Live Correlation of Threat Intelligence with Historical Data

Matthias Vallentin

TENZIR

DFN CERT®

IFB | innovations starter

maritimes cluster norddeutschland

Outline

1. **Complex Attacks:** the Need for SOCs
2. **Network Forensics:** Retrospective Analysis
3. **Threat Intelligence:** Managing Security Knowledge
4. **Live Correlation:** Adding Value through Automation

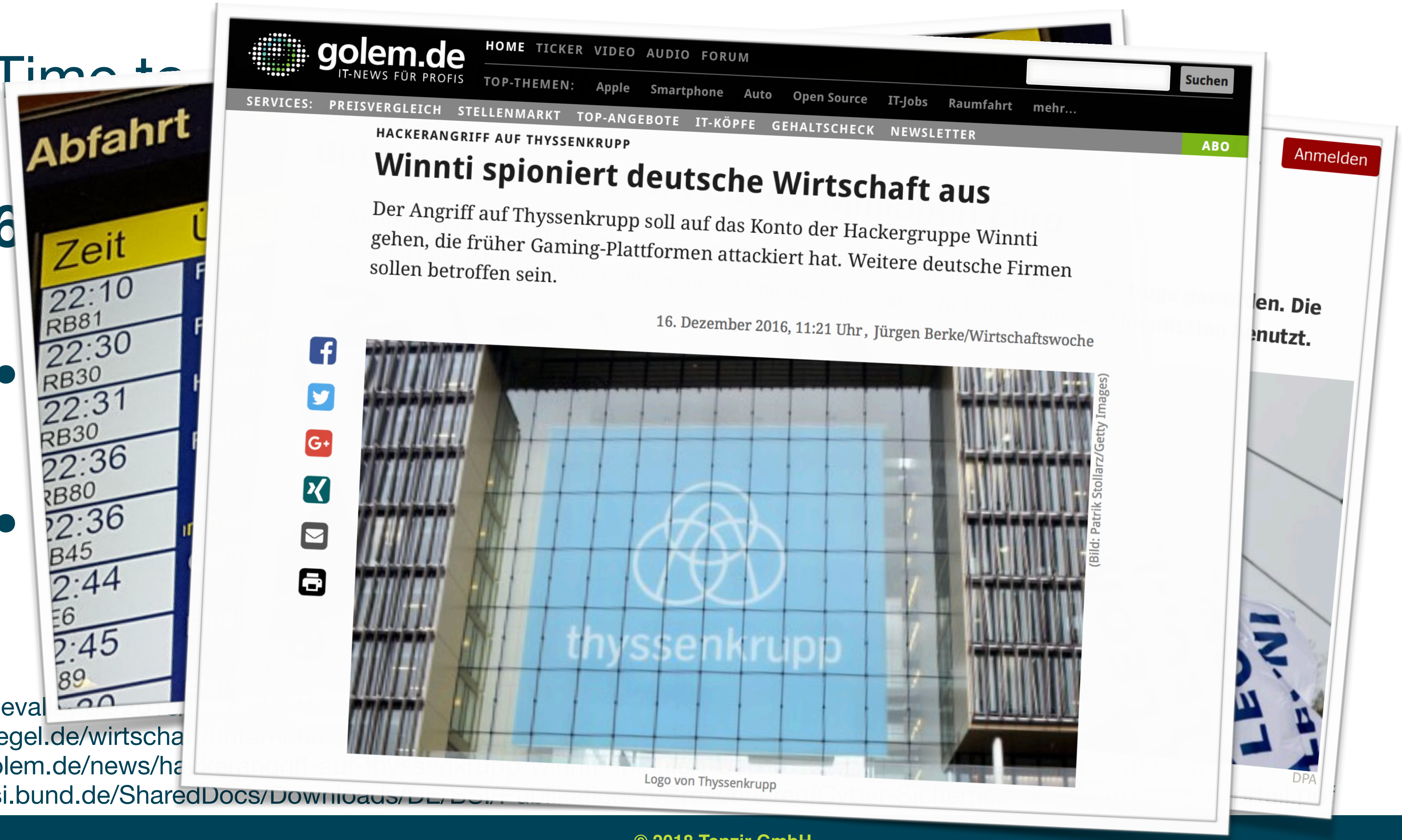
Complex Attacks

The Need for SOCs

Complex Attacks

aka. Advanced Persistent Threats (APTs)

