EUROPEAN
BIG DATA
VALUE FORUM
VERSAILLES, NOV 21-23 2017

European Commission

BDV BIG DATA VALUE ASSOCIATION

Inria inventors for the digital world

Big Data Analytics in Cyber Security: F-Secure's View

Alexey Kirichenko
Research Collaboration Manager
F-Secure Corporation

INDEX

1. F-Secure’s Operations
2. Data Analytics: Where High Value Can Be
3. Opportunities and Foundations
4. AI Work Avenues, as of Today
5. Targets and Challenges

SECTION 1

F-Secure’s Products and Services

Broad range: Prevention, Protection, Detection, Response, Recovery

In both corporate and consumer domains

Global operations, with ~ 3/4 of the revenues from Europe

Traditionally, focusing on endpoints, aiming at expanding

Since 1988

F-Secure

CYBER SECURITY LIVES HERE

Key products for consumers

F-Secure SAFE	End point protection, family protection
F-Secure FREEDOME	VPN & privacy
F-Secure KEY	Password management
F-Secure SENSE NEW	Connected home, Internet of things

Key products for businesses

	Small businesses	Mid-market	Global enterprises
Protection Service for Business **Business Suite** – Endpoint Protection	●	●	
Rapid Detection Service – Managed Detection & Response		●	
F-Secure Radar – Vulnerability Management	○	●	
Cyber security services – Cyber security Consultancy		○	●

SECTION 2

Where Data Analysis Can Be Instrumental

Identify or detect malicious objects and activities: more and faster.

Reduce noise, decision mistakes, human expert effort.

Enable optimal ways of combining human expertise and automation.

Provide Business Intelligence.

SECTION 3

Foundations: Data, Expertise, Technology

Our client SW and other operations bring highly relevant data.

Our cyber security experts, researchers, and consultants provide invaluable knowledge and insight.

We have a team fully focusing on data analytics for cyber security.

We are building a platform for data storage and processing, Data Lake: metadata handling, support for installation and use of task- and dataset-specific tools, enabling correlation, access control, cost efficiency, traceability, GDPR compliance.

SECTION 4

Primary Applications Today

Intrusion detection, in particular, Rapid Detection Service:
- detecting threats similar to known ones
- detecting attack-relevant anomalies
- reducing amounts of data to process in near-real-time
- assisting security experts, in particular, via visualization

Malware identification in the backend.

Malware detection in the endpoint, behavior-based, near-real-time.

Web content classification: parental control and browsing protection.

SECTION 5

Where Do We Want to Go Tomorrow?

Better tuning detection models for specific endpoint – user profiles

Assisted learning, utilization of expert feedback

Interpretability of detection, enabling effective response

Threat Intelligence

THANK YOU