Project Management Institute Germany

infoGuard
SWISS CYBER SECURITY

SETTING UP A SECURITY OPERATIONS CENTER (SOC) / CYBER DEFENCE CENTER (CDC)

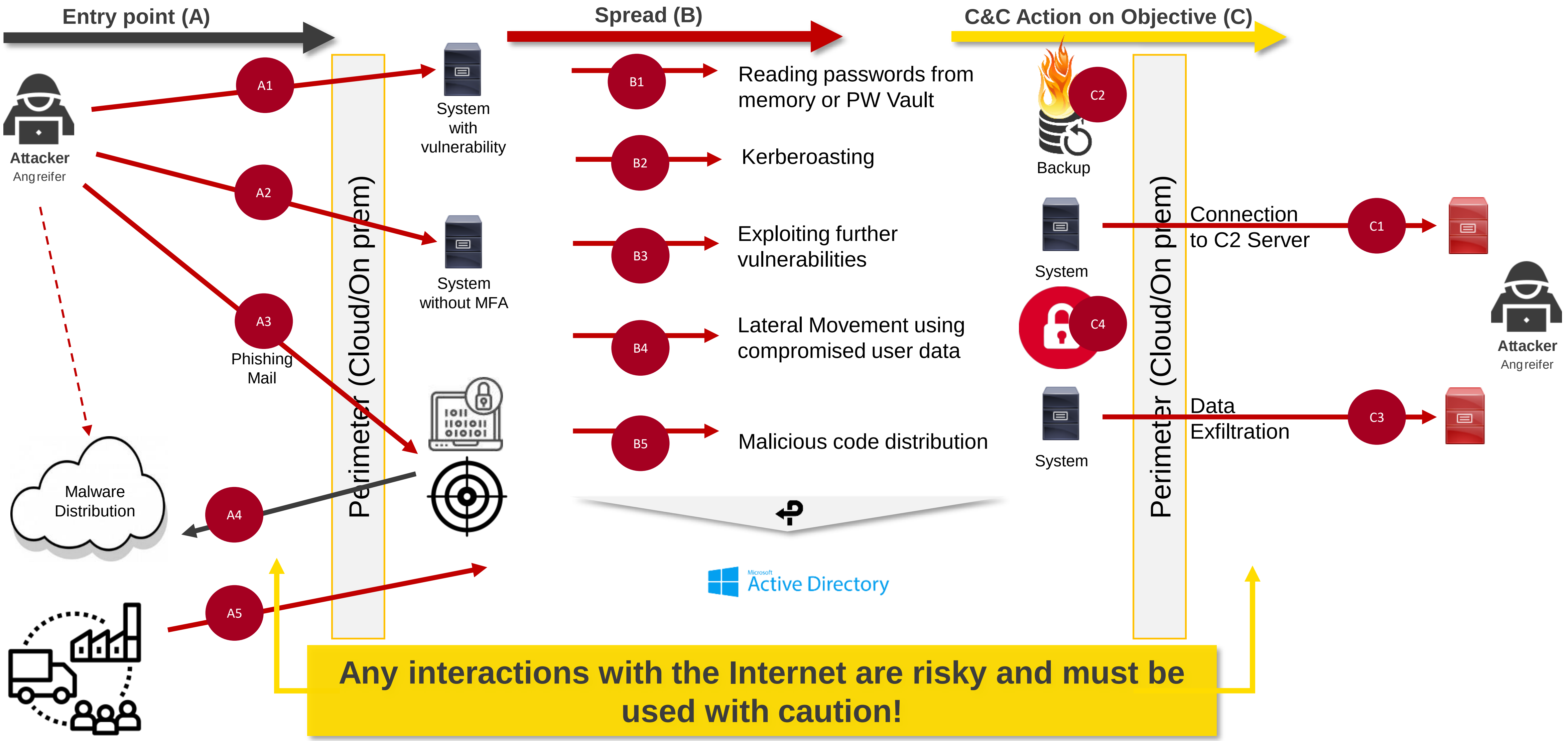
Ernesto Hartmann, Chief Cyber Defence Officer, InfoGuard AG

Some basic before we start with the project setup

InfoGuard
SWISS CYBER SECURITY

The goal of a SOC/CDC is to identify attack chains and stop them with an adequate response before any damage is occurs.

What are attack chains?
Anatomy of ransomware attacks



Entry point (A)

Spread (B)

C&C Action on Objective (C)

B1 Reading passwords from memory or PW Vault

B2 Kerberoasting

B3 Exploiting further vulnerabilities

B4 Lateral Movement using compromised user data

B5 Malicious code distribution

C1 Connection to C2 Server

C3 Data Exfiltration

Any interactions with the Internet are risky and must be used with caution!

