THE LEADER IN SECURITY OPERATIONS

SETUP AND OPERATING A SECURITY OPERATIONS CENTER
Dos and Don’ts and Best Practice

Dr. Sebastian Schmerl

Halle 7, Stand: 7-715

Agenda

01 Current Cyber Threats & Challenges

02 Building Blocks for Cyber Defense

03 State of the art Security Protection

04 How to measure and improve Cyber Security

05 Typical inhouse SOC setup fails

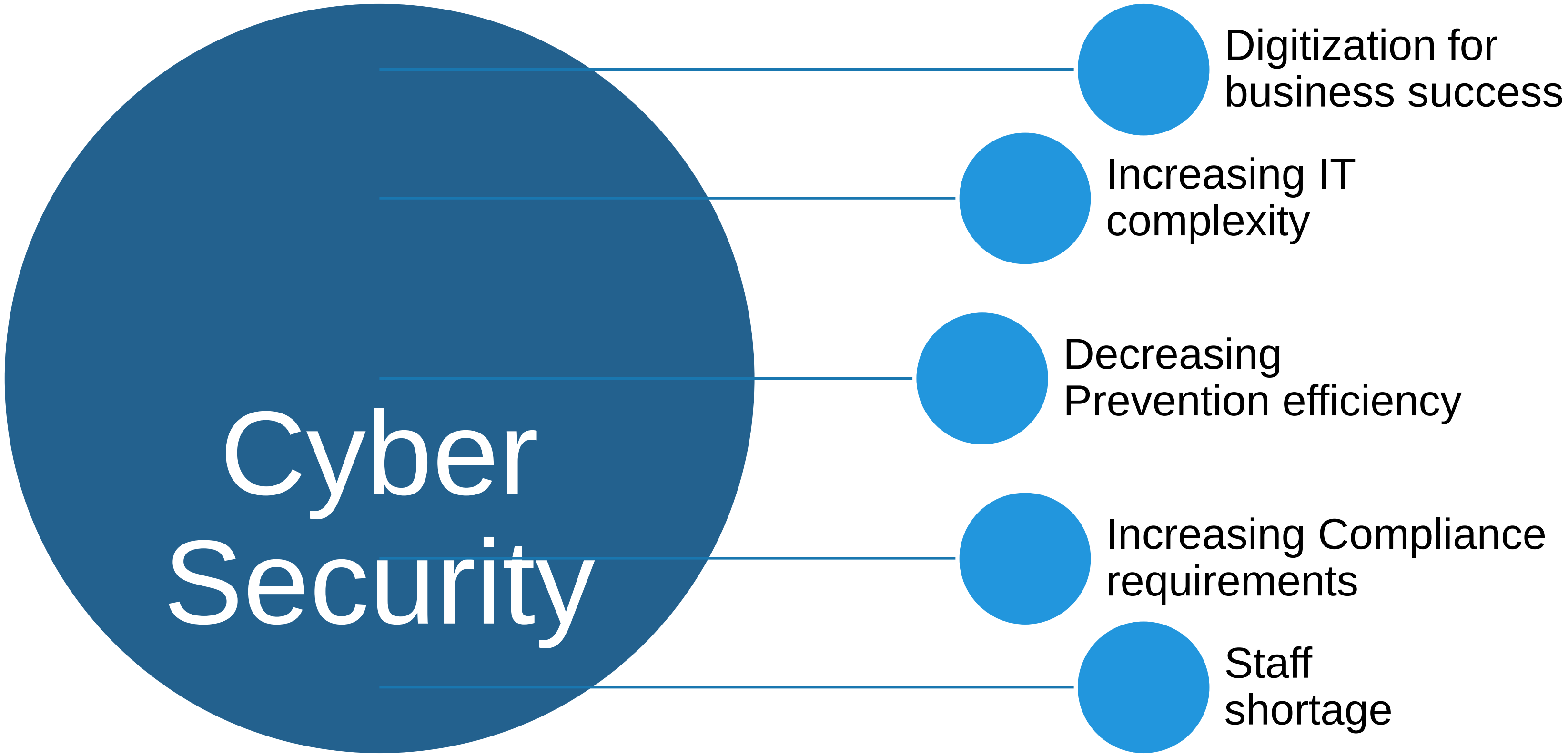
01

Current Challenges & Threats

in Cyber Security

Drivers in Security & Challenges

Security is often considered as a “just” technology follower…


Cyber Security
Digitization for business success
Increasing IT complexity
Decreasing Prevention efficiency
Increasing Compliance requirements
Staff shortage

