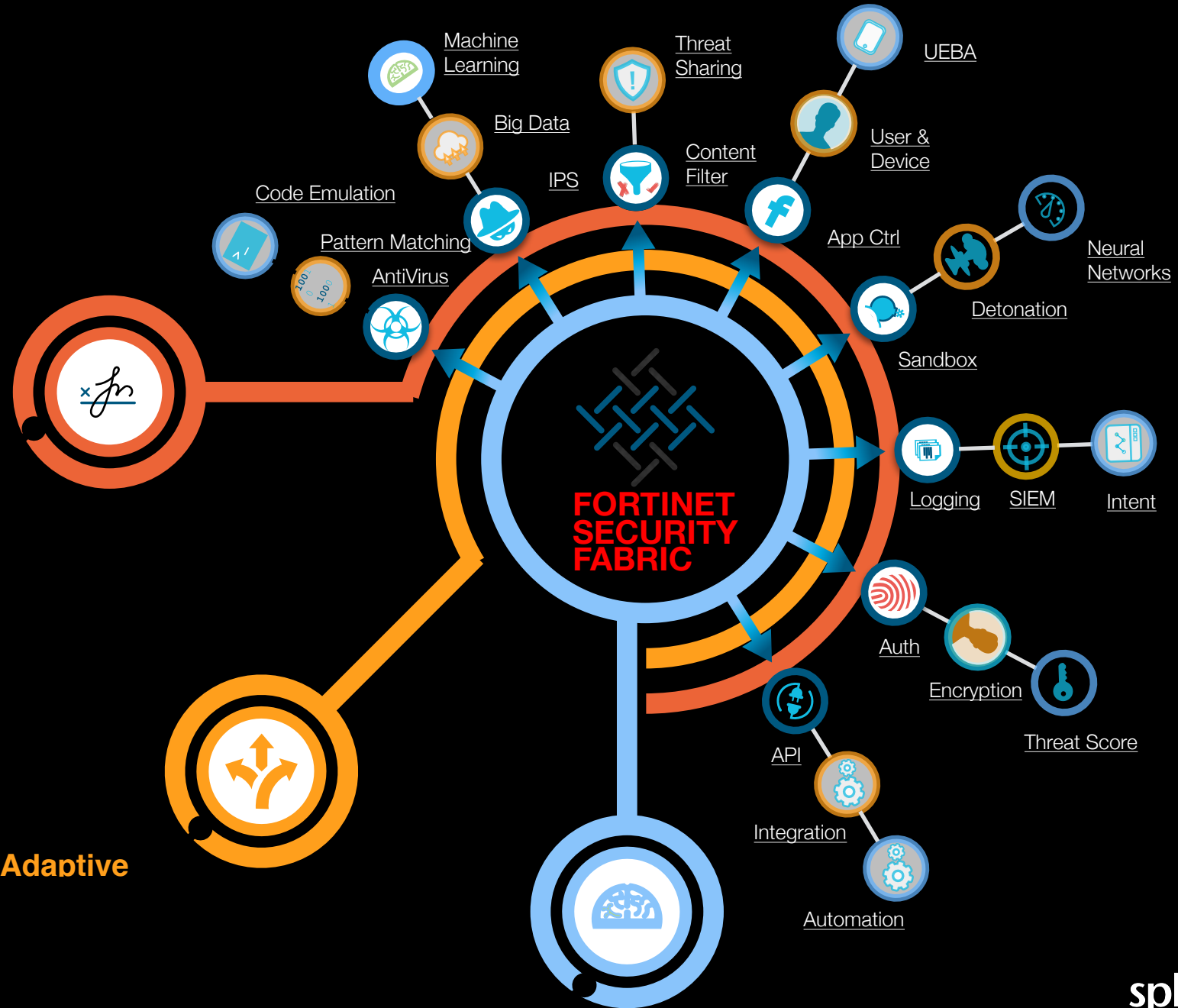
Today, start expecting your technology to work together, for you

- ▶ Intent based security
- ▶ Expedite containment response
- ▶ Continuous audit & enforcement
- ▶ Simplify operations, staffing

Signature
Proactive
Advanced
Defense
(PADing)

Adaptive

Behavior



Don't forget to **rate this session** in the
.conf2017 mobile app

splunk> .conf2017