CUSTOMER ONBOARDING

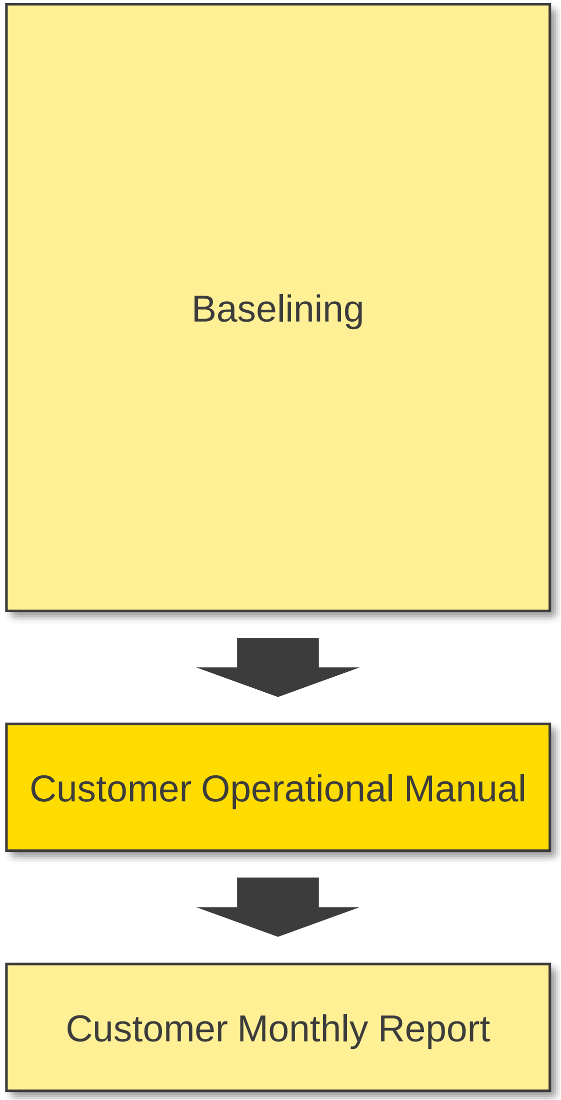
Projectplan – This is how we bring you on board!

InfoGuard
SWISS CYBER SECURITY

	Init	Realisation	Baselining	Operations
Governance Structure	• Kick off Meeting • Service Edge design • Interconnection design • Architecture • Alignment of onboarding procedure • Allocation of internal and customer resources • Modelling workshop I (Technology) • Asset & network classification • Service Edge design • Service Edge and Interconnection Architecture	• Setup Service Edge • Setup VPN • Interconnection of ticketing • Setup Backend Tenants @ InfoGuard	• Modelling workshop II (People / Process) • Setup of the Governance structure • Setup of the collaboration processes • Definition of CDC Organization • Alignment of CDC Process	• Service Reporting • Incident Triage & Analysis • Continuous optimization of event rules • Continuous improvement • Monthly Reporting • Threat analysis (On demand) • Incident Response (On demand)
EDR		• Setup Tanium Backend @ Customer • Rollout Agents 1. Pilot 2. Bulk	• Compromise Assessment • Rule tuning (thresholds and system peaks)	• Continuous Security Monitoring • On EDR UC's • Tanium Platform Management
Stream VuM Ext		• Setup Vuma Backend • Initial Discovery and Network Scan • VuM UC Onboarding	• False Positive Tuning	• Continuous Security Monitoring • On VuM UC's • Cont. Ext. Vulnerability Discovery • HandOver report to Customer
Stream SIEM	• Kick-Off QRadar & UC-Evaluation Workshop	• Implementation of QRadar • Setup • API Access to Backend	• Rule tuning (thresholds and system/network peaks) • Interconnect Dashboard sync	• Continuous Security Monitoring • On SIEM UC's • QRadar Platform Management
Stream NDR	• Kick-Off Vectra & Brain and Sensor Design Workshop	• Implementation of Vectra • Brain • Sensors	• Rule tuning (thresholds and system peaks)	• Continuous Security Monitoring • On NDR UC's • Vectra Platform Management