> “Cyber security prevention products lacking efficiency

> “cybersecurity industry has an effectiveness problem

> “There is no 100% prevention, assume breach

> “Security relays on humans

Current Cyber Security Threats

Most of them are very hard to prevent, which makes them so successful

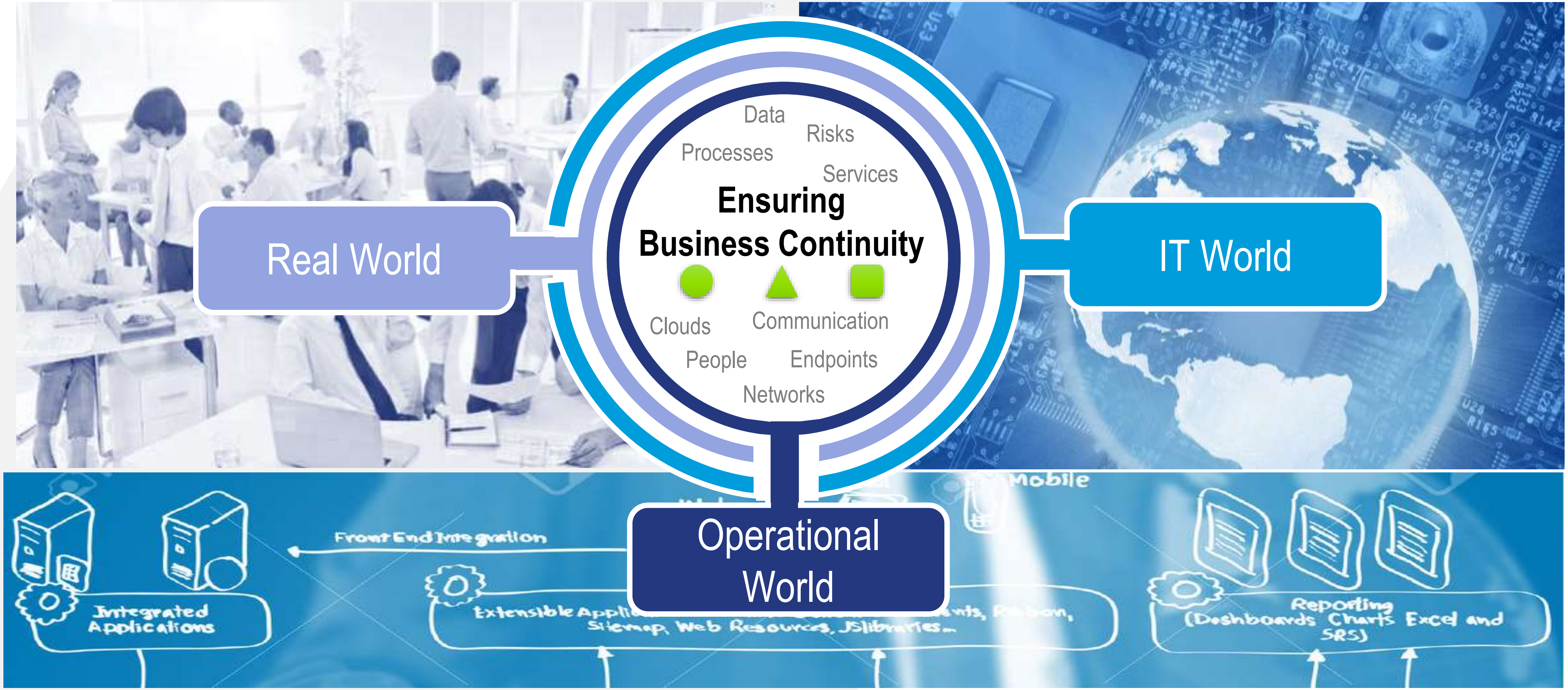
- Phishing likes COVID-19
- Remote Work Exploitation
- Business Email Compromise
- Ransomware Attacks and Double Extortion
- Leaked Passwords
- ~~Zero~~-day exploits
- Deepfakes & Identity Theft
- Cloud Breaches / Takeovers

