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> .conf2017

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.
-

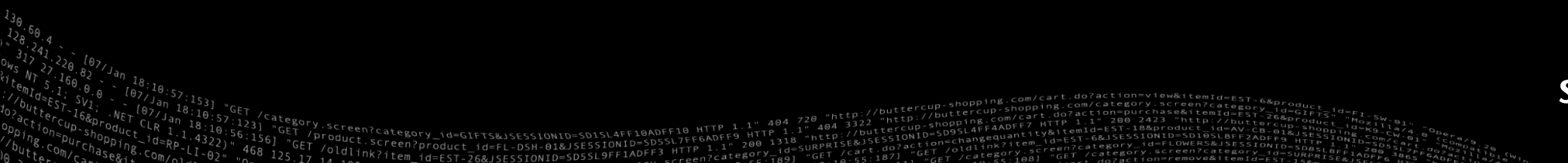
splunk> .conf2017

Before you get a phone call ..

Core concepts in 5 minutes

- **Teaming of core technologies required**
  - 'Basics' must be absolute and automatic
  - Complexity is the enemy of secure operations
  - Only hope for risk management as the speed of everything increases

- **Risk management largely measured on response ability**
  - Defense in depth is a methodology, not a device count
  - Push controls to lowest level possible

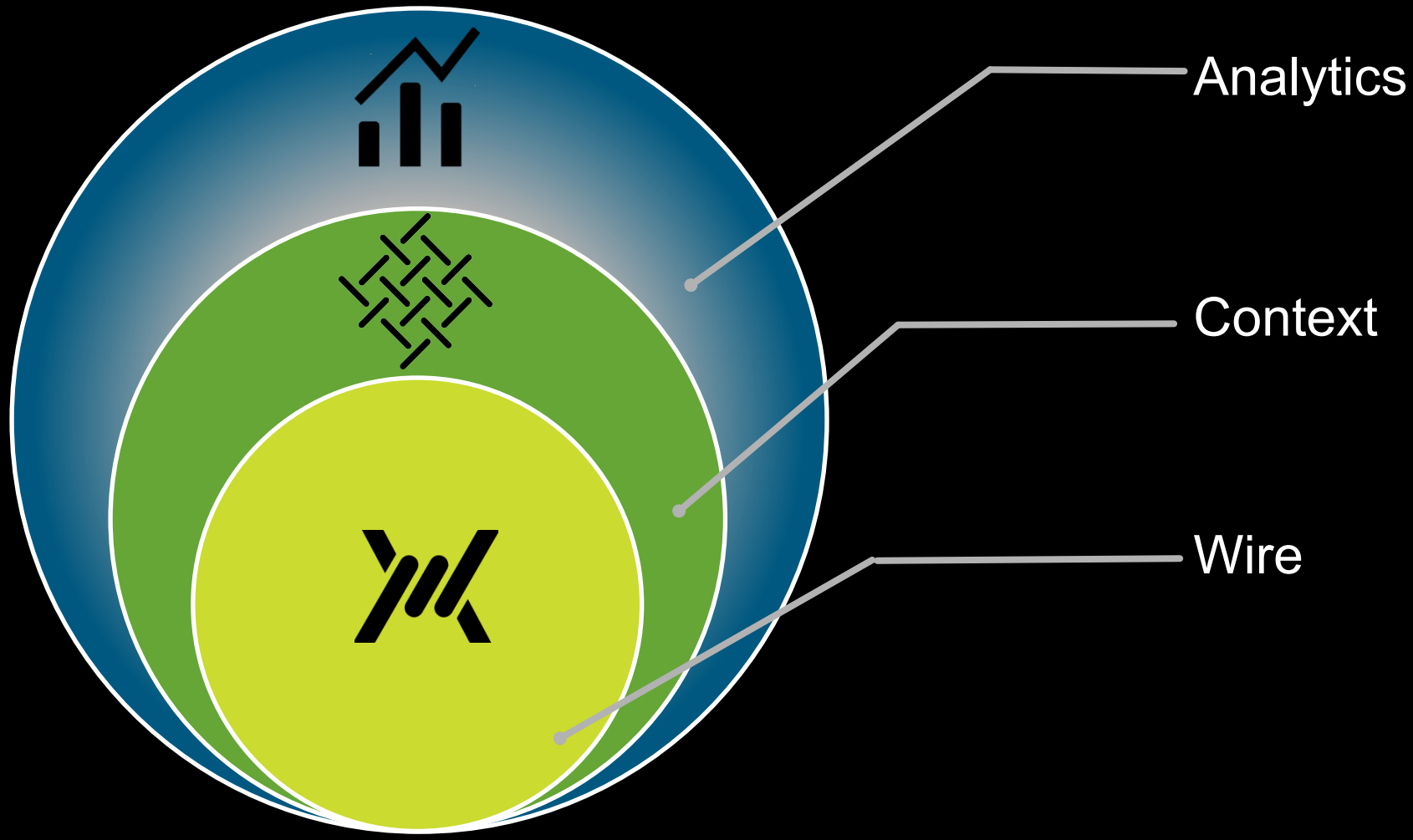