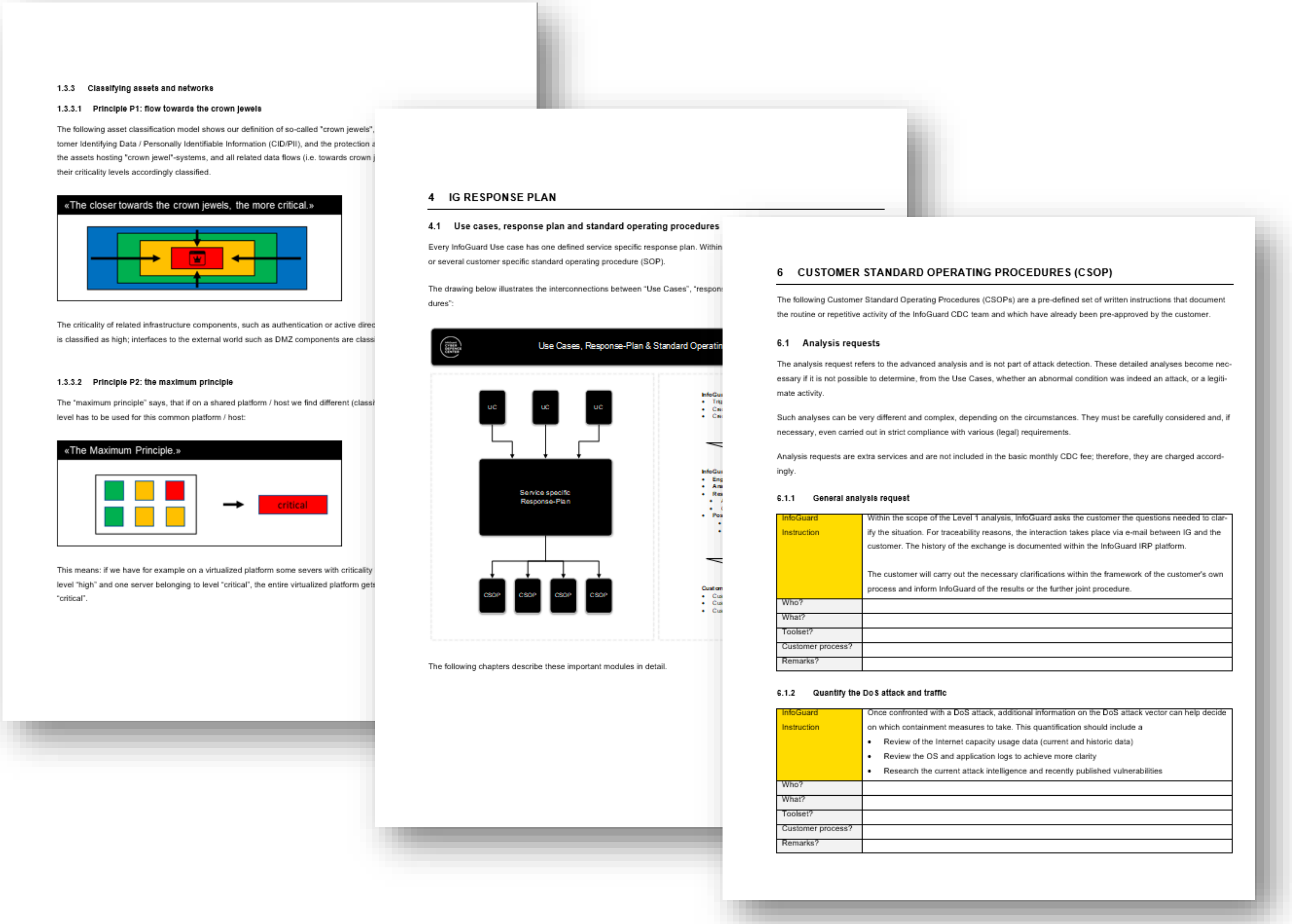
Service deliverables
Baselining -> Operational manual

InfoGuard
SWISS CYBER SECURITY


Baselining

Customer Operational Manual

Customer Monthly Report



1.3.3 Classifying assets and networks

1.3.3.1 Principle P1: flow towards the crown jewels

The following asset classification model shows our definition of so-called "crown jewels",
tomer Identifying Data / Personally Identifiable Information (CID/PII), and the protection a
the assets hosting "crown jewel"-systems, and all related data flows (i.e. towards crown j
their criticality levels accordingly classified.

«The closer towards the crown jewels, the more critical.»

The criticality of related infrastructure components, such as authentication or active direc
is classified as high; interfaces to the external world such as DMZ components are classi

1.3.3.2 Principle P2: the maximum principle

The "maximum principle" says, that if on a shared platform / host we find different (classi
level has to be used for this common platform / host:

«The Maximum Principle.»

This means: if we have for example on a virtualized platform some severs with criticality
level "high" and one server belonging to level "critical", the entire virtualized platform gets
"critical".

4 IG RESPONSE PLAN

4.1 Use cases, response plan and standard operating procedures

Every InfoGuard Use case has one defined service specific response plan. Within
or several customer specific standard operating procedure (SOP).

The drawing below illustrates the interconnections between "Use Cases", "respon
dures":

Use Cases, Response-Plan & Standard Operatin

The following chapters describe these important modules in detail.

6 CUSTOMER STANDARD OPERATING PROCEDURES (CSOP)

The following Customer Standard Operating Procedures (CSOPs) are a pre-defined set of written instructions that document the routine or repetitive activity of the InfoGuard CDC team and which have already been pre-approved by the customer.

6.1 Analysis requests

The analysis request refers to the advanced analysis and is not part of attack detection. These detailed analyses become necessary if it is not possible to determine, from the Use Cases, whether an abnormal condition was indeed an attack, or a legitimate activity.

Such analyses can be very different and complex, depending on the circumstances. They must be carefully considered and, if necessary, even carried out in strict compliance with various (legal) requirements.

Analysis requests are extra services and are not included in the basic monthly CDC fee; therefore, they are charged accordingly.

