Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

MARESEC 2021

IT Security Monitoring at a Port Terminal Operator

Jens Wettlaufer, Matthias Marx, Jens Lindemann, Hannes Federrath

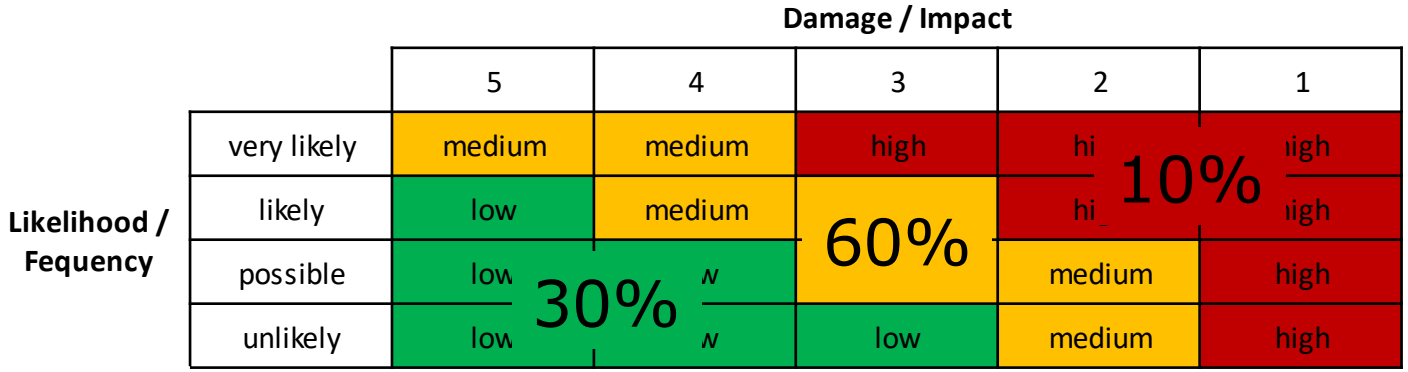
June 14th 2021

Research Questions & Agenda

- How can we detect sophisticated attacks in the diverse threat landscape of a port terminal operator?
  - Inventory and cyber risk assessment
  - Kill Chain-based contextualization and choice of intrusion detection methods
  - Anomaly detection use cases
- How can we integrate the information in the day-to-day business of non-specialized personnel?
  - Goal-driven visualization for non-specialized personnel

Inventory and Cyber Risk Assessment*

- Identification of critical applications
  - incl. redundancy, processing of personal data, importance of IT security objectives
- Collection of risk scenarios
  - e.g. container theft, data theft, terminal sabotage
- Evaluation of risks
  - regarding likelihood and impact



