Collaborative Security Model

Christof Jungo

Head of Security Architecture,

Swisscom Switzerland Ltd.

Haiyan Song

SVP Security Markets,

Splunk Inc.

splunk>

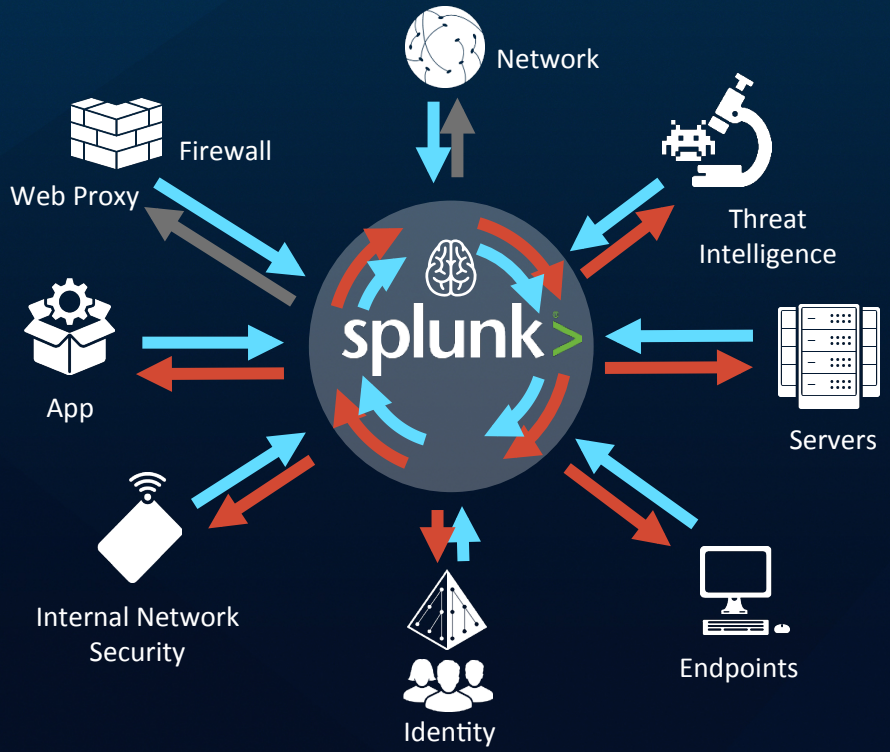
Disclaimer

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 the 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.

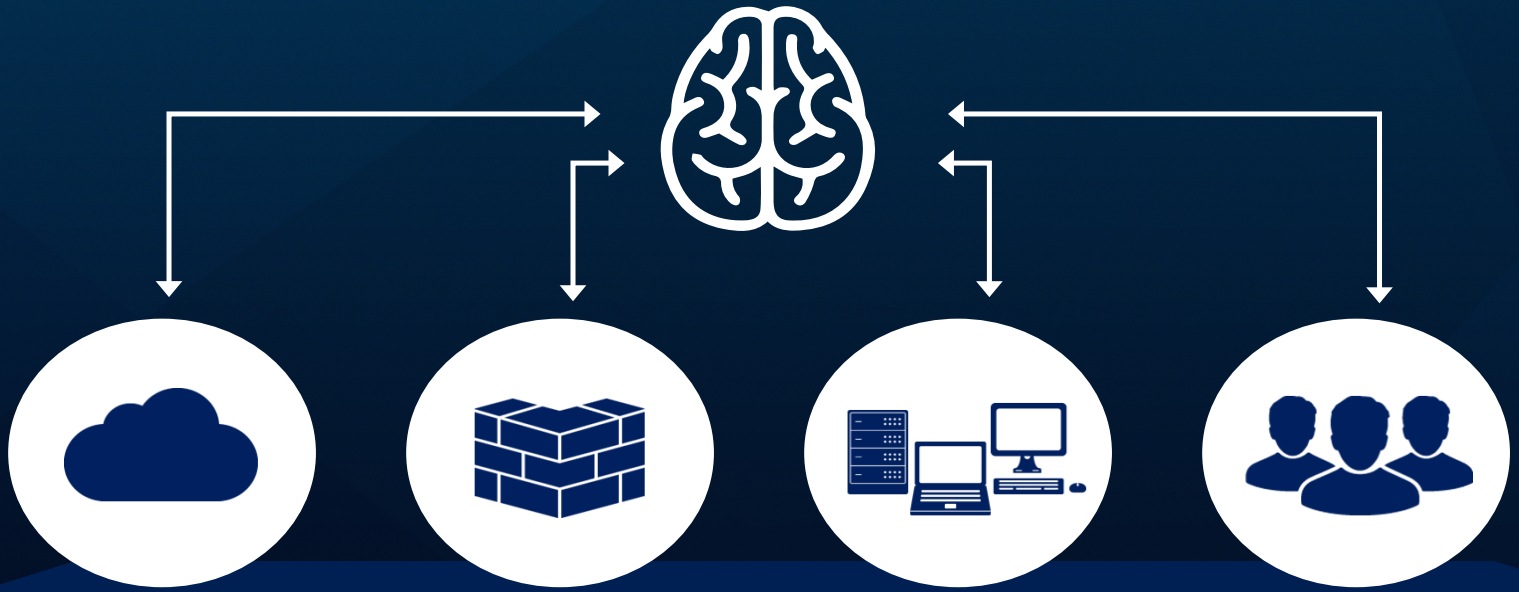
In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.