… to be continued

02 Building Blocks for Cyber Defense

Cyber-Defense @ Arctic Wolf

THREE WORLDS, THREE PERSPECTIVES, BUT ONE GOAL



Real World

IT World

Operational World

Data

Risks

Processes

Services

Ensuring Business Continuity

Clouds

Communication

People

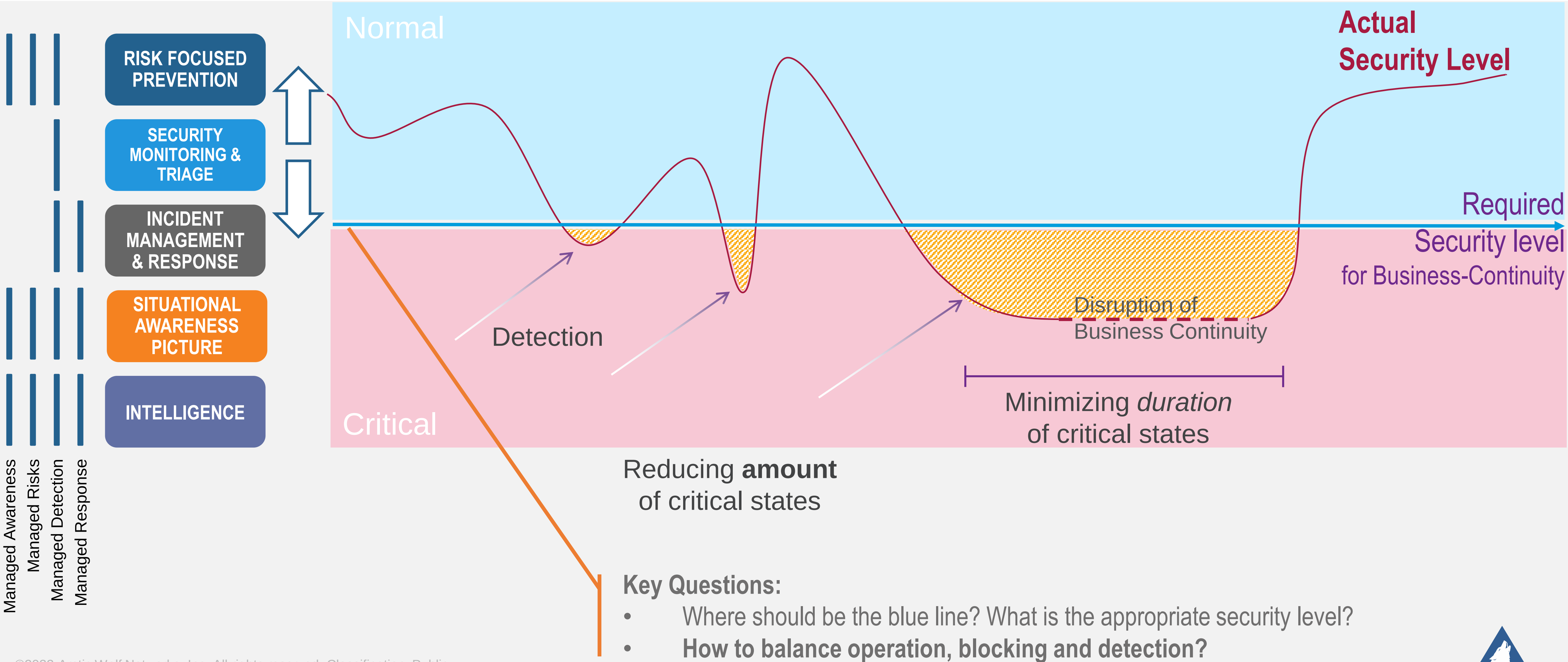
Endpoints

Networks

Mobile
Front End Integration
Integrated Applications
Extensible Appli... Sitemap, Web Resources, JSlibraries
Reporting (Dashboards Charts Excel and SRS)