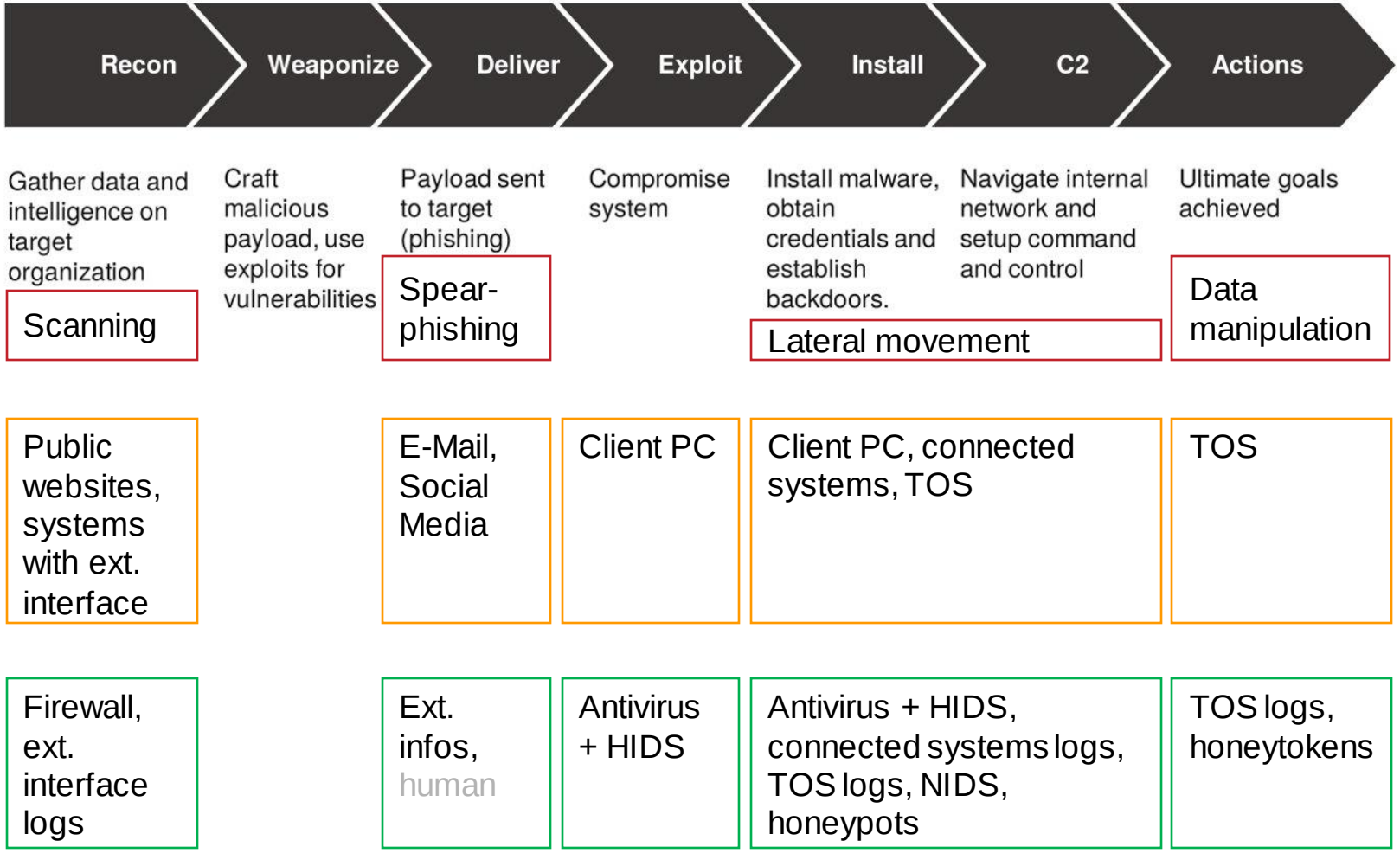
Application	Users	Redundancy	Personal Data	Confidentiality	Integrity	Availability	External Interface
TOS-Container Tracking	Terminal	yes	yes	x/5	x/5	x/5	yes

* based on *ISO 27001* and *BSI IT-Grundschutz*

Kill Chain-based Contextualization of Damage Scenarios

- Integration of scenarios
  - e.g. terminal sabotage using malware
- Identification of potentially involved systems
- Identification of detection sources

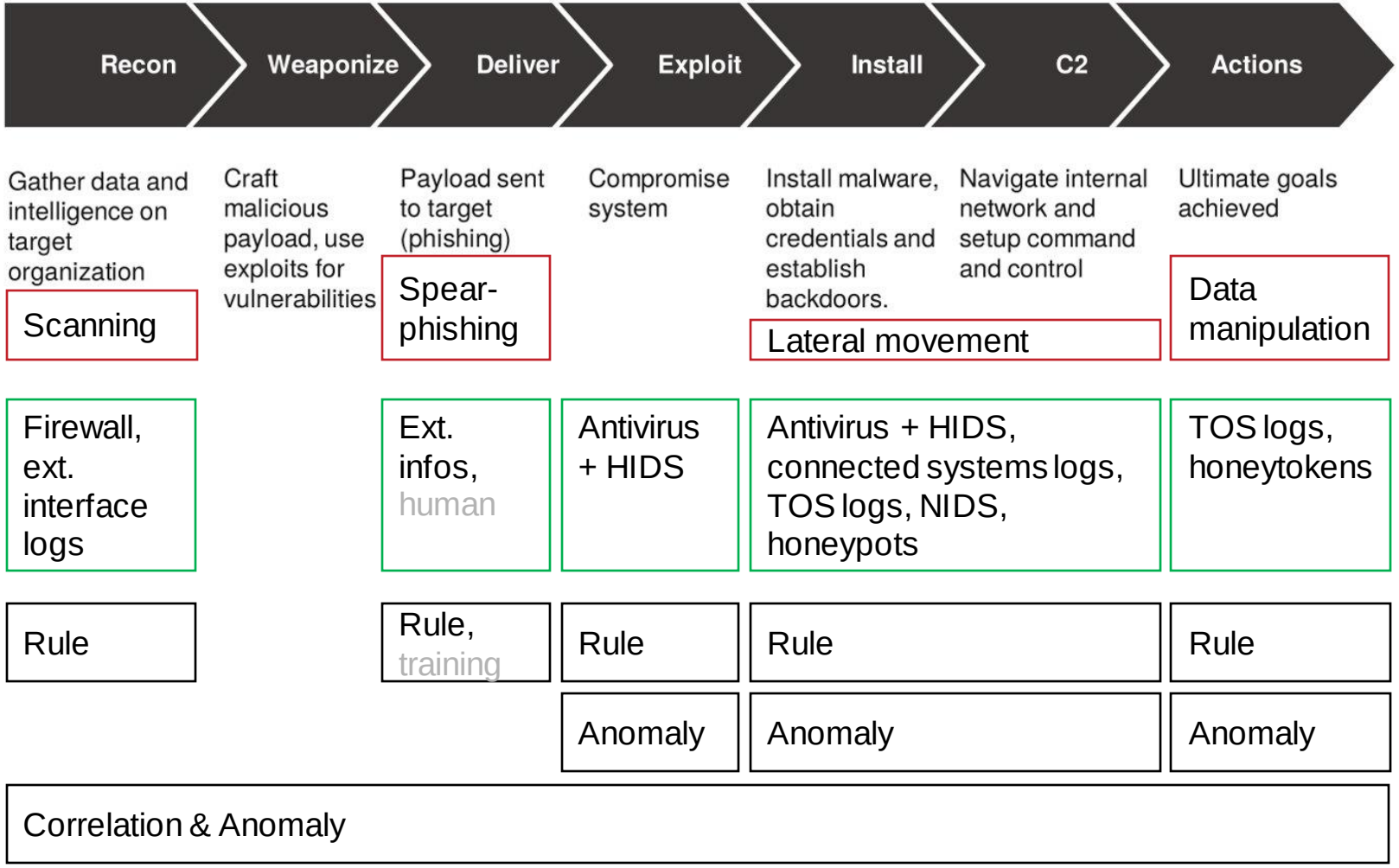
Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin. *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. Leading Issues in Information Warfare & Security Research. 2011.



