basefarm

# Pa$sw0rd1

How to build & maintain a resilient & agile cyber security structure in the age of international turmoil

31.03.22

basefarm

# TALKING PLAN

- Who am I?
- Current Cyber Threat Landscape
- Cyber vs Physical security
- The role of a CyberSOC
- Basefarm / Orange Cyberdefense partnership

basefarm

# WHO AM I ?

- Age 57, engaged to Brit, father of two, worked for Basefarm since 2005
- Claim to fame: Made all the TV-graphics for the Lillehammer Olympics in 94
- Also worked with transport security services, building Gardermobanen and establishing the GSM-R ops center for the Norwegian railways

**ESTEN HOEL**
SVP Governance, Risk & Compliance

**BASEFARM** | Nydalen Allé 37a | 0484 Oslo | Norway
Phone: +47 4000 4100 | Mobile: +47 951 76 422
esten.hoel@basefarm.com | www.basefarm.com

Blog | Twitter | Facebook | LinkedIn

basefarm

# WHO AM I ?

- Age 57, engaged to Brit, father of two, worked for Basefarm since 2005
- Claim to fame: Made all the TV-graphics for the Lillehammer Olympics in 94
- Also worked with transport security services, building Gardermobanen and establishing the GSM-R ops center for the Norwegian railways
- Enjoy: football, biking, geocaching and golf (sometimes)

basefarm

# WHO AM I ?

- Age 57, engaged to Brit, father of two, worked for Basefarm since 2005
- Claim to fame: Made all the TV-graphics for the Lillehammer Olympics in 94
- Also worked with transport security services, building Gardermobanen and establishing the GSM-R ops center for the Norwegian railways
- Enjoy: football, biking, geocaching and golf (sometimes)
- Don’t enjoy: speaking in front of audiences…

basefarm

# WHO AM I ?

- Age 57, engaged to Brit, father of two, worked for Basefarm since 2005
- Claim to fame: Made all the TV-graphics for the Lillehammer Olympics in 94
- Also worked with transport security services, building Gardermobanen and establishing the GSM-R ops center for the Norwegian railways
- Enjoy: football, biking, geocaching and golf (sometimes)
- Don’t enjoy: speaking in front of audiences… And golf (most of the time)

basefarm

Orange Cyberdefense

# CURRENT CYBER THREAT LANDSCAPE

- Several cyber-attacks toward Ukraine targets has been observed since early January, and hacktivist groups have since the war started tried to hit Russian targets
- Some increased activity in the Nordics/Western Europe, but no large-scale «cyberwar» so far
- Businesses with direct ties to Ukraine and Russia need to be extra vigilant
- All businesses should monitor the situation continously and adapt to the situation
- Prepare and test incident and emergency response capabilities
- If you have a well tested response to the ransomware threat, you are well positioned

basefarm

Orange Cyberdefense

# CYBER THREAT LEVEL

## Threat level

Current

Unaware

Aware

**Alert**

Alarm

Engage

Cooper color system.

