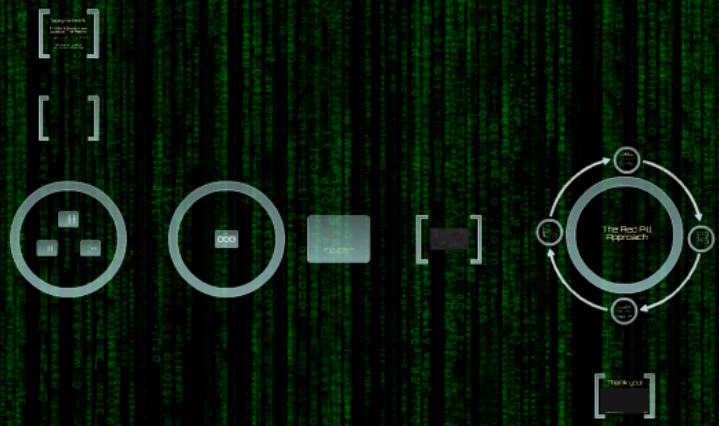


.....DESIGNED BY CHRIS HILDEN.....



Taking the Red Pill  
Incident Response  
outside The Matrix.  
All Rights Reserved  
www.redpill.ir

[ ]



# Taking the Red Pill - Incident Response outside The Matrix

Lorenz Inglin & Stephan Rickauer, Swisscom (Switzerland) AG

*28th Annual FIRST Conference  
Seoul, 12th June - 17th June 2016*



### Whoam?



Whoam? Who is he? What is he doing? What is he thinking? What is he feeling? What is he saying? What is he doing? What is he thinking? What is he feeling? What is he saying?

### About Swisscom



swisscom



### Our Adversaries



# whoami



## Stephan Rickauer

- Senior CSIRT Manager
- 40y, no kids, no dogs
- enjoys traditional Karate
- Leads SC's Red Team
- loves his Kawa Z800

## Lorenz Inglin

- Head of CSIRT
- 37y, 3 kids
- 15+ years in Security
- loved his Ducati 998

# Stephan Rickauer

- Senior CSIRT Manager
- 40y, no kids, no dogs
- enjoys traditional Karate
- Leads SC's Red Team
- loves his Kawa Z800

# Lorenz Inglin

- Head of CSIRT
- 37y, 3 kids
- 15+ years in Security
- loved his Ducati 998



# About Swisscom



## Business

26mio. fixed access line customers

15mio. mobile customers

14mio. TV customers

2mio. broadband customers

13mio. cloud services (SaaS, IaaS, PaaS)

## Facts & Figures

In January, we:

detected and blocked over 200 phishing attacks

took 20,000 malware infected customer computers offline

received 25,000 customer complaints related to Spam and problems caused by malware

notified 1500 customers because of malware infections on their computers

contacted 1200 customers because of stolen credentials

# Business



2.6 mio. fixed access line customers



6.6 mio. mobile customers



1.4 mio. TV customers



2.3 mio. broadband customers



Outsourcing services (banking, ...)

# Facts & Figures

In January, we ...



detected and blocked over **300** phishing attacks



took **20'000** malware infected customer computers offline



received **25'000** customer complaints related to Spam and problems caused by malware