SECURITY NEEDS
A NEW APPROACH
AND A WELL
ORCHESTRATED SYSTEM

Splunk is the Security Nerve Center

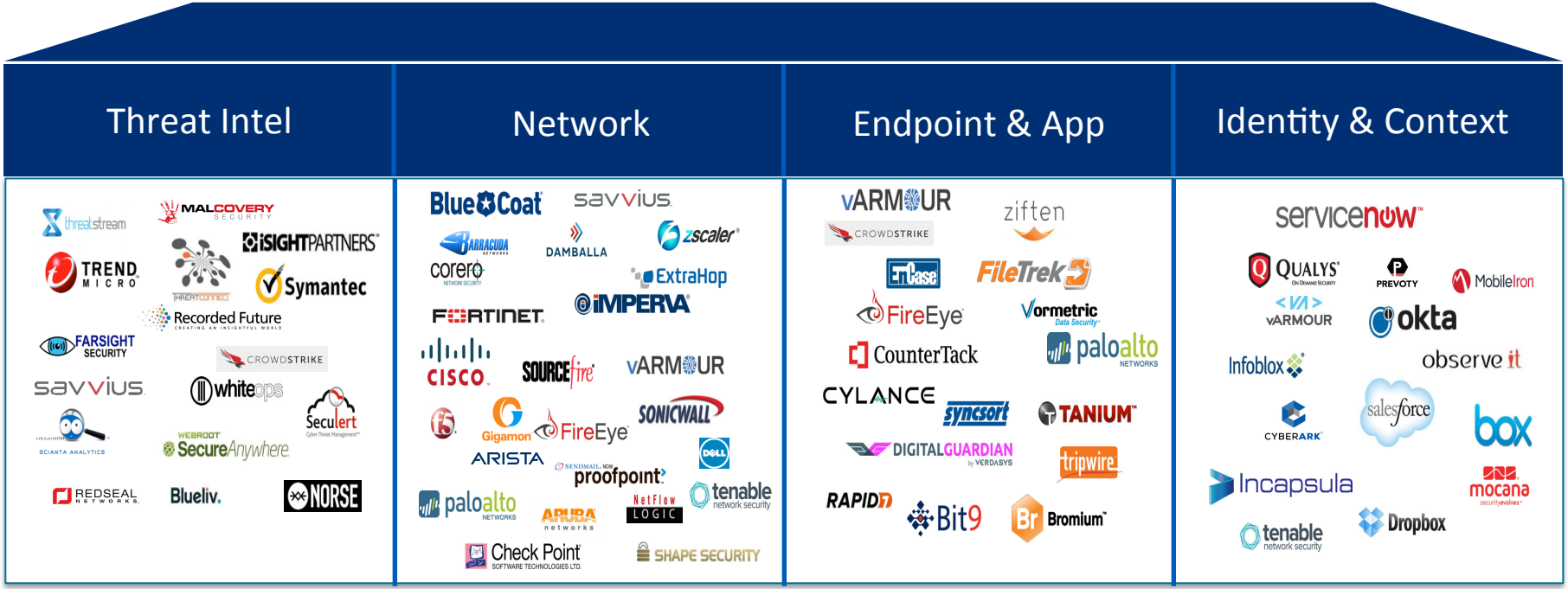


Nerve Center & the Ecosystem



Threat Intel | Network | Endpoint & App | Identity & Context

Security Ecosystem



Collaborative Security Model

Christof Jungo

Head of Security Architecture,

Swisscom Switzerland Ltd.