## Threat actor

Russia deemed primary aggressor

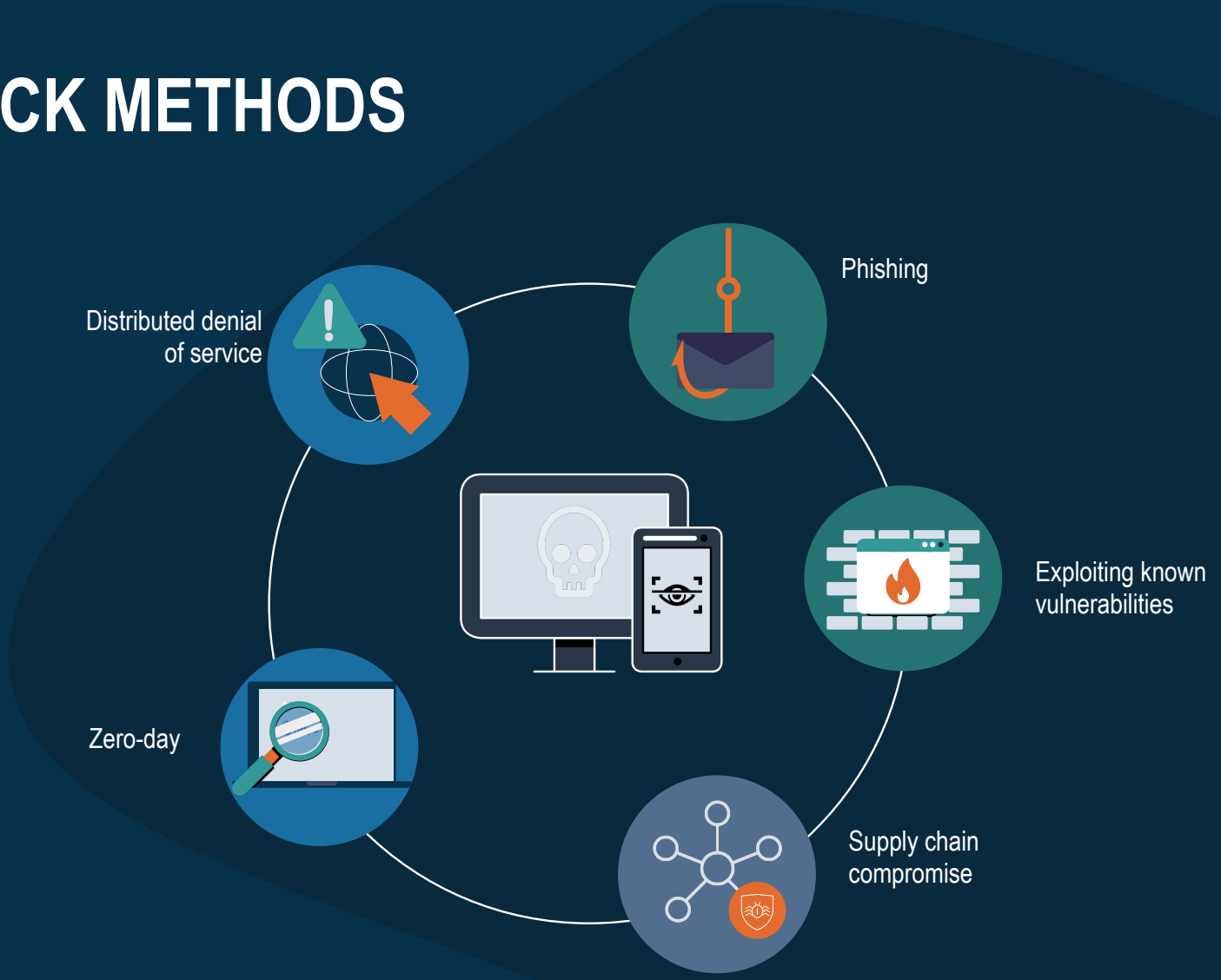
## Potential targets

- Ukrainian **government institutions**
- **Defense & military** institutions, including manufacturers
- **Telecom** sector and internet traffic
- European **media**
- U.S and European **industries invested** in Ukraine
- U.S, European and other governments **allied** with either party or imposing sanction.