General Cyber Defence Strategy

AWARENESS, PROTECTION, DETECTION, REACTION, RESILIENCE


Managed Awareness
Managed Risks
Managed Detection
Managed Response
RISK FOCUSED PREVENTION
SECURITY MONITORING & TRIAGE
INCIDENT MANAGEMENT & RESPONSE
SITUATIONAL AWARENESS PICTURE
INTELLIGENCE
Normal
Critical
Actual Security Level
Required Security level for Business-Continuity
Detection
Disruption of Business Continuity
Minimizing *duration* of critical states
Reducing **amount** of critical states

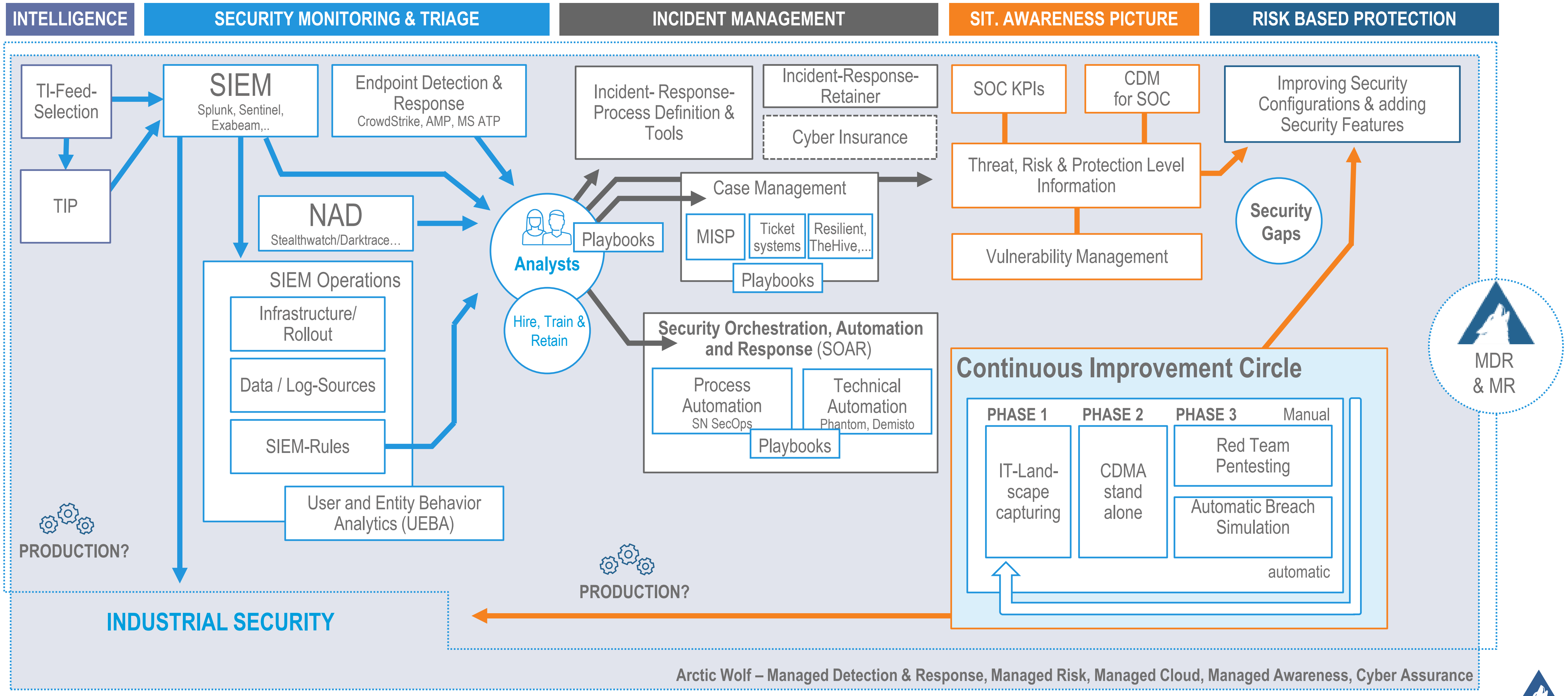
Key Questions:

- Where should be the blue line? What is the appropriate security level?
- **How to balance operation, blocking and detection?**

03 State of the art Security Protection

Cyber Protection – Building Blocks you need to cover

STATE-OF-THE-ART CYBER DEFENCE



INTELLIGENCE

SECURITY MONITORING & TRIAGE

INCIDENT MANAGEMENT

SIT. AWARENESS PICTURE

RISK BASED PROTECTION

TI-Feed-Selection

TIP

SIEM
Splunk, Sentinel, Exabeam,..

Endpoint Detection & Response
CrowdStrike, AMP, MS ATP

NAD
Stealthwatch/Darktrace…

SIEM Operations

Infrastructure/ Rollout

Data / Log-Sources

SIEM-Rules

User and Entity Behavior Analytics (UEBA)

Analysts

Playbooks

Hire, Train & Retain

Incident- Response-Process Definition & Tools

Incident-Response-Retainer

Cyber Insurance

Case Management

MISP

Ticket systems

Resilient, TheHive,...

Playbooks

Security Orchestration, Automation and Response (SOAR)

Process Automation
SN SecOps

Technical Automation
Phantom, Demisto

Playbooks

SOC KPIs

CDM for SOC

Threat, Risk & Protection Level Information

Vulnerability Management

Improving Security Configurations & adding Security Features

Security Gaps

Continuous Improvement Circle

PHASE 1

PHASE 2

PHASE 3

Manual

IT-Land-scape capturing

CDMA stand alone

Red Team Pentesting

Automatic Breach Simulation

automatic

MDR & MR

PRODUCTION?

PRODUCTION?