splunk>

Personal Introduction

swisscom

- Christof Jungo is the Head of Security Architecture and Engineering at Swisscom, the largest Telco provider in Switzerland
- More than ten years of experience in managing the design and development of security solutions in the Internet provider domain
- Previously, Chief Technology Officer and member of the management at NETIX, specializing in networking and security
- Author of numerous articles on Cloud Security and council member of the Information Security Forum (ISF)

Swisscom Network

Our network infrastructure

Ultra-fast broadband coverage (fibre optic) | > 1.4 million homes and businesses

TV coverage

- 93% digital TV
- 88% HDTV

Mobile broadband coverage

- 99% 2G
- 98% 3G
- 98% 4G/LTE

Universal service & ADSL | • 97% (>2Mbps)

Swisscom has one of the best telecoms infrastructures in the world.

Fixed network:

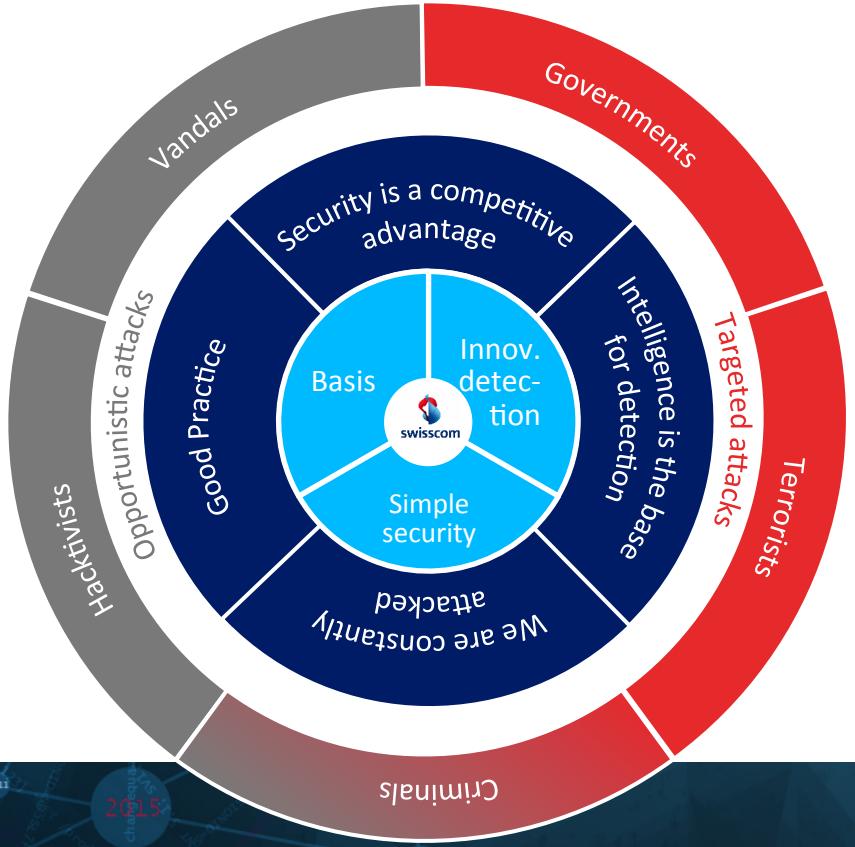
By the end of 2015, Swisscom will supply 2.3 million homes and businesses with ultra-fast broadband.

Mobile network:

By 2016, Swisscom will have extended 4G/LTE coverage to 99% of the Swiss population.