- Ransomware, financial fraud, cyber espionage
- Time to
- 6



Abfahrt
Zeit
22:10
RB81
22:30
RB30
22:31
RB30
22:36
RB80
22:36
B45
2:44
E6
2:45
89
golem.de
IT-NEWS FÜR PROFIS
HOME TICKER VIDEO AUDIO FORUM
TOP-THEMEN: Apple Smartphone Auto Open Source IT-Jobs Raumfahrt mehr...
Suchen
SERVICES: PREISVERGLEICH STELLENMARKT TOP-ANGEBOTE IT-KÖPFE GEHALTSCHECK NEWSLETTER
ABO
Anmelden
len. Die
nutzt.
DPA

HACKERANGRIFF AUF THYSSENKRUPP

Winnti spioniert deutsche Wirtschaft aus

Der Angriff auf Thyssenkrupp soll auf das Konto der Hackergruppe Winnti gehen, die früher Gaming-Plattformen attackiert hat. Weitere deutsche Firmen sollen betroffen sein.

16. Dezember 2016, 11:21 Uhr, Jürgen Berke/Wirtschaftswoche

(Bild: Patrik Stollarz/Getty Images)

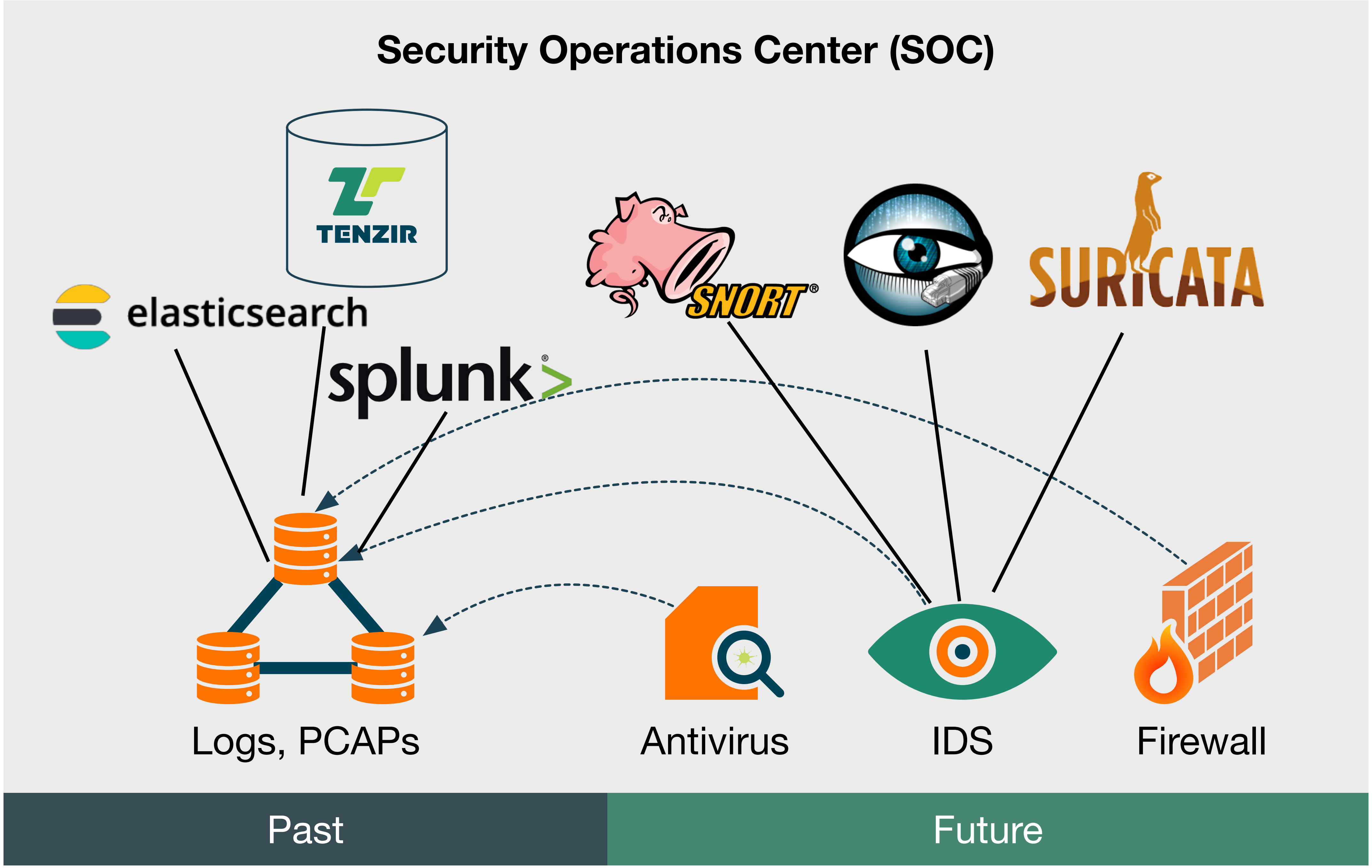
Logo von Thyssenkrupp

https://hh.hanseval
http://www.spiegel.de/wirtscha
https://www.golem.de/news/ha
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/

Infection Vectors

- Commonly
  - **Spear phishing**: personalized email with malware attachment (or link to it)
  - **Drive-by downloads**: visiting websites that install malware automatically
- Rarely
  - **Direct attack** by exploiting software vulnerabilities