Intrusion Detection Methods

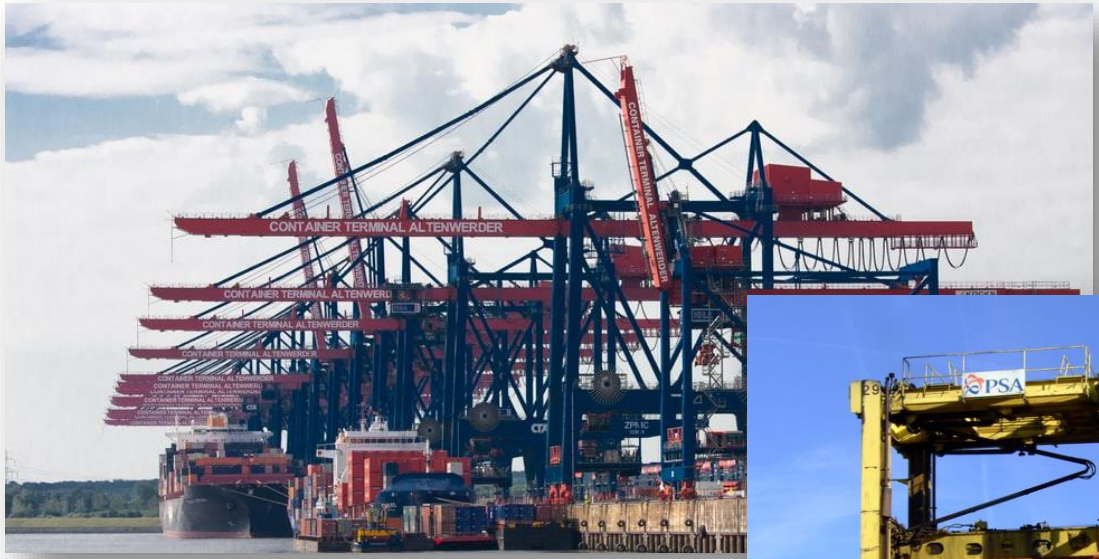
- Application-specific rule-based
  - e.g. >3 login failures for one username internally, log with type 'warning'
- Application-specific anomaly-based
  - e.g. communication with unusual IPs/subnets
- Correlation-based across applications
  - e.g. same user login failures in different systems, NIDS anomaly + honeytoken

Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin. *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. Leading Issues in Information Warfare & Security Research. 2011.