basefarm

Orange Cyberdefense

# CYBER ATTACK METHODS



# RECOMMENDATIONS

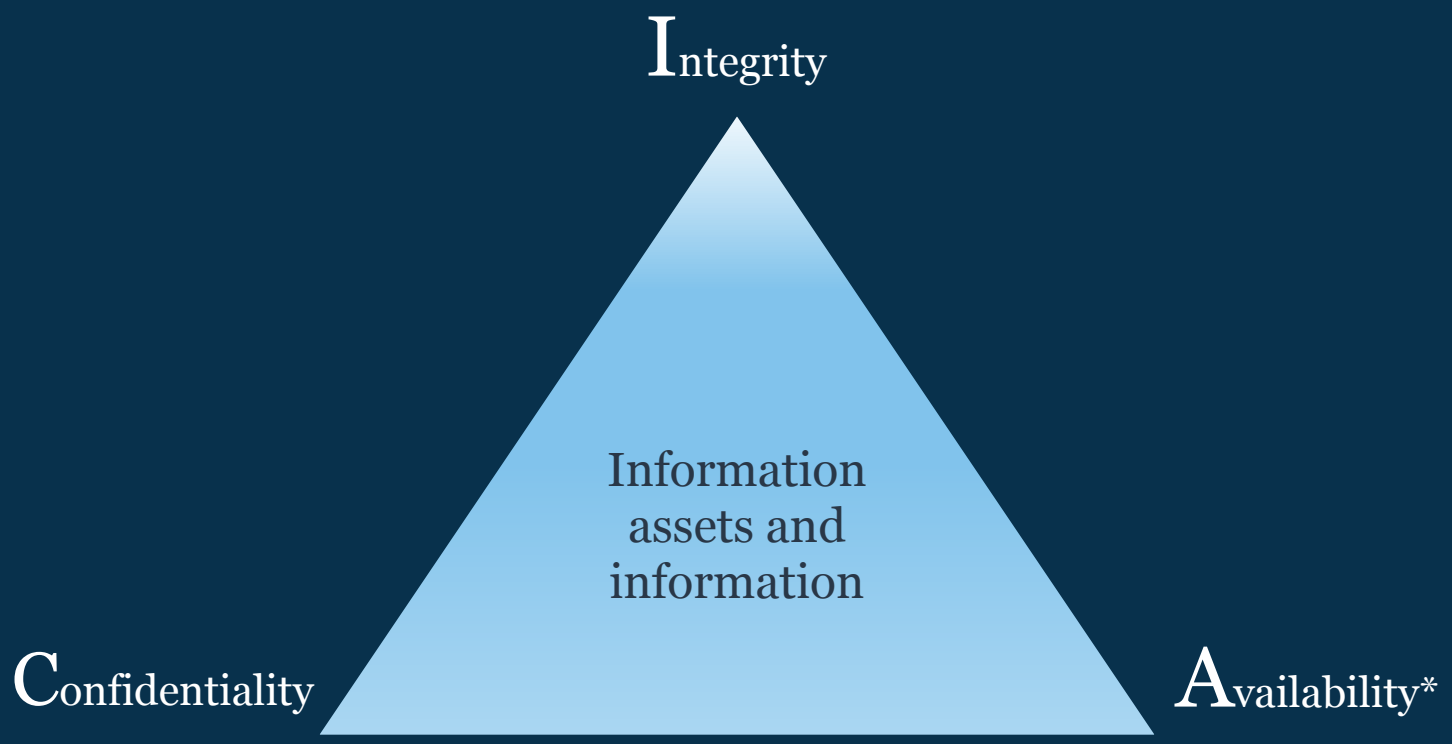
**Our primary recommendation include:**

1) **Emergency-and Incident Response**, with trained people to execute it
2) **Map your stakeholders** to understand your risk
3) Understand your **current state** and ensure your **operational security functions** are effective (e.g., Backup and recovery and Vulnerability- and Patch Mgmt.)

basefarm

# CYBER VS PHYSICAL SECURITY

First; Cybersecurity is all about protecting the CIA Triad:




*
Protection against intended actions.

basefarm

# CYBER VS PHYSICAL SECURITY

Path of least resistance
(cyber criminals are lazy too)

basefarm

# CYBER VS PHYSICAL SECURITY

Path of least resistance
(cyber criminals are lazy too)

basefarm

# CYBER VS PHYSICAL SECURITY

How physical threat vectors can compromise cyber security:

- An infected USB drive is planted in a parking lot, lobby etc., which an employee picks up and loads onto the network.
- An attacker breaks into a server room and installs rogue devices that capture confidential data.
- The internet drop line is accessible from outside of the building, allowing an attacker to intercept data or cut the line completely.
- An attacker pretends to be an employee and counts on a real employee's courtesy to hold the door for him as they enter together.
- An inside actor looks over the shoulder of a system engineer as they type administrative credentials into a system.