“Sometimes the questions are complicated and the answers are simple.”

-Dr. Seuss

Running circles around your framework

Systems and Controls Strategy



Example: FortiGate Client Reputation

Proving theorem: local meshing required

Today, we cannot even keep up

And it is going to worse

- Encryption

- Dynamic Workloads

- Devices

How you already rely upon a fabric

Authentication

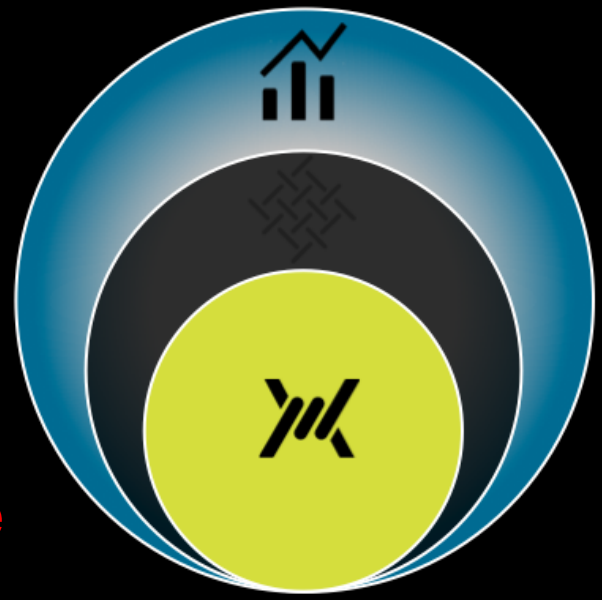
- Credential management
- Centralized revocation
- Access auditing & tracking

Network Traffic Routing

- Dynamic routing
- Domain Name Servers
- Centralized File Shares

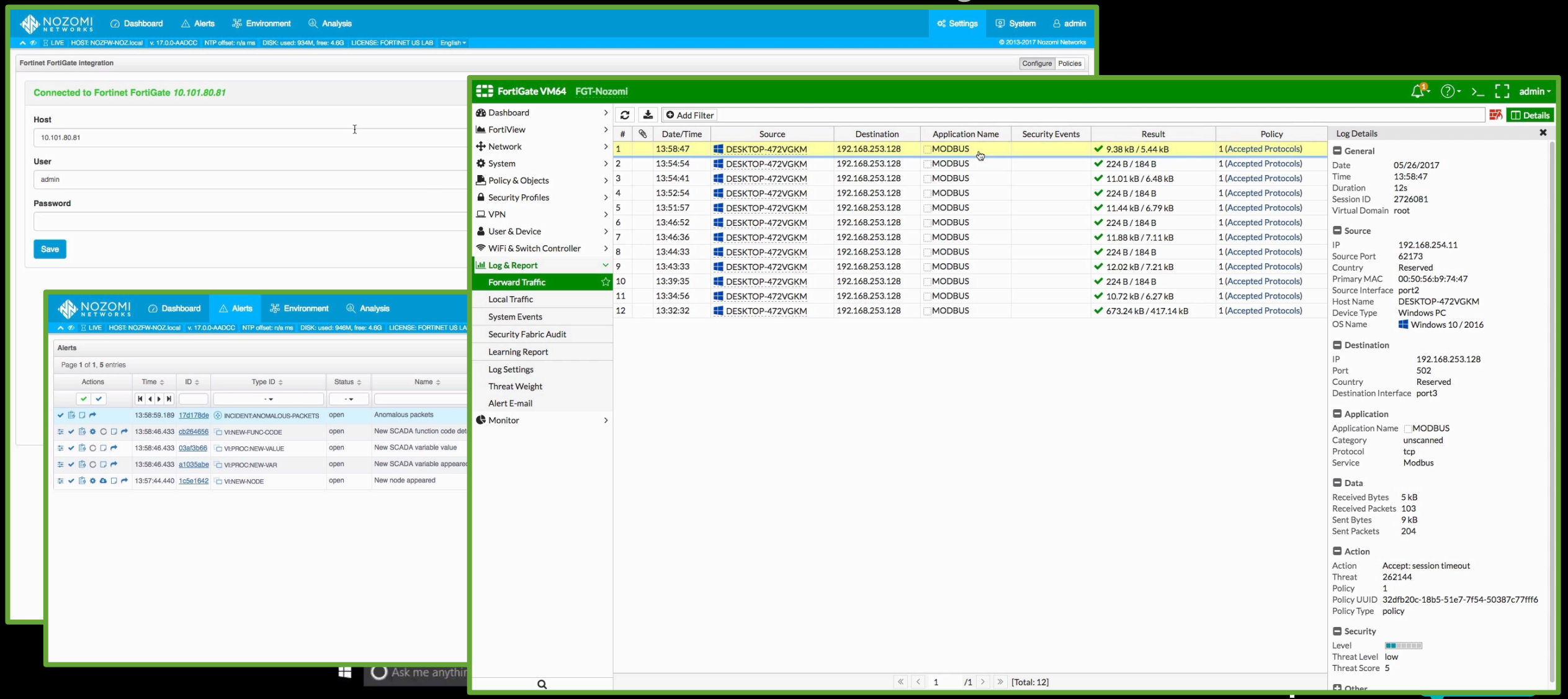
- Local Passwords
- Local access records
- Individual host revocation