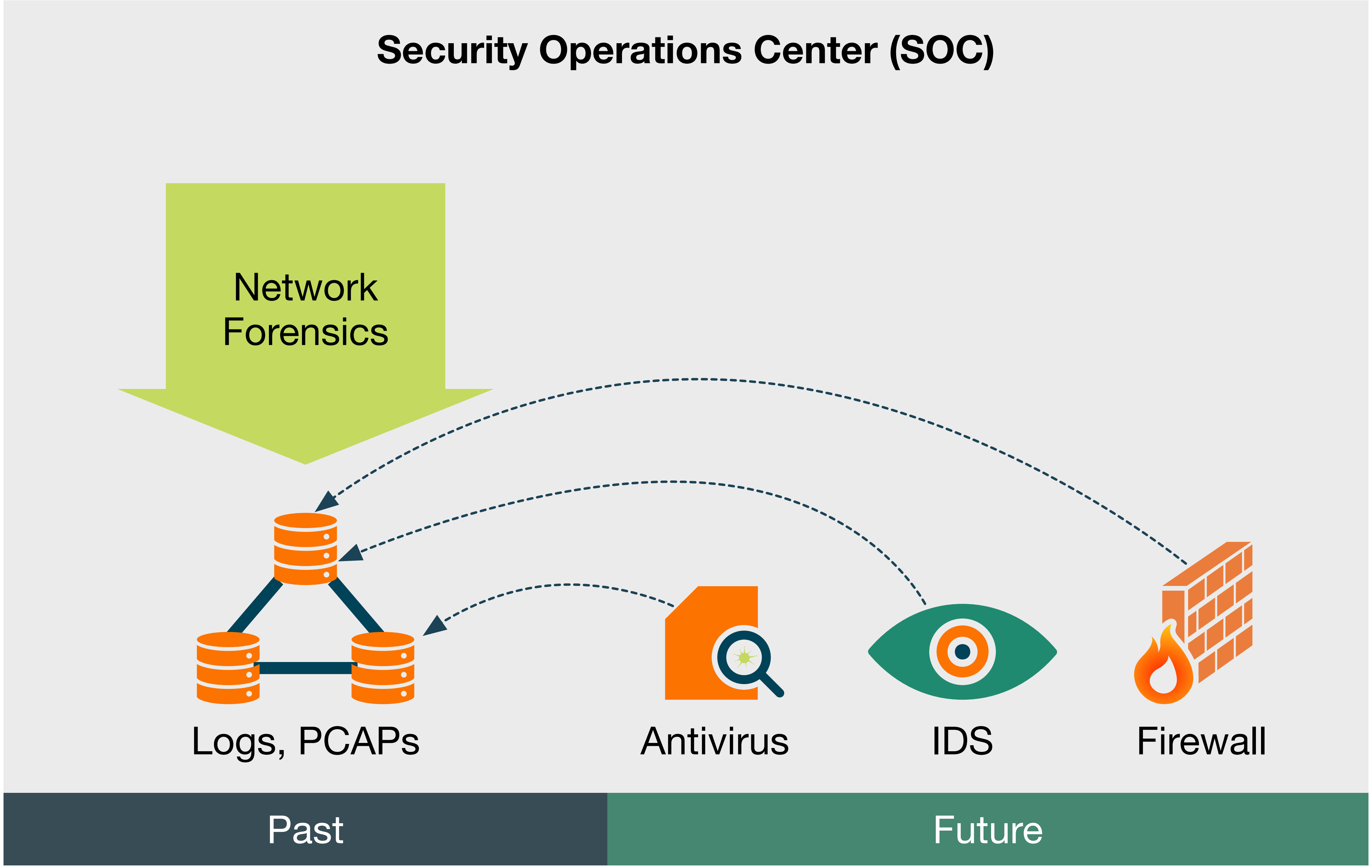
Building Blocks



Network Forensics

Retrospective Analysis

Building Blocks



Demo

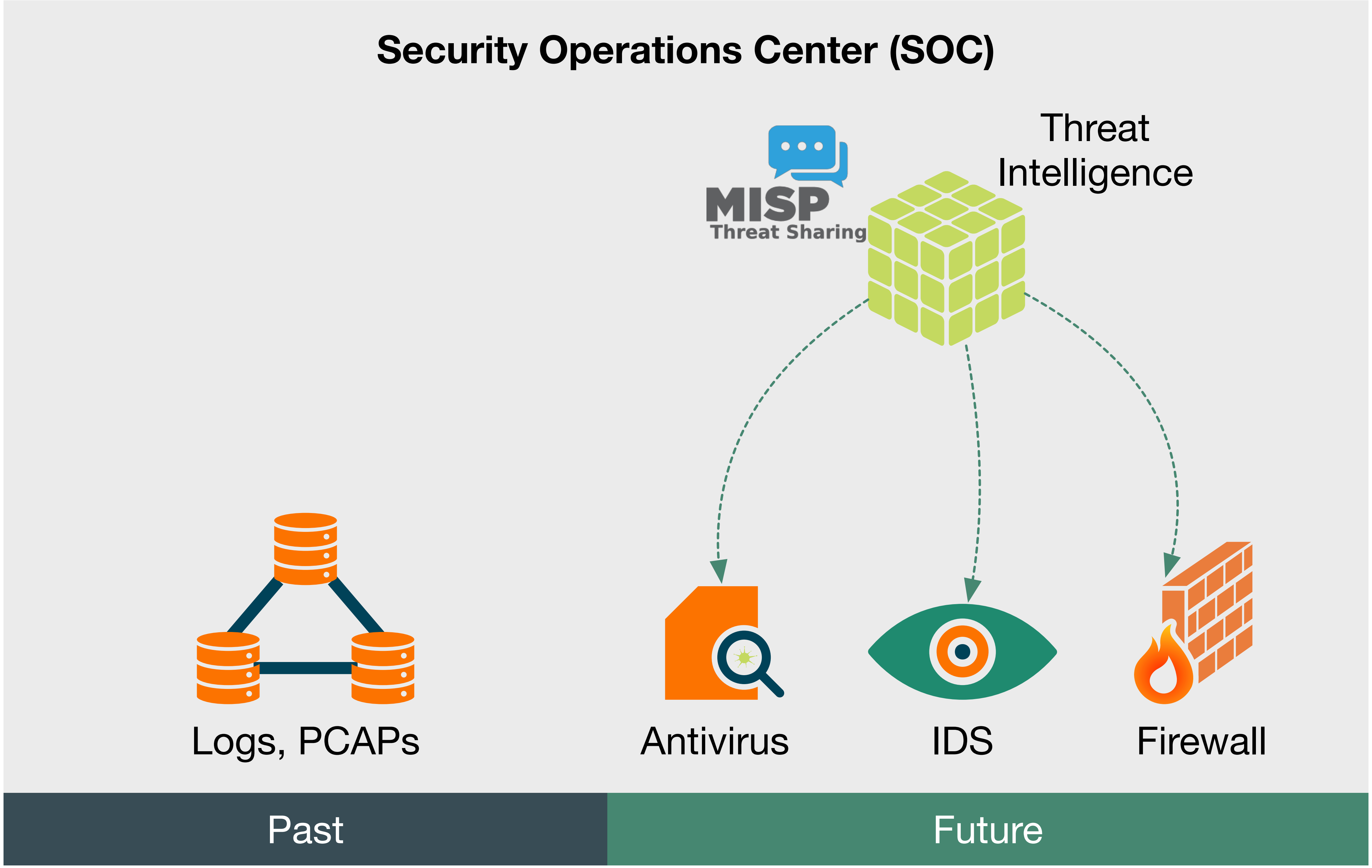
Threat Intelligence

Managing Security Knowledge

Threat Intelligence

- **Knowledge** about:
  - **Intention and capabilities of threat actors**
  - **Tactics, techniques, and procedures (TTPs)**
- **Goal:** improve decisions on risk and effects of threats
- Served as **feeds**: continuously updating **streams of data**
  - **Indicators of Compromise (IoC)**: attack evidence operators can look for

Building Blocks



MISP

Malware Information Sharing Platform

- Tool to **manage threat intelligence lifecycle**
- Enables **automated sharing** of data at fine granularity
- **Stores and correlates** indicators of compromise (IoCs)
- **Data model** to describe events, feeds, and threat actors
- **Import/export** supporting many tools and formats
- **API**: REST & Python