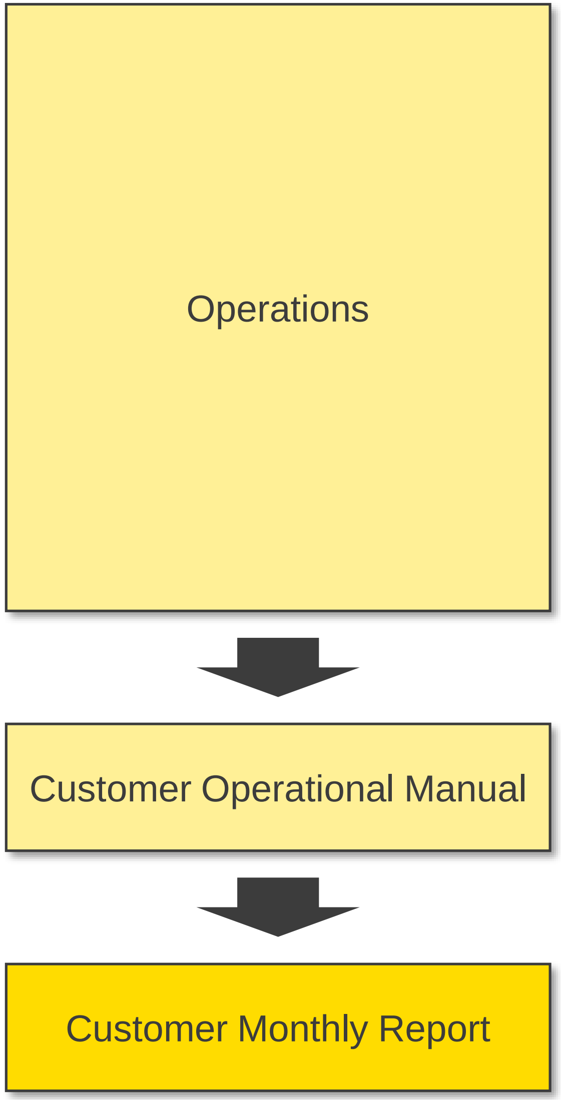
6.1.1 General analysis request

InfoGuard Instruction	Within the scope of the Level 1 analysis, InfoGuard asks the customer the questions needed to clarify the situation. For traceability reasons, the interaction takes place via e-mail between IG and the customer. The history of the exchange is documented within the InfoGuard IRP platform. The customer will carry out the necessary clarifications within the framework of the customer's own process and inform InfoGuard of the results or the further joint procedure.
Who?	
What?	
Toolset?	
Customer process?	
Remarks?	

6.1.2 Quantify the DoS attack and traffic

InfoGuard Instruction	Once confronted with a DoS attack, additional information on the DoS attack vector can help decide on which containment measures to take. This quantification should include a • Review of the Internet capacity usage data (current and historic data) • Review the OS and application logs to achieve more clarity • Research the current attack intelligence and recently published vulnerabilities
Who?	
What?	
Toolset?	
Customer process?	
Remarks?	

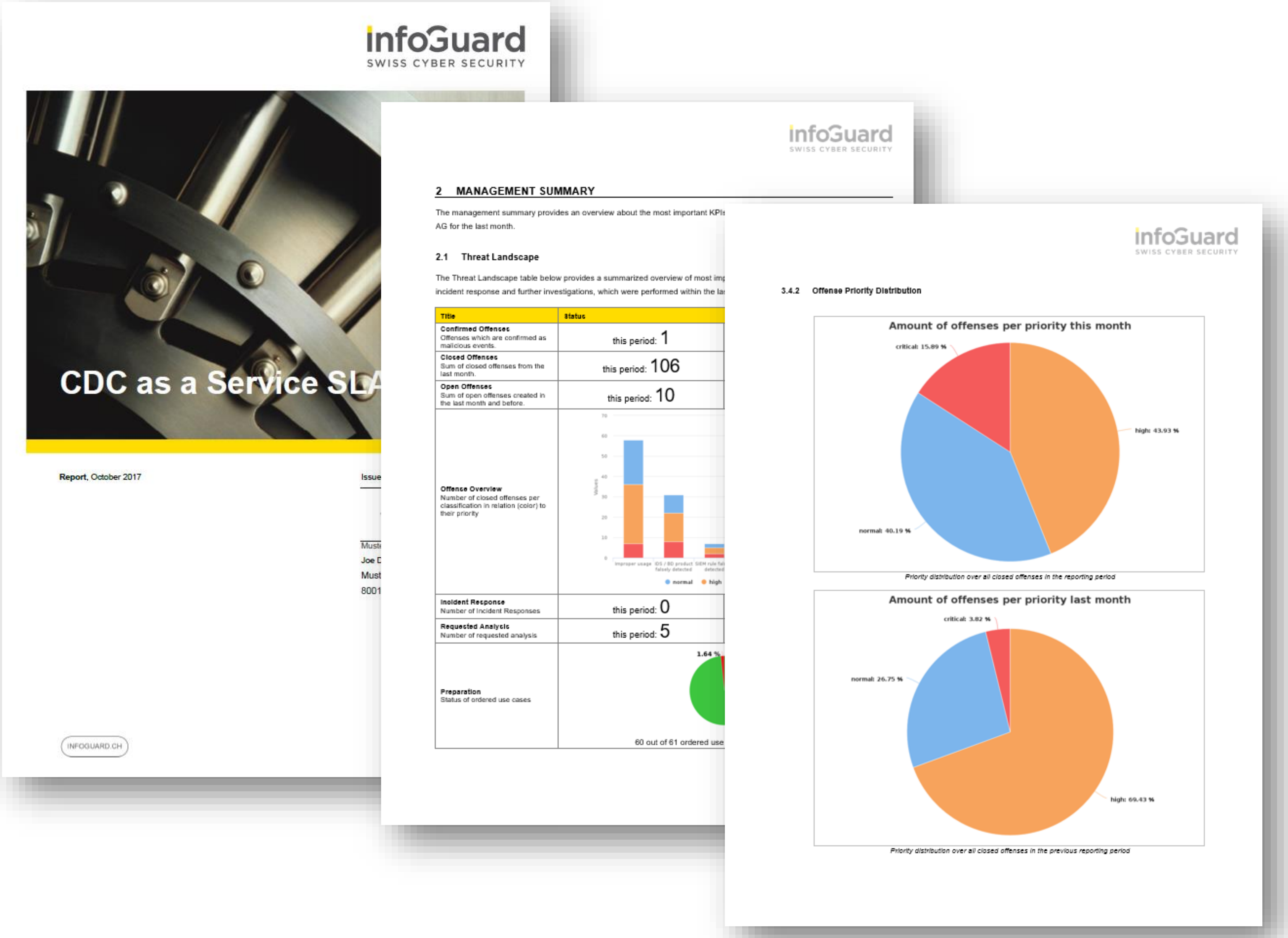
Service deliverables
Operations -> Monthly report