- Static Routes
- IP addresses for each website
- Isolated storage



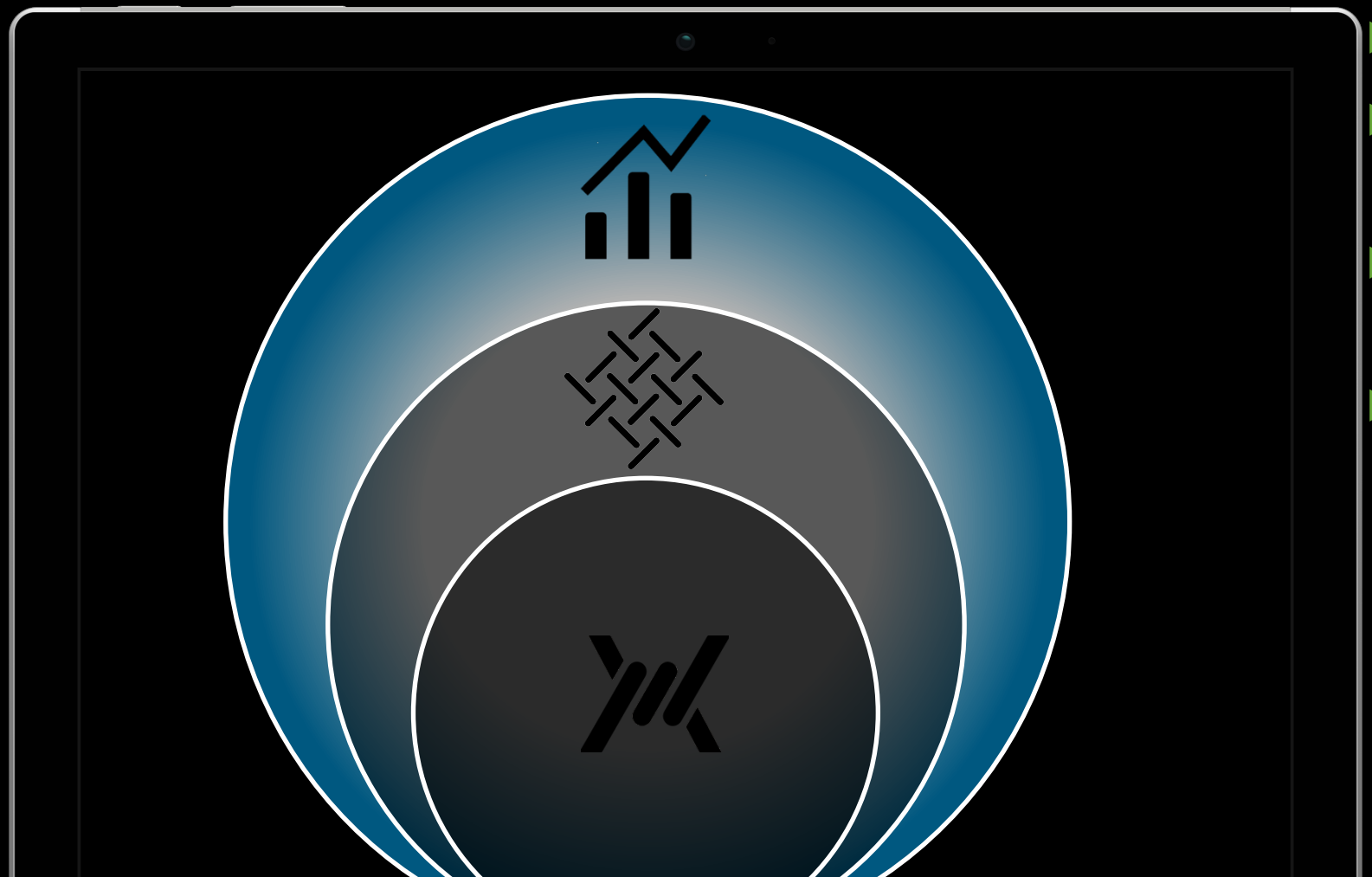
Example: Operational Technology

FortiGate and Nozomi integration



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 Respone