Swisscom Security

Our Aspiration: << We build security for people in a connected world – always and everywhere>>



How to Protect the Business

Targeted cooperation is required for success

Prevention	Detection	Intervention
• Proactive protection of data at various levels Systems, Employees, Networks	• Early detection of attacks • Collection of information on intrusions from the Internet and the data	• Efficient and effective response to security incidents
• Training/awareness of employees (phishing campaign) • Continuity management • Resilience • Security risk management	• Data leakage prevention • SIEM • Threat intelligence • HoneyNet • Exchange with third parties	• Robust incident processes • Abuse and fraud management • Automated reactions • Disaster recovery and crisis management

Basic Principles

- Basic protection provisions, processes and technologies on which other measures are based

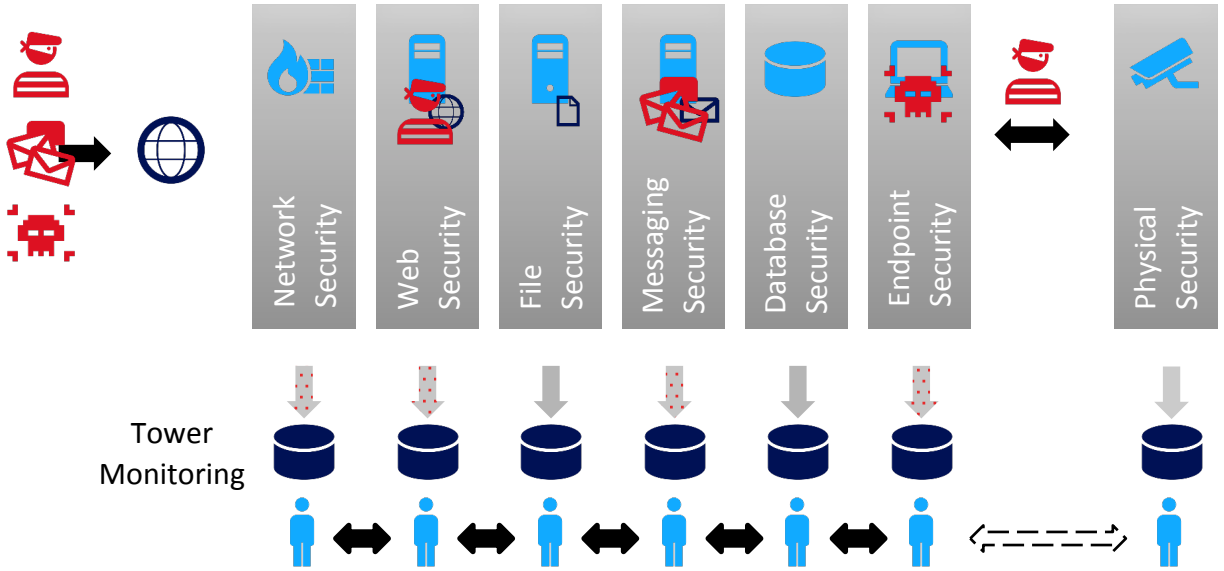
- Policy framework
- Identity and access management
- Physical security
- Cooperation with other organizations
- Asset & risk inventory
- Knowledge about the threat situation
- Firewalls, intrusion detection systems, antivirus software, …

Internal Challenge

Environments have developed over time

Impact of IT Industrialization

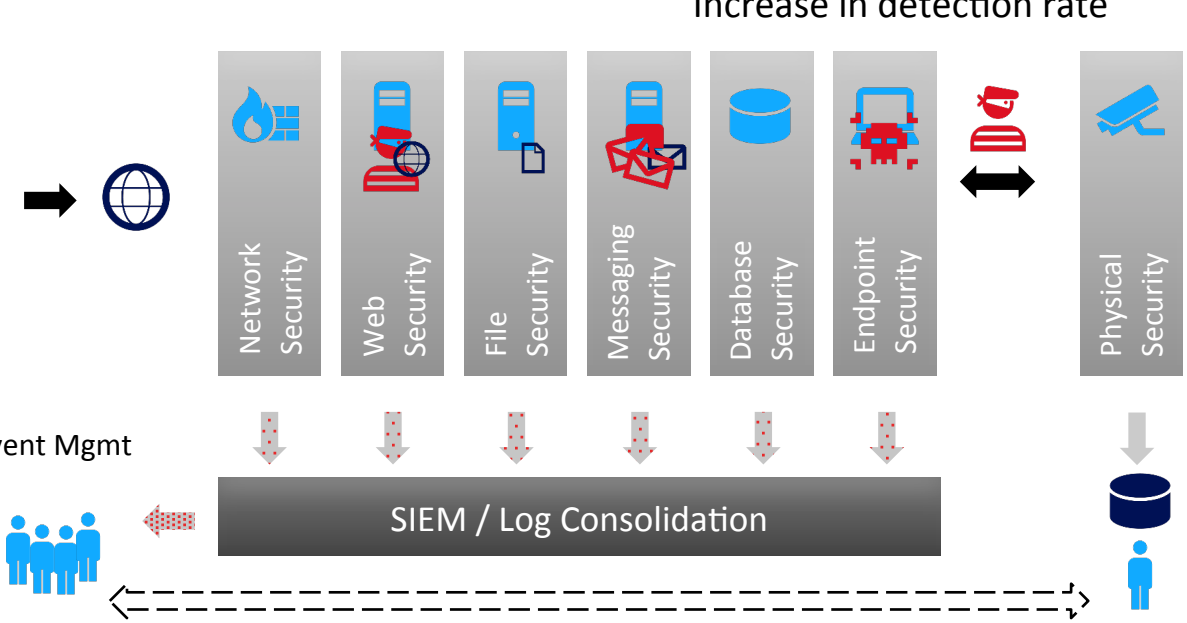
Silo landscapes and isolated analysis of security