basefarm

# CYBER VS PHYSICAL SECURITY

How Cybersecurity weaknesses can enable physical attacks:

- Attacker shuts down internet-connected security cameras, allowing a break-in to go undetected, deleting footage, etc.
- The internet-facing keycard access system is compromised, allowing an attacker to grant or remove physical access to the building.
- Network-connected DC Infra systems can be attacked and shut down, causing loss of productivity or a safety incident.
- CPU-intensive malware can be loaded onto a server cluster which spikes power consumption, resulting in overheating, brownouts, or a total loss of power.
- Ransomware on a hospital network can prevent physicians from accessing patient records and providing necessary care.

basefarm

## WHAT IS A CYBERSOC?

24/7 command center responsible for monitoring, analyzing, and protecting an organization from cyber attacks

basefarm

# CYBERSOC RESPONSIBILITIES

- Threat intelligence management
- Security event monitoring, detection, investigation, triage and reporting
- Security incident response management, including malware analysis and IT forensics
- Risk-based vulnerability management (notably, the prioritization of patching)
- Threat hunting
- Security device management and maintenance
- Development of data and metrics for compliance reporting/management

# About Orange Cyberdefense

**We are Europe's leading go-to security services provider, supporting your business globally.**

**Over 2,100**
multi-skilled cybersecurity experts.

**€700+ million***
turnover in 2019

**3,700+**
customers worldwide, best in class in all verticals.

Notable vendor Managed Detection and Response

Gartner

**50 billion**
logs captured daily by our Cyber SOCs.

**Rated Strong Performer MSS**

FORRESTER®

**24/7/365**
continuous monitoring of security systems worldwide.

**European market leading Managed Security Service provider**

pwc

# A holistic portfolio and experience to enable your business.

## Anticipate

- Managed Vulnerability Intelligence
- Threat Detection - Intelligence
  - Data Leakage Detection
  - Brand Protection
  - Attack Surface Reduction
- World Watch

## Identify

- Assessment Services
- Advisory Services
- Security Awareness Training
- Penetration testing
- Red and purple teaming
- DevSecOps

## Protect

- Data-centric Security
- Infrastructure Security
- Network Security
- Security Intelligence
- Endpoint Security
- Identity & Access Management
- Managed Vulnerability Scanning

## Detect

- Managed Threat Detection
  - Log based (SIEM)
  - Network based
  - Endpoint based
- Managed Cybercrime monitoring