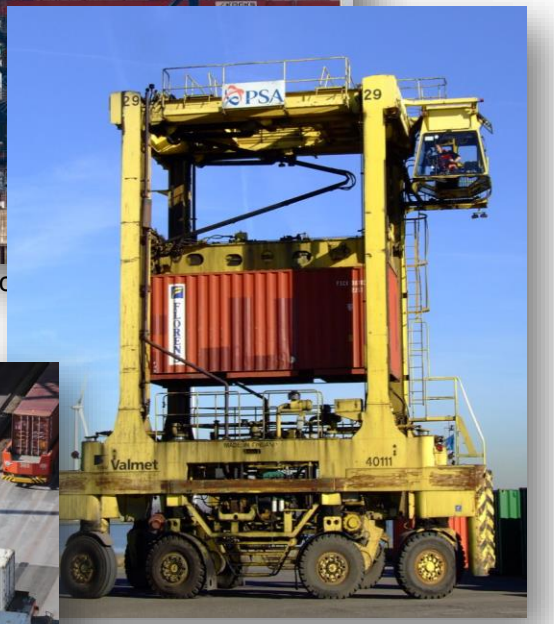


Meaningful Anomaly Detection Use Cases in Port IT Security

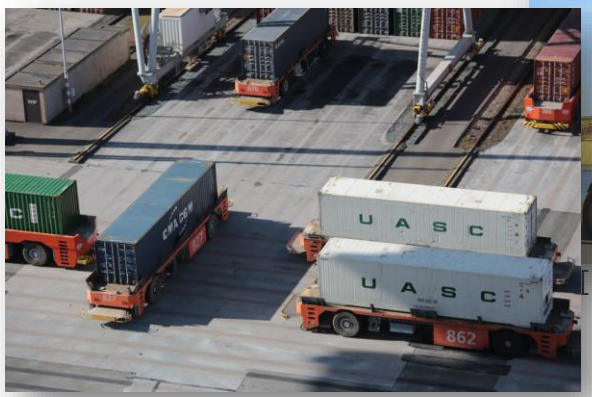
- Log/Alert time-series
  - e.g. count, frequency, …
- Profile building of user behavior
  - e.g. office personnel, crane drivers, straddle carrier drivers, …
- Behavior of network traffic
  - e.g. TOS communication, container bridge communication, …
- Behavior of industrial control systems
  - e.g. container bridges, autonomous cranes, AGVs, …



[https://unsplash.co



[https://commons.wikimedia.org/w/index.php?curid=21424585]

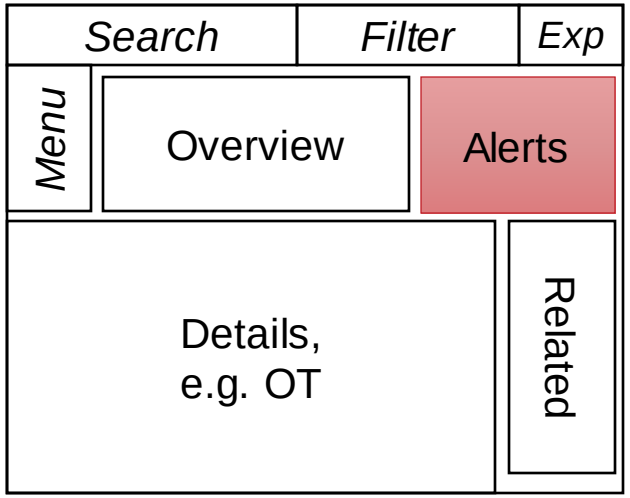


[https://unsplash.com/photos/eCc7FjMoR74]

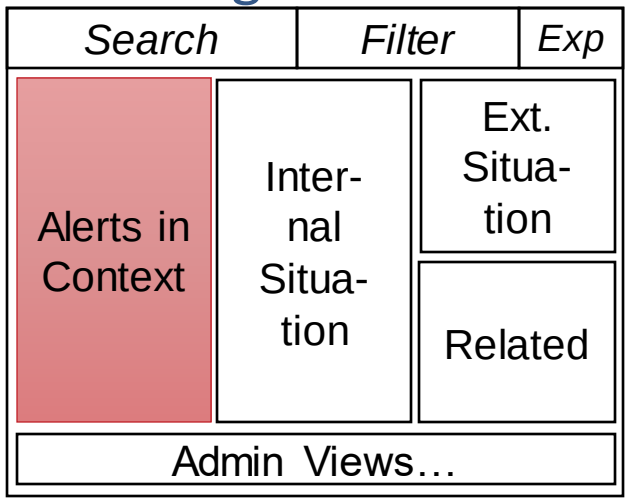
Goal-driven* Visualization for Non-specialized Personnel

- Interviews with multiple different departments
- Creation of *personas* based on similar goals