Operations

Customer Operational Manual

Customer Monthly Report



CDC as a Service SLA

Report, October 2017

Issue

Must
Joe D
Must
8001

INFOGUARD.CH

2 MANAGEMENT SUMMARY

The management summary provides an overview about the most important KPIs AG for the last month.

2.1 Threat Landscape

The Threat Landscape table below provides a summarized overview of most im incident response and further investigations, which were performed within the la

Title	Status
Confirmed Offenses Offenses which are confirmed as malicious events.	this period: 1
Closed Offenses Sum of closed offenses from the last month.	this period: 106
Open Offenses Sum of open offenses created in the last month and before.	this period: 10
Offence Overview Number of closed offenses per classification in relation (color) to their priority	
Incident Response Number of Incident Responses	this period: 0
Requested Analysis Number of requested analysis	this period: 5
Preparation Status of ordered use cases	60 out of 61 ordered use

3.4.2 Offense Priority Distribution

Priority distribution over all closed offenses in the reporting period

Priority distribution over all closed offenses in the previous reporting period

Do´s, Don´ts and pitfalls

InfoGuard
SWISS CYBER SECURITY

A Security Information and Event Management (SIEM) centric approach does not work! We need to have the ability to act quick in case of an attack.

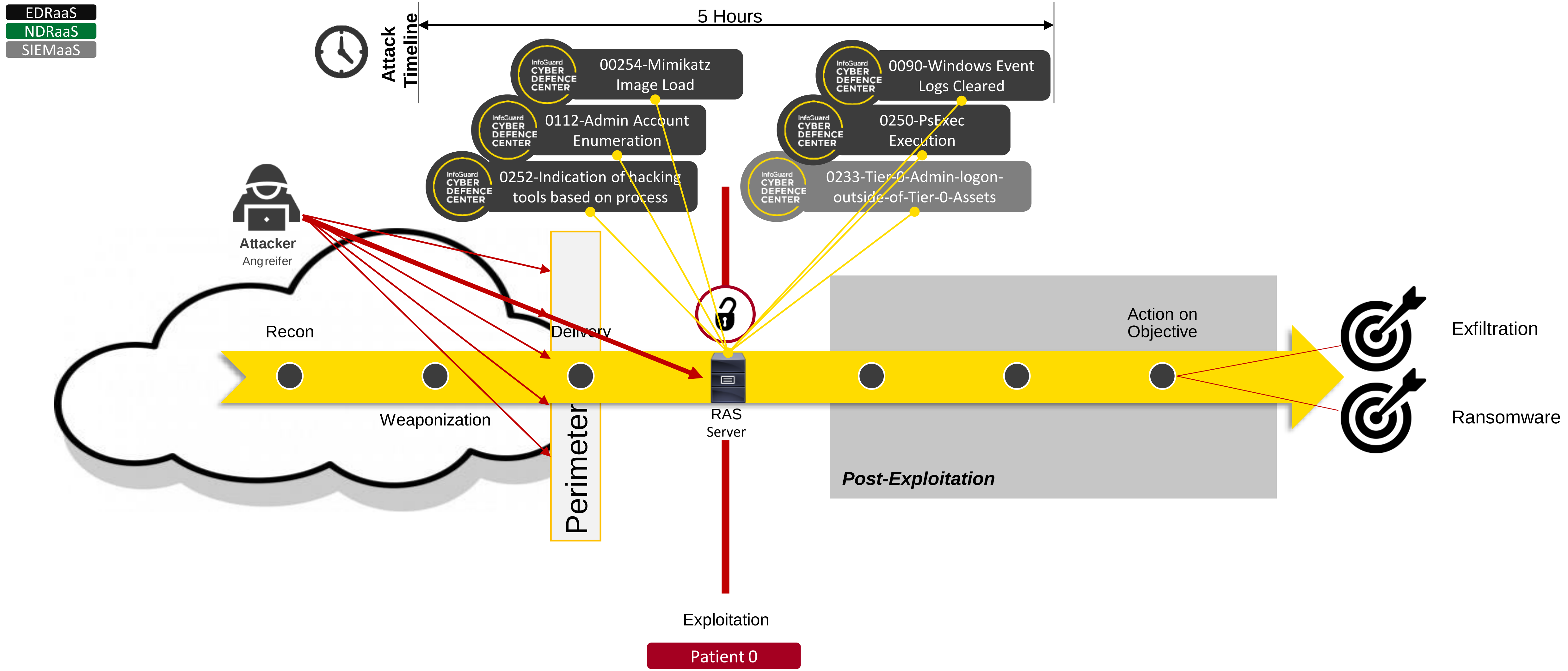
Cyber Defence Capabilities

InfoGuard CYBER DEFENCE CENTER	CDC CAPABILITIES					
CDC SERVICE	**THREAT PREVENTION**	**THREAT DETECTION**	**BASIC VERIFICATION**	**ADVANCED VERIFICATION**	**CONTAINMENT**	**ERADICATION**
IR as a Service		X	X	X	X	X
TH as a Service		X	X	X	X	
EDR as a Service	**X***	**X**	**X**	**X**	**X**	**X**
CDR & NDR as a Service		X	X			
SIEM as a Service		X	X			

- **Threat Prevention** – the capability to prevent threats
- **Threat Detection** – the capability to detect threats
- **Basic Verification** – verification of threat alerts based on pre-collected data
- **Advanced Verification** – the capability to collect further data for threat analysis
- **Containment** – the capability to execute remediation actions such as client isolations
- **Eradication** – the capability to clean infected systems

* Only with an EPP/EDR combined Agent

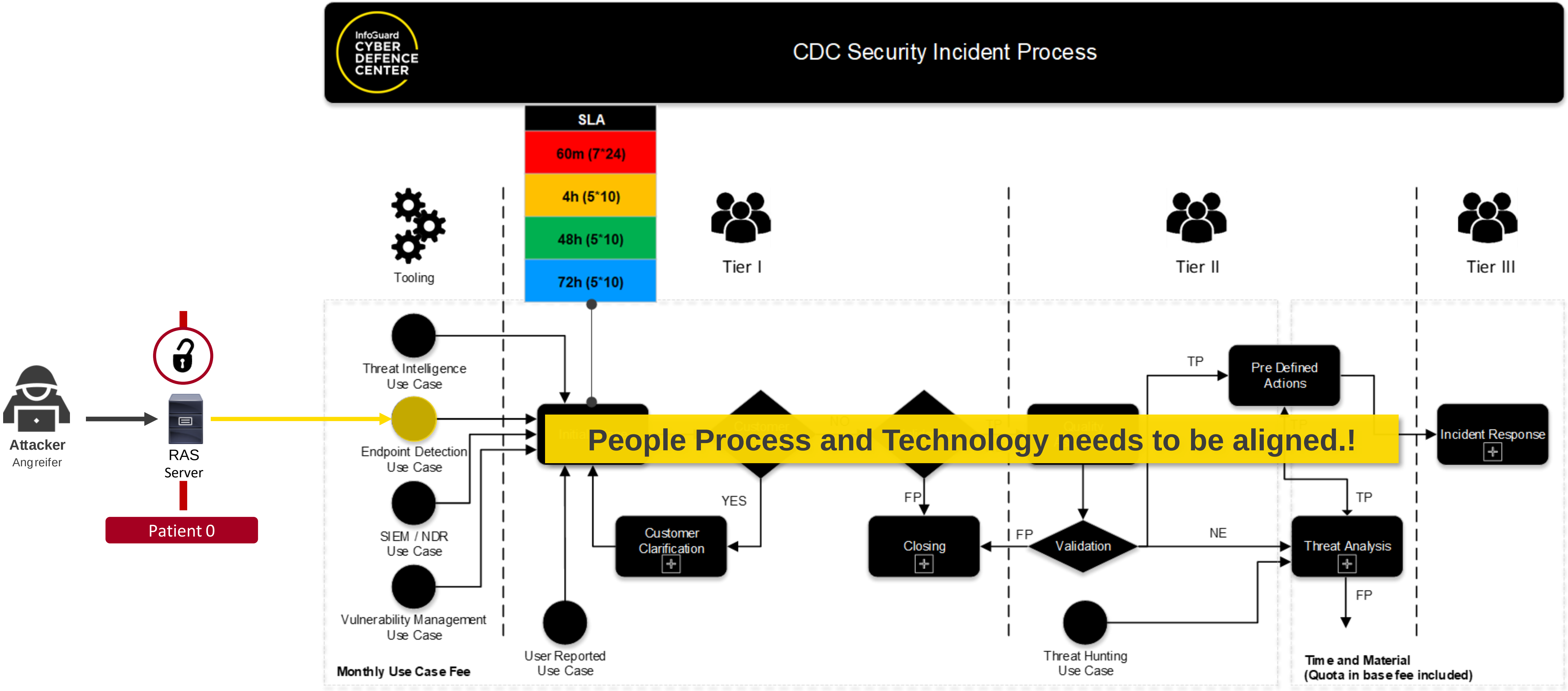
The attackers land on an operating system after the initial intrusion!