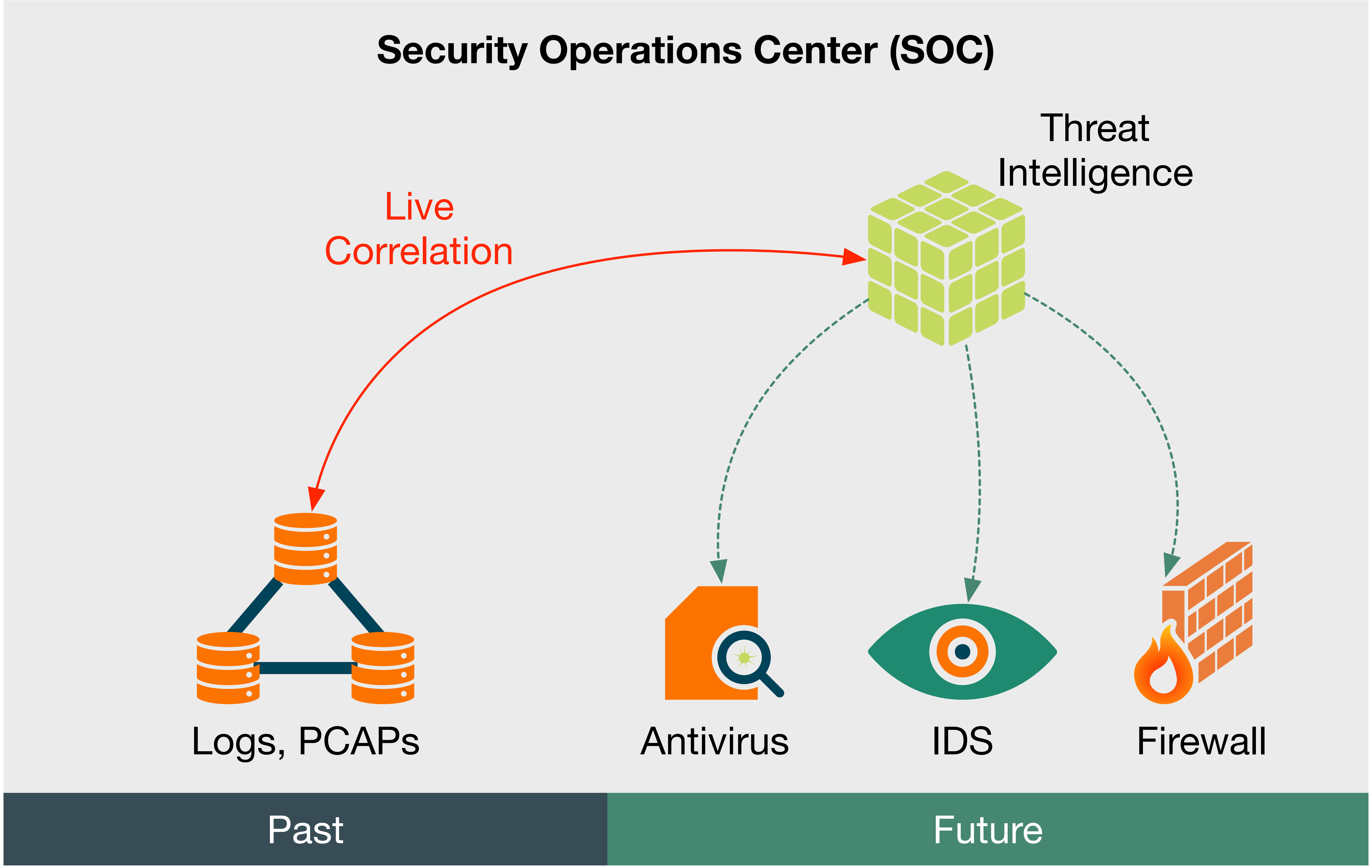
MISP
Threat Sharing

Demo

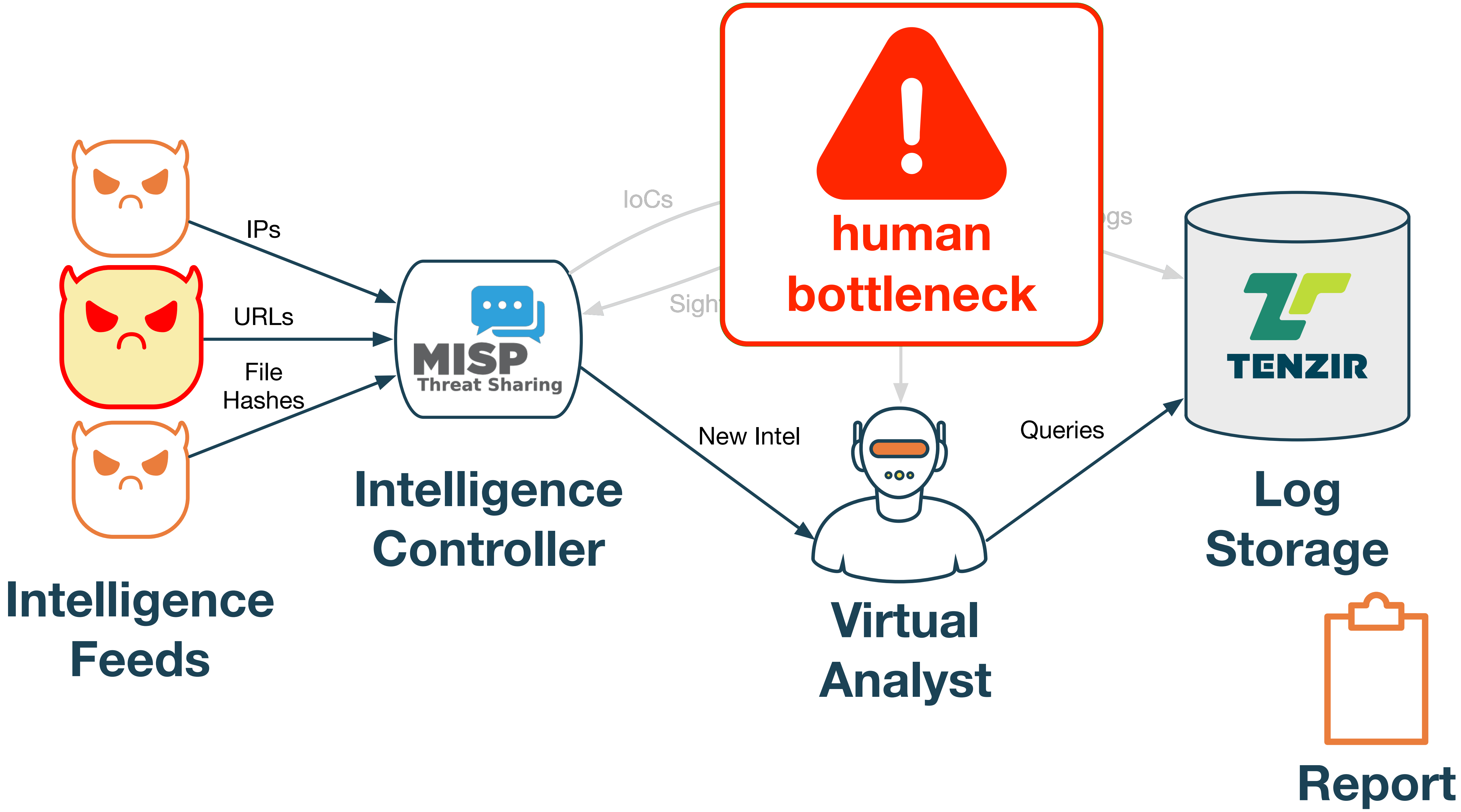
Live Correlation

Adding Value through Automation

Building Blocks



Workflow



human bottleneck

Intelligence Feeds

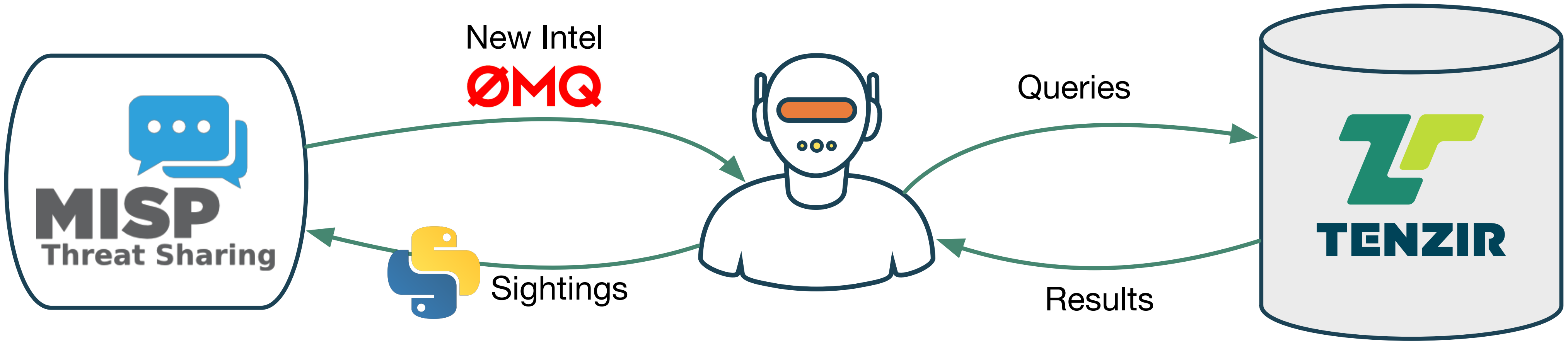
Intelligence Controller

Virtual Analyst

Log Storage

Report

Implementation



Demo

Conclusion

- **Complex attacks** manifest over long time periods

  ➡ **Network forensics** must be first-class citizen in analysis

- **Threat intelligence** is a key component of a modern SOC

  ➡ Today, integration primarily with **detection systems**

- Value in **automating historical intelligence correlation**

  ➡ **Less experts needed** in already understaffed SOC

  ➡ **Automated reporting** consumable by "normal" sys admins

  ➡ Enables **automated data processing** where no humans are allowed

Thanks for Listening!

tenzir.com

tenzir_company

vast-io/vast

Backup Slides

Tenzir CORE

- Scalable **data plane** for network forensics
- Built on top of **open-source engine VAST**
- Features
  - **Interactive search** in typed query language
  - **Native support for Zeek & PCAP** import and export
  - Integration with **R, Python/Pandas, Spark***
- We are looking for alpha testers. Come talk to us!

*under development