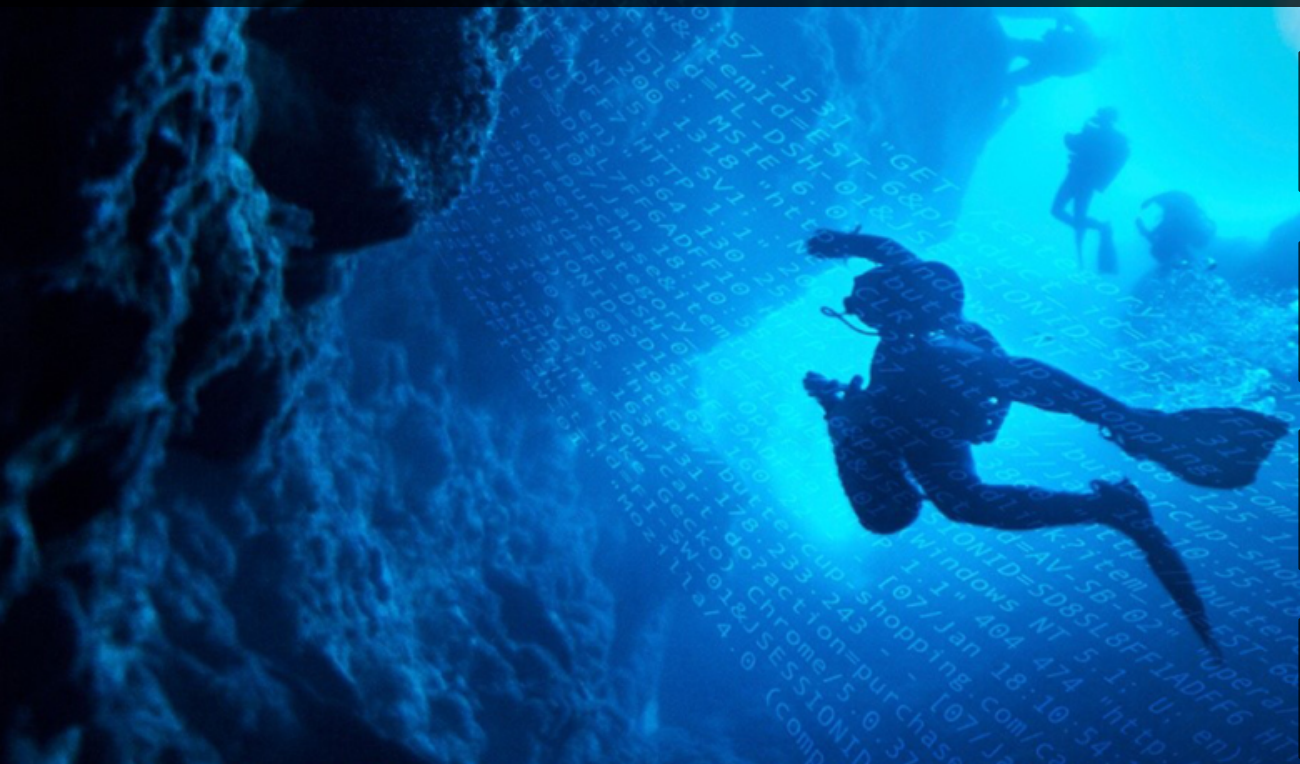
"I like the concept of a security fabric because it **simplifies security**, and it enables network and security professionals to **respond** to cyber attacks **faster**, **minimizing** the impact of a **breach**."