EDRaaS
NDRaaS
SIEMaaS
Attack Timeline
5 Hours
00254-Mimikatz Image Load
0112-Admin Account Enumeration
0252-Indication of hacking tools based on process
0090-Windows Event Logs Cleared
0250-PsExec Execution
0233-Tier-0-Admin-logon-outside-of-Tier-0-Assets
InfoGuard CYBER DEFENCE CENTER
Attacker
Angreifer
Recon
Weaponization
Delivery
Perimeter
RAS Server
Exploitation
Patient 0
Action on Objective
Post-Exploitation
Exfiltration
Ransomware

The attack chain must be interrupted as quickly as possible!

InfoGuard
SWISS CYBER SECURITY



InfoGuard CYBER DEFENCE CENTER

CDC Security Incident Process

SLA
60m (7*24)
4h (5*10)
48h (5*10)
72h (5*10)

Tooling

Tier I

Tier II

Tier III

Attacker
Angreifer

RAS
Server

Patient 0

Threat Intelligence
Use Case

Endpoint Detection
Use Case

SIEM / NDR
Use Case

Vulnerability Management
Use Case

Monthly Use Case Fee

User Reported
Use Case

Customer
Clarification

YES

FP

Closing

FP

Validation

NE

TP

Pre Defined
Actions

Incident Response

TP

Threat Analysis

FP

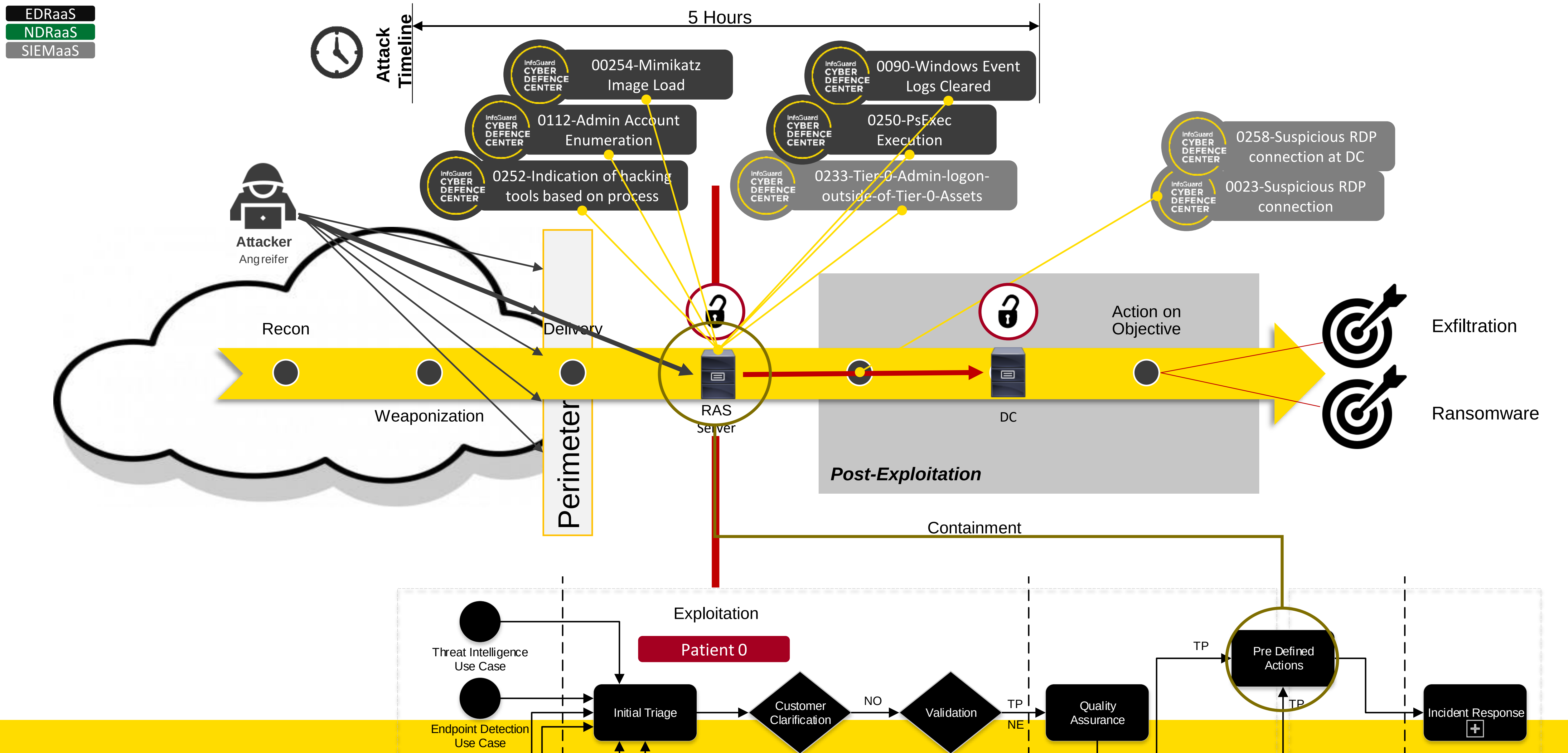
Threat Hunting
Use Case

Time and Material
(Quota in base fee included)

People Process and Technology needs to be aligned.!