IT Admin



IT Management

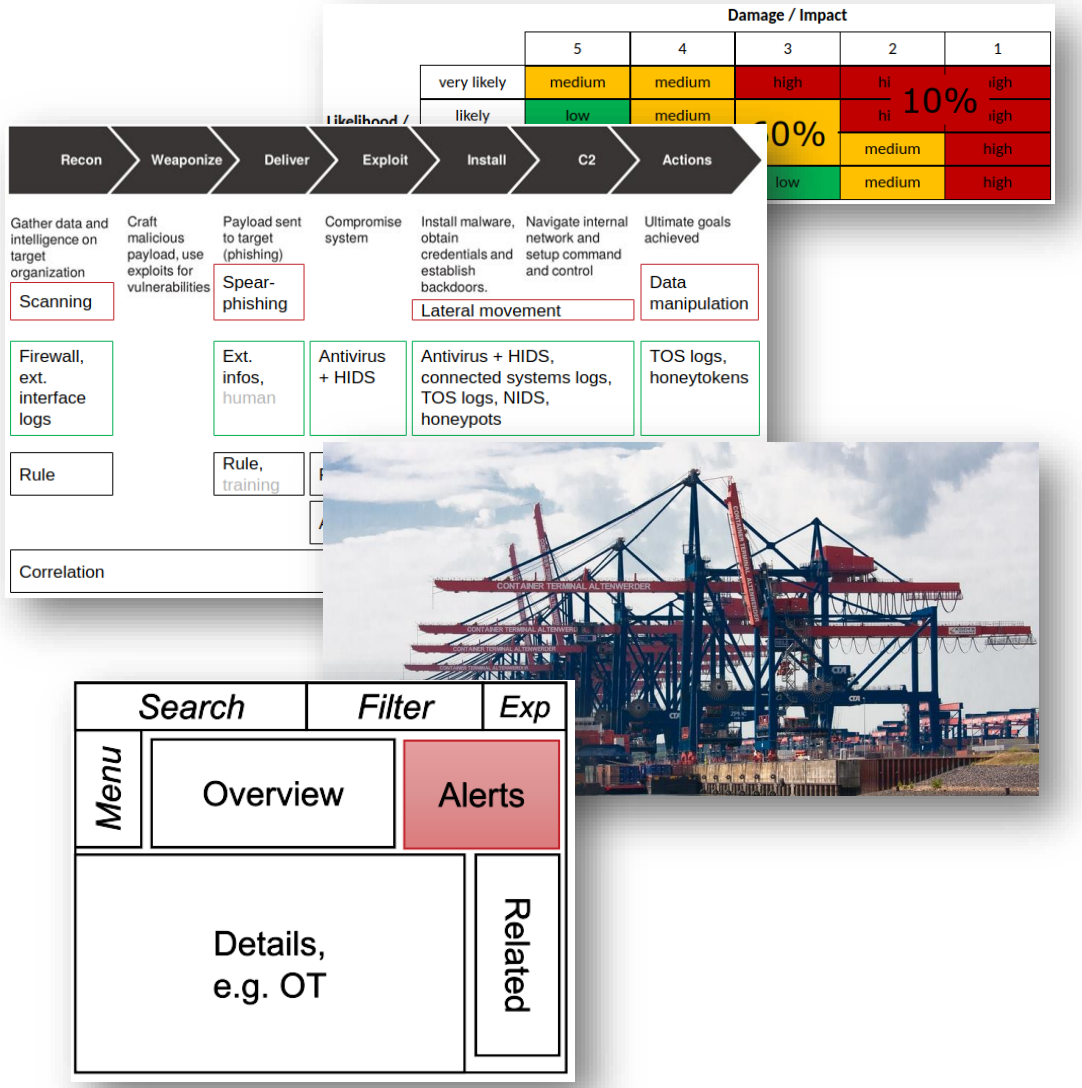


*Alan Cooper, Robert Reimann, David Cronin, and Christopher Noessel. *About face: the essentials of interaction design.* John Wiley & Sons. 2014.

- Prioritization influenced by
  - **protection needs analysis**
  - **risk scenario assessment**
  - **kill chain placement**
  - **detection source**, e.g. application logs, additional sensors
  - **attack**, e.g. data manipulation, scanning
  - **detection mechanism**, e.g. correlation, anomaly
  - **external sources**, e.g. public, private feeds
  - **human interaction**, e.g. hint, personal intuition

Summary

- Human and technical IT security awareness and contextualization
- Detection of sophisticated attacks using an appropriate combination of detection sources and mechanisms
- Goal-driven visualization embedded into the non-specialized personnel day-to-day business environment



Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Thank you for your attention. Questions or comments?

IT Security Monitoring at a Port Terminal Operator

Jens Wettlaufer
jens.wettlaufer@uni-hamburg.de

Security in Distributed Systems &
IT Security and Security Management

Computer Science Department
University of Hamburg
Germany