- Detection time: modest
- Coordination time: high
- Remediation time: high to very high
- Integration costs: very high with umbrella systems

Centralization and Consolidation

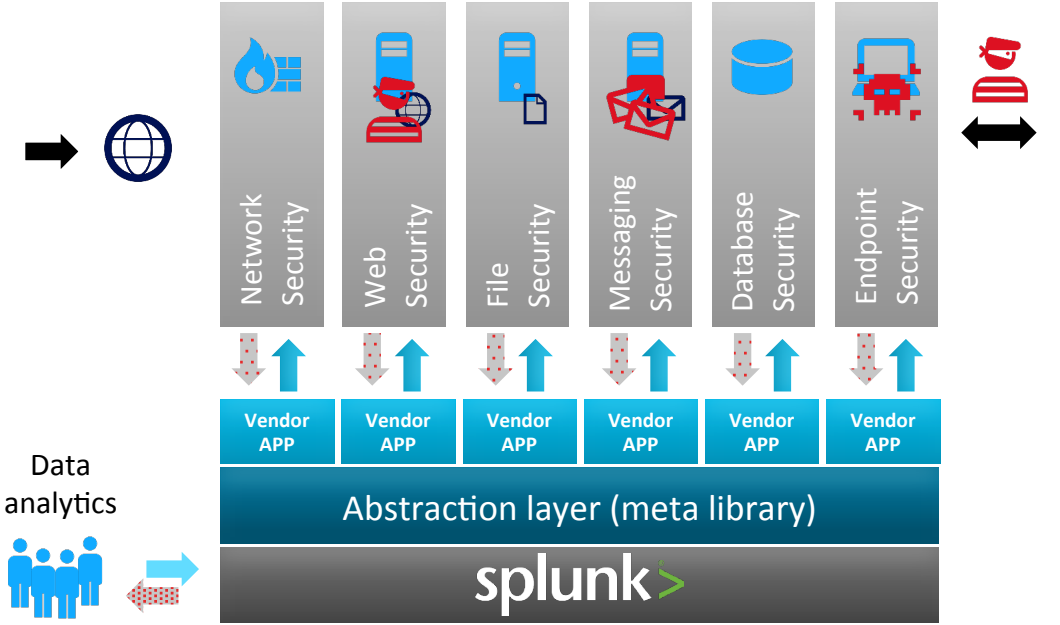
Increase in detection rate



- Detection time: good
- Coordination time: average
- Remediation time: average
- Integration costs: high

Active Response

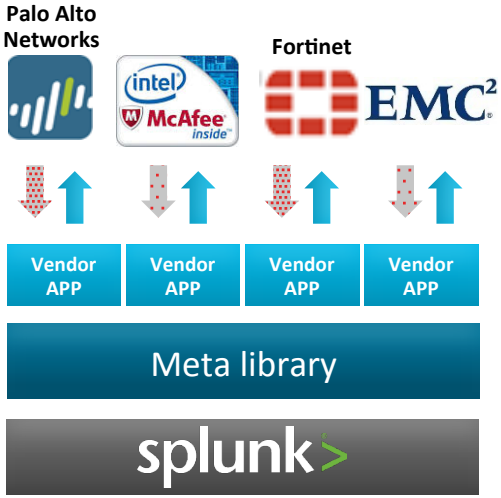
Set-up of abstraction layer and response channel



