



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

		Damage / Impact				
		5	4	3	2	1
Likelihood / Frequency	very likely	medium	medium	high	hi	high
	likely	low	medium	60%	hi	high
	possible	low	30%	low	medium	high
	unlikely	low	low	low	medium	high

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

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.



Integration of scenarios

- e.g. terminal sabotage using malware

Gather data and intelligence on target organization

Scanning

Craft malicious payload, use exploits for vulnerabilities

Payload sent to target (phishing)

Spear-phishing

Compromise system

Install malware, obtain credentials and establish backdoors.

Lateral movement

Navigate internal network and setup command and control

Ultimate goals achieved

Data manipulation

Identification of potentially involved systems

Public websites, systems with ext. interface

E-Mail, Social Media

Client PC

Client PC, connected systems, TOS

TOS

Identification of detection sources

Firewall, ext. interface logs

Ext. infos, human

Antivirus + HIDS

Antivirus + HIDS, connected systems logs, TOS logs, NIDS, honeypots

TOS logs, honeypots

Intrusion Detection Methods

- Application-specific rule-based

- e.g. >3 login failures for one username internally, log with type 'warning'

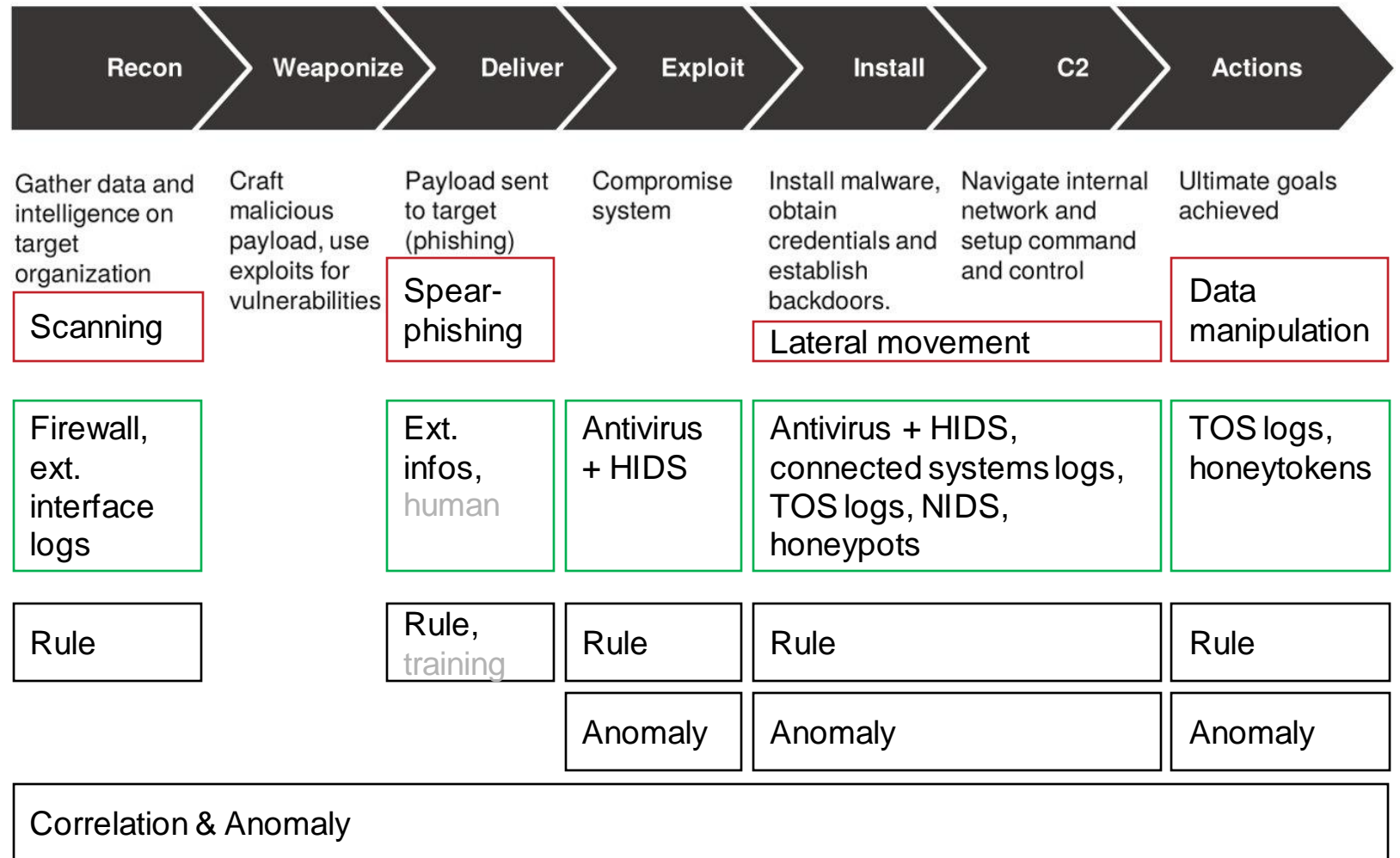
- Application-specific anomaly-based

- e.g. communication with unusual IPs/subnets

- Correlation-based across applications