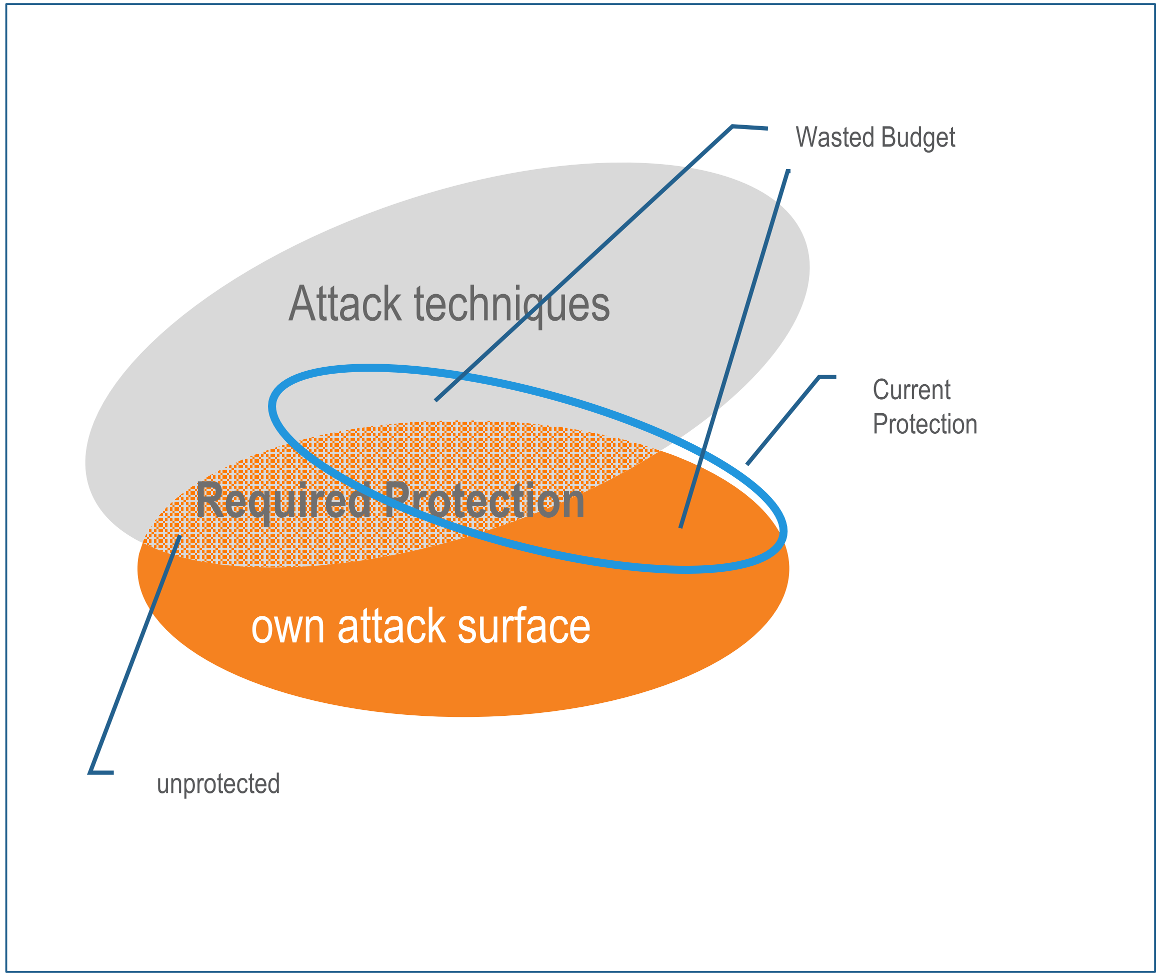
INDUSTRIAL SECURITY

Arctic Wolf – Managed Detection & Response, Managed Risk, Managed Cloud, Managed Awareness, Cyber Assurance