- Detection time: good
- Coordination time: low
- Remediation time: low
- Integration costs: low

Prototype/Demonstrator

Set-up of eco-system



Meta library

- Open and freely upgradeable abstraction layer for security commands as per CSS (design language in web design)
- Standardisation by a body aka W3C World Wide Web Consortium
- Integral element of Splunk (without additional costs)

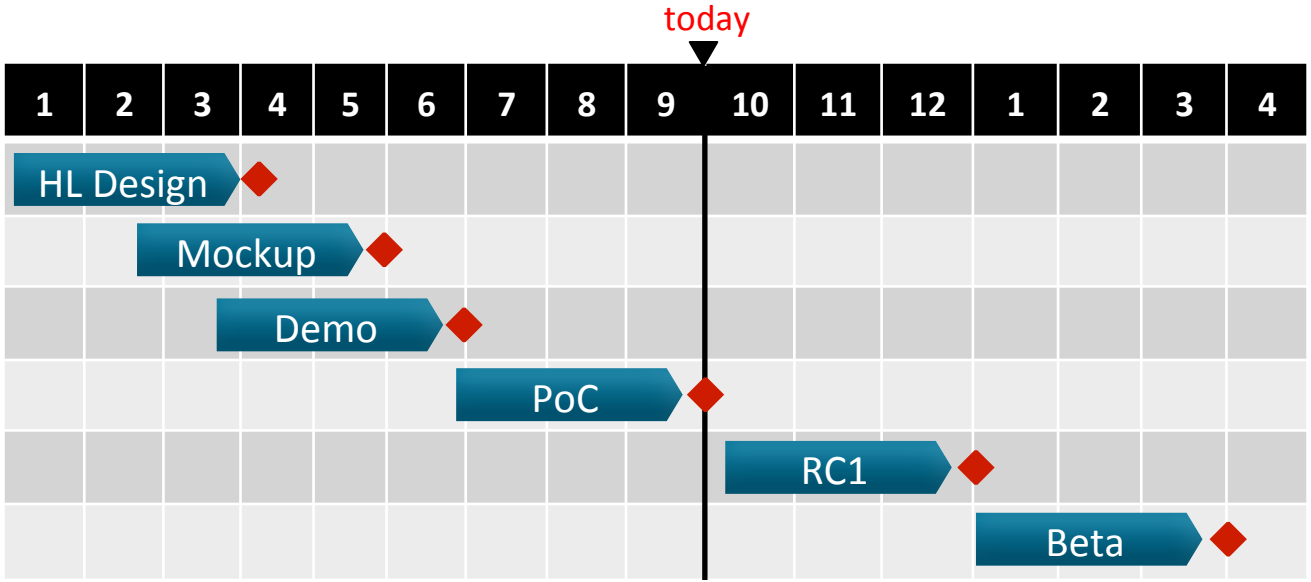
Vendor APP

- Establishment of the communication channel
- Translation of the meta library into device-specific commands and configurations
- APP development by manufacturers
- APP store for manufacturers

Onboarding

- Straightforward onboarding processes for manufacturers
- Quality assurance processes for APP

Planning and Milestones



Benefits of the Collaborative Security Model

Interaction and adaptability

Collaboration and eco-system through open interfaces, easy integration and distributed development costs. The focus is on simplicity, flexibility and dynamism.