## Respond

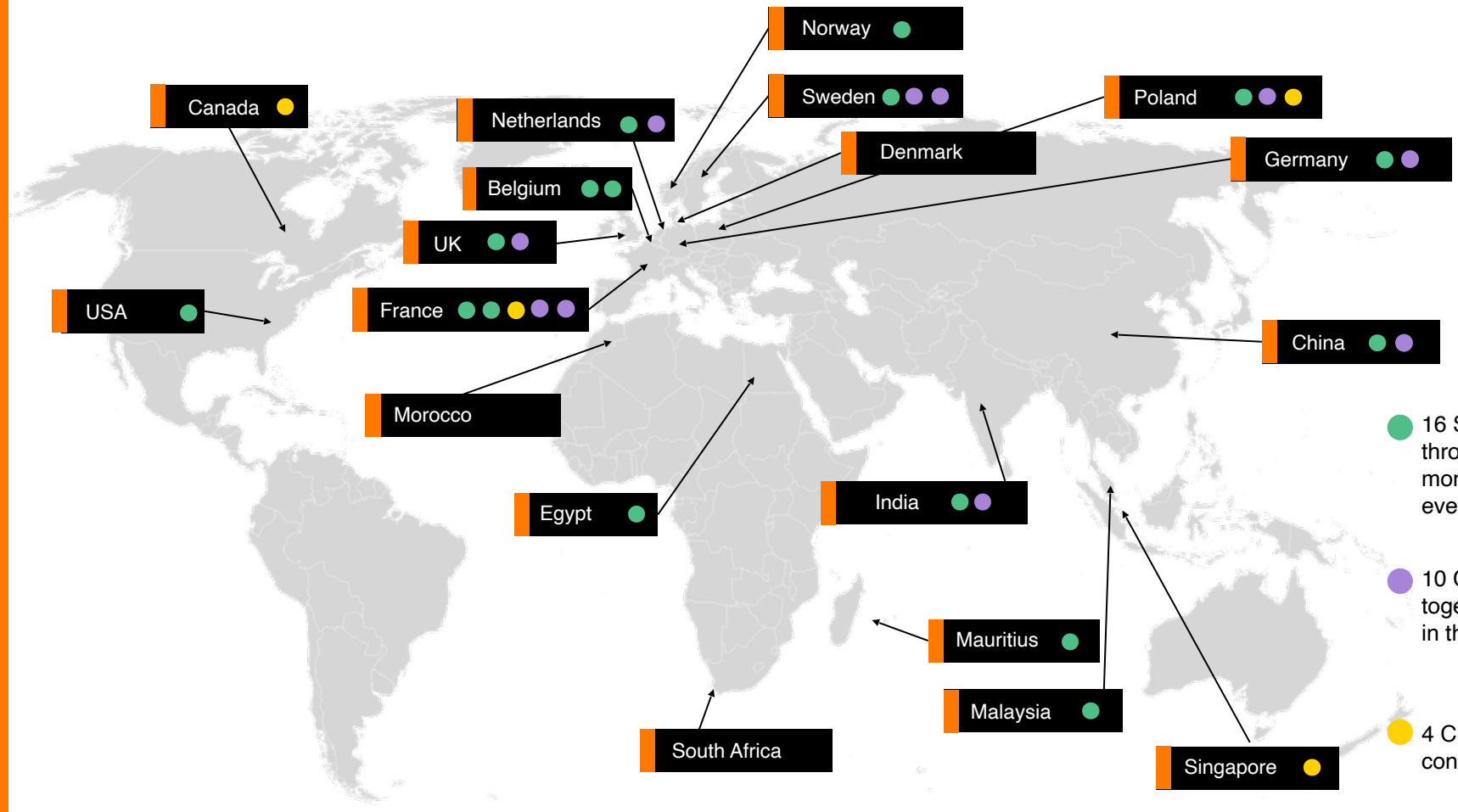
- Incident response
  - Retainer
  - Emergency Response
  - Incident Response Consulting
- Digital forensics
- Malware Analysis
- Endpoint Quarantine

# Global protection with local expertise

**160**
countries with sales and support

## End-to-end solutions
Anticipate, identify protect, detect, and react to cyber attacks

## Partnerships & Alliances
including top security tech vendors, TFCSIRT, FIRST, Phishing Alliance and Europol




- 16 SOCs spread throughout the world monitor and respond to events 24/7/365
- 10 Cyber SOC that bring together the best expertise in threat analysis 24/7/365
- 4 CERTs operate continuously

**2,200+**
Cybersecurity experts working to keep customers secure

**20'000+**
Rogue websites taken down per year

**12 million+**
IOC in our own data lake db 600+ sources

**30 billion+**
potential threats correlated and prevented/day

**1500**
Qualified security incidents managed per month, in average

basefarm


Professional services and advisory

Security testing

Managed Security Services

World wide Threat Intelligence

System acquisition and support

24/7 CSIRT

basefarm

# THANK YOU!


Basefarm Norway
Nydalen Allé 37a
0484 Oslo
Phone: +47 4000 4100
Web: basefarm.no

Basefarm AB
Gårdsvägen 6
169 70 Solna
Phone: +46 8 5011 2600
Web: basefarm.se

Log*in Consultants
Nederland B.V.
Motion Building
Radarweg 60,
1043 NT Amsterdam
Sloterdijk
Phone: +31 20 406 64 66
Web: basefarm.nl

The Unbelievable Machine
Company GMBH
Grolmanstr. 40, D-10623 Berlin
Phone: +49 308 892 65 60
Web: unbelievable-machine.com


**Basefarm**
an Orange Business Subsidiary

**SHAPING TOMORROWS SOLUTIONS TODAY**