- e.g. same user login failures in different systems, NIDS anomaly + honeypot

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.com/photos/eCc7FjMoR74>]



[<https://commons.wikimedia.org/wiki/index.php?curid=21424585>]

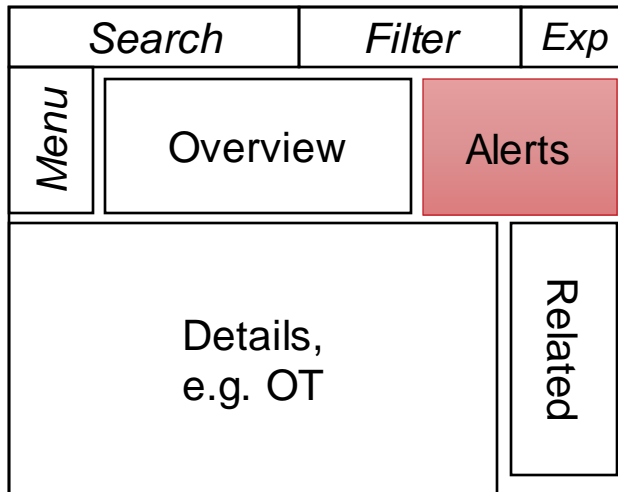


[<https://unsplash.com/photos/eCc7FjMoR74>]

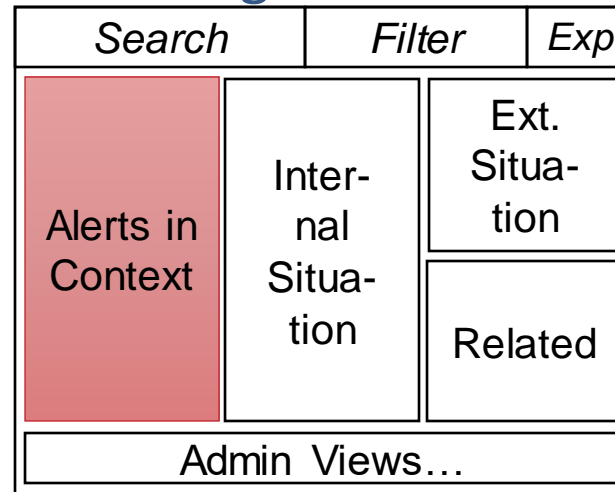
Goal-driven* Visualization for Non-specialized Personnel

- 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

		Damage / Impact				
		5	4	3	2	1
Likelihood /	very likely	medium	medium	high	hi	igh
	likely	low	medium	0%	hi	igh
					10%	
					medium	high
					low	high

Recon → **Weaponize** → **Deliver** → **Exploit** → **Install** → **C2** → **Actions**

Recon	Weaponize	Deliver	Exploit	Install	C2	Actions
Gather data and intelligence on target organization Scanning	Craft malicious payload, use exploits for vulnerabilities Spear-phishing	Payload sent to target (phishing)	Compromise system	Install malware, obtain credentials and establish backdoors. Lateral movement	Navigate internal network and setup command and control	Ultimate goals achieved Data manipulation
Firewall, ext. interface logs	Ext. infos, human	Antivirus + HIDS	Antivirus + HIDS, connected systems logs, TOS logs, NIDS, honeypots	TOS logs, honeypots		
Rule	Rule, training					
Correlation						

	Search	Filter	Exp
Menu	Overview	Alerts	
	Details, e.g. OT		Related



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