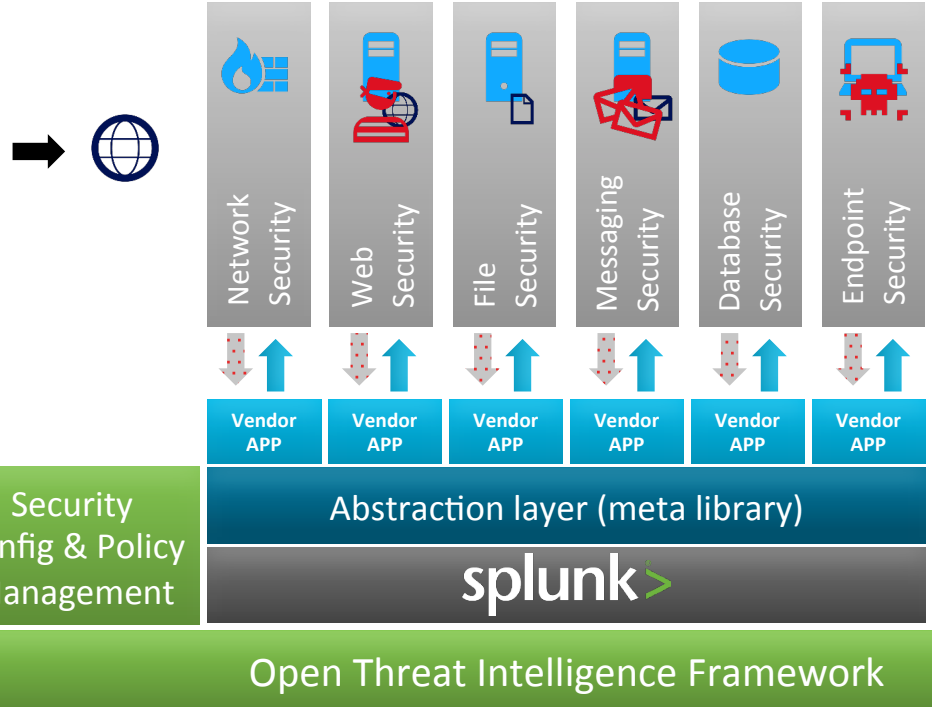
The Collaborative Security Model

- Reduces the dependence of security manufacturers and encourages them to improve the quality of their products
- Enables interaction between various manufacturers
  - Eco-system instead of silo landscape
- Facilitates the integration of new components (Plug&Play)
- Reduces management requirements (SoC & CSIRT) and costs

The market functions well if willingness to collaborate is part of the manufacturers' product strategy.

The Next Level

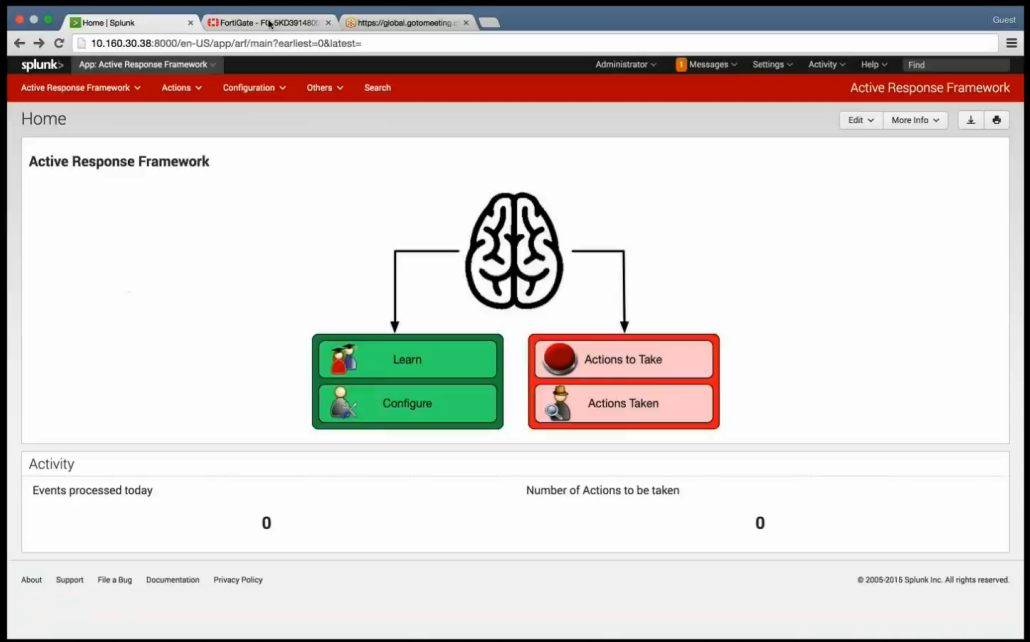
Integration with other threat detection components



The next level is a tight integration with exitsting Threat Intelligence Network as well as Automatic Testing Environments like Vulnerability Scanning or Penetration Testing Frameworks

Demo

Integration between Fortinet and Splunk



Questions?

THANK YOU

splunk>