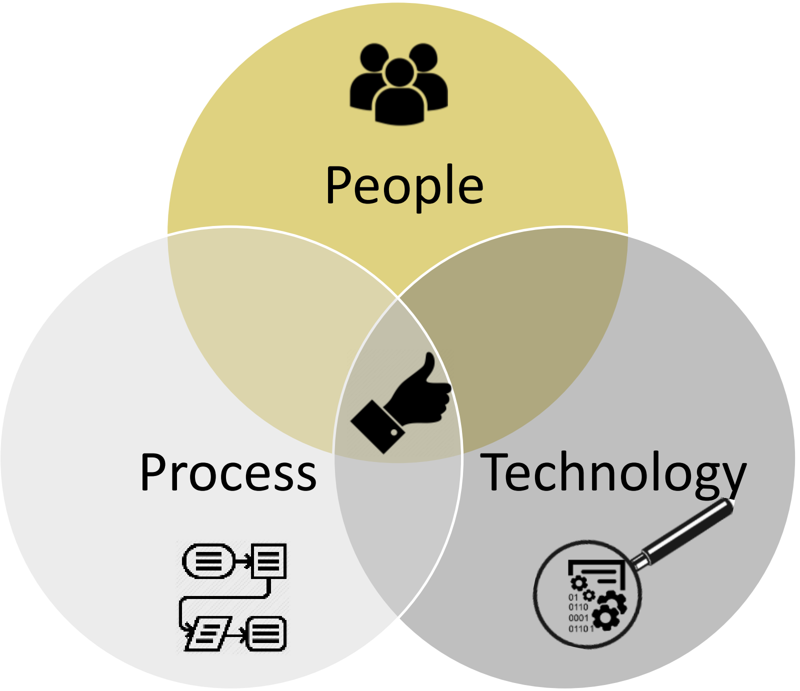
If the attack chain is not interrupted, the attackers move laterally.

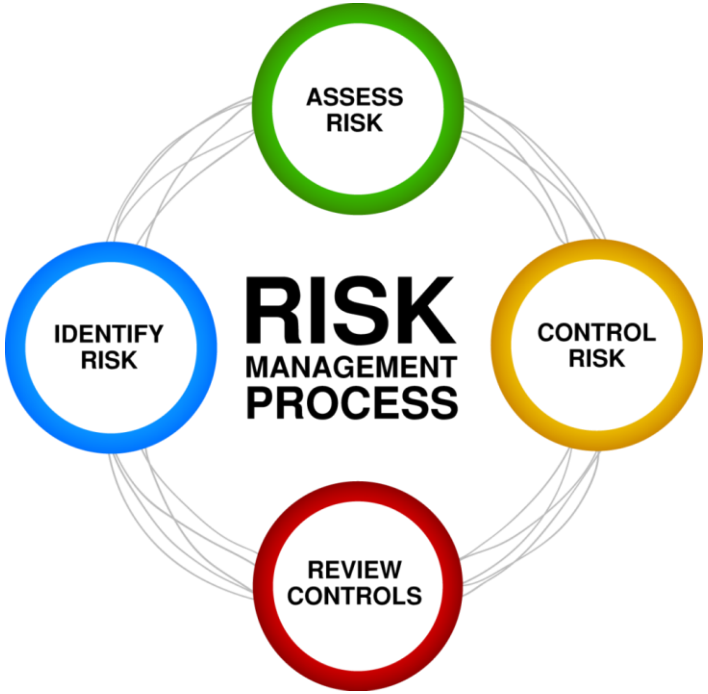
InfoGuard
SWISS CYBER SECURITY



EDRaaS
NDRaaS
SIEMaaS
Attack Timeline
5 Hours
InfoGuard CYBER DEFENCE CENTER
00254-Mimikatz Image Load
0112-Admin Account Enumeration
0252-Indication of hacking tools based on process
0090-Windows Event Logs Cleared
0250-PsExec Execution
0233-Tier-0-Admin-logon-outside-of-Tier-0-Assets
0258-Suspicious RDP connection at DC
0023-Suspicious RDP connection
Attacker
Angreifer
Recon
Weaponization
Delivery
Perimeter
RAS Server
DC
Action on Objective
Post-Exploitation
Exfiltration
Ransomware
Containment
Exploitation
Patient 0
Threat Intelligence Use Case
Endpoint Detection Use Case
Initial Triage
Customer Clarification
NO
Validation
TP
NE
Quality Assurance
TP
Pre Defined Actions
TP
Incident Response

Do´s, Don´ts and pitfalls
A few words in conclusion





A Cyber Defence Center can detect and prevent cyber-attacks.

InfoGuard
SWISS CYBER SECURITY

Ernesto Hartmann
Chief Cyber Defence Officer

ernesto.hartmann@infoguard.ch

https://www.linkedin.com/in/ernesto
hartmann-343908100/

InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz

Telefon +41 41 749 19 00