Simplification for faster, better response

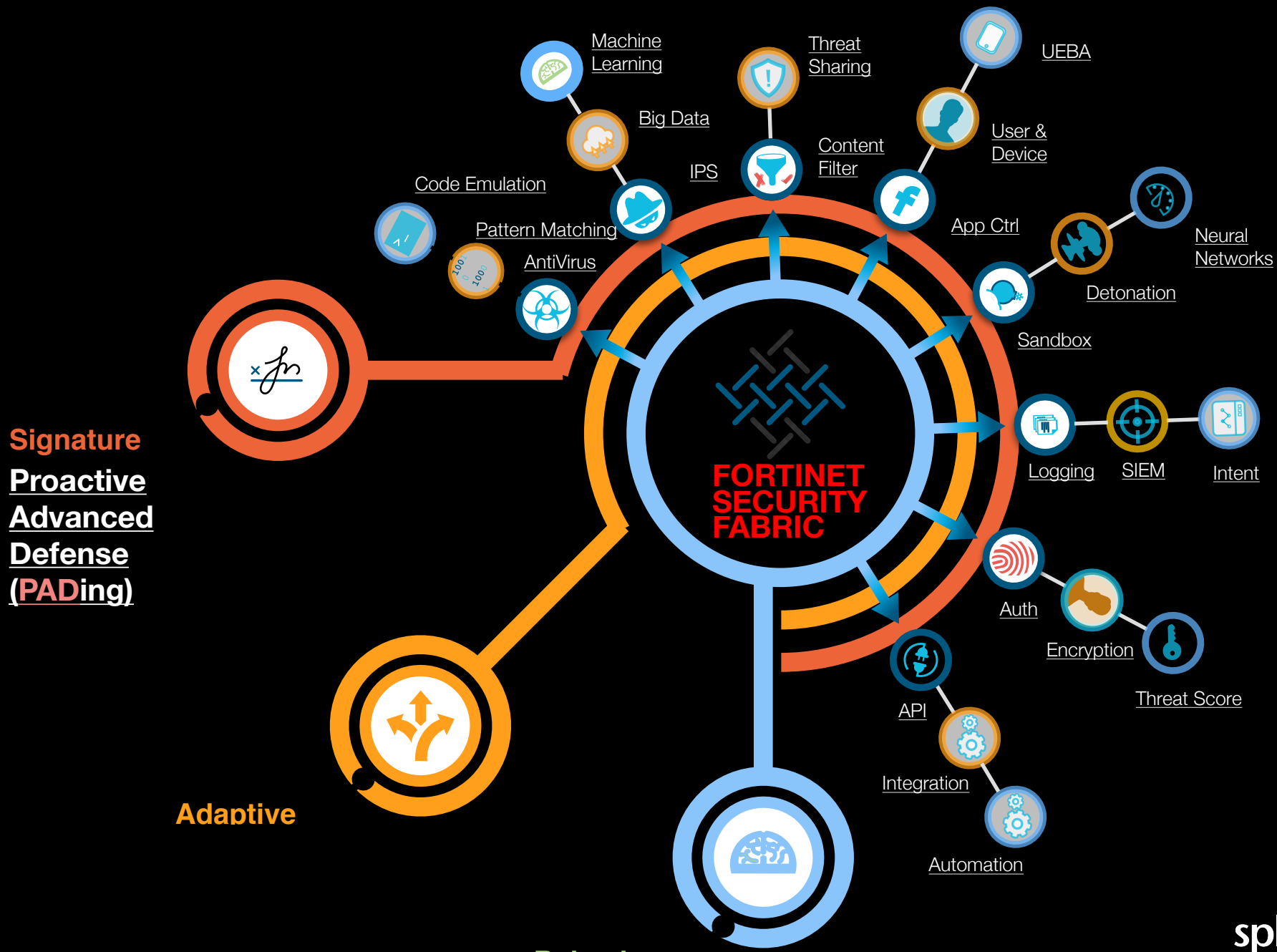
Network World, 2017
https://goo.gl/k1dGwH

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



splunk> .conf2017

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