04 How to measure and improve your Cyber Security

Cyber Defense Maturity – Security Journey

Adapting security to the required scope

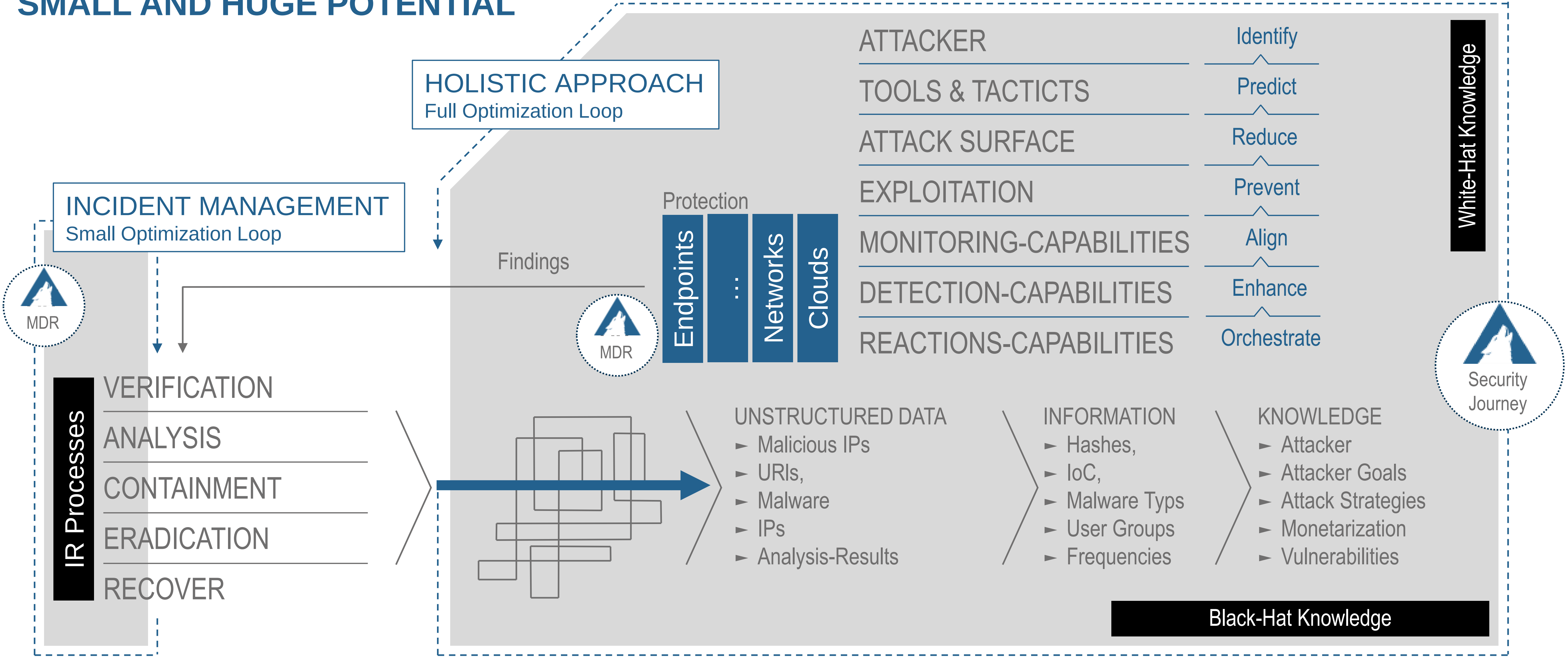


- **If you know**
  - the threats,
  - the attacker,
  - used techniques and
  - your attack surface.

→ adjustment of the cyber protection

CYBER DEFENSE – TWO OPTIMIZATION LOOPS

SMALL AND HUGE POTENTIAL



HOLISTIC APPROACH
Full Optimization Loop

INCIDENT MANAGEMENT
Small Optimization Loop

MDR

IR Processes

- VERIFICATION
- ANALYSIS
- CONTAINMENT
- ERADICATION
- RECOVER

Findings

MDR

Protection

Endpoints | … | Networks | Clouds

ATTACKER	Identify
TOOLS & TACTICTS	Predict
ATTACK SURFACE	Reduce
EXPLOITATION	Prevent
MONITORING-CAPABILITIES	Align
DETECTION-CAPABILITIES	Enhance
REACTIONS-CAPABILITIES	Orchestrate

White-Hat Knowledge

Security Journey

UNSTRUCTURED DATA
- Malicious IPs
- URIs,
- Malware
- IPs
- Analysis-Results

INFORMATION
- Hashes,
- IoC,
- Malware Typs
- User Groups
- Frequencies

KNOWLEDGE
- Attacker
- Attacker Goals
- Attack Strategies
- Monetarization
- Vulnerabilities

Black-Hat Knowledge

05 Typical inhouse SOC setup fails

Stop fiddling and go for a professional service

Typical Shortfalls

1. **Fail to hire & train and retain security analysts**
2. **SOC operation limited Monday to Friday 8am-5pm**
3. **Missing authority and advisory power of the SOC**
4. **Underestimate to integrate the SOC solutions into an efficient SOC stack & processes**
    - Technology integrations
    - Process integrations
5. **Underestimate the effort to fine tune detections capabilities**
    - getting lost in detail
    - Basic monitoring vs. 100% coverage for crown jewels
6. **Lack Threat Intelligence Information and threat sharing**
7. **Incident focused work only, without follow-up and proactive security improvements**
8. **Concentration on point-security-solutions and belief in security vendor marketing**

...

999. Belief that Machine Learning will solve above challenges

Thank You

SECURITY IS N
IT IS A NECE

ARCTIC WOLF: *IT'S TIME TO END CYBER RISK*

Halle 7, Stand: 7-715