notified **1'500** customers because of malware infections on their computers



contacted **1'200** customers because of stolen credentials

# Our Adversaries



- Vandals
- Hacktivists
- Criminals
- Terrorists
- Governments

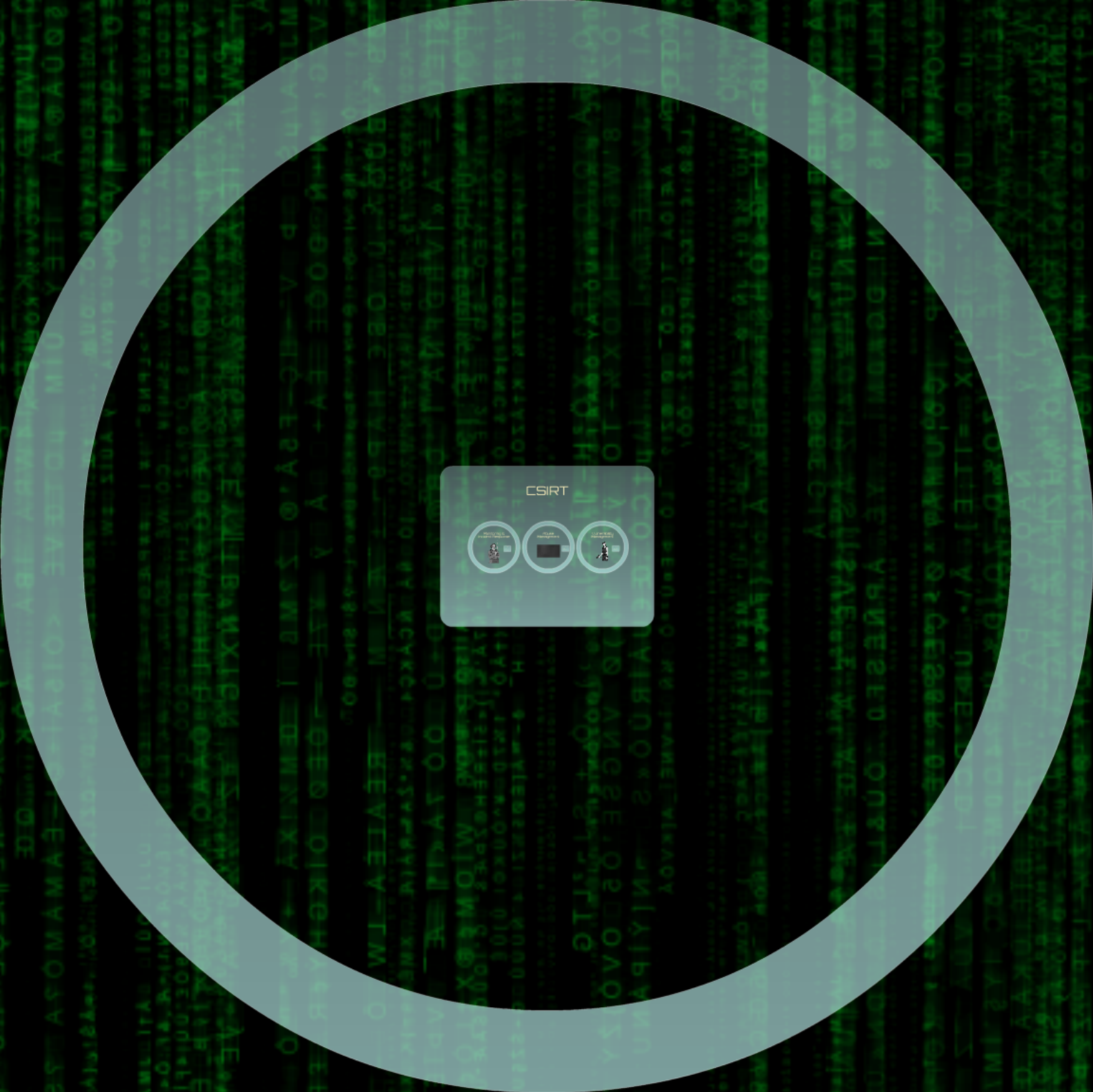
Vandals

Hacktivists

Criminals

Terrorists

Governments



CSIRT



# CSIRT

## Monitoring & Incident Response



Monitoring & Incident Response

## Abuse Management



Abuse Management

## Vulnerability Management



Vulnerability Management

# Monitoring & Incident Response



- Advanced Monitoring
- Forensic Investigations
- Malware Analysis
- Breach Detection
- Threat Intelligence



- Advanced Monitoring
- Forensic Investigations
- Malware Analysis
- Breach Detection
- Threat Intelligence

# Abuse Management



- Sandboxing of infected wireline customers
- Spam
- Phishing
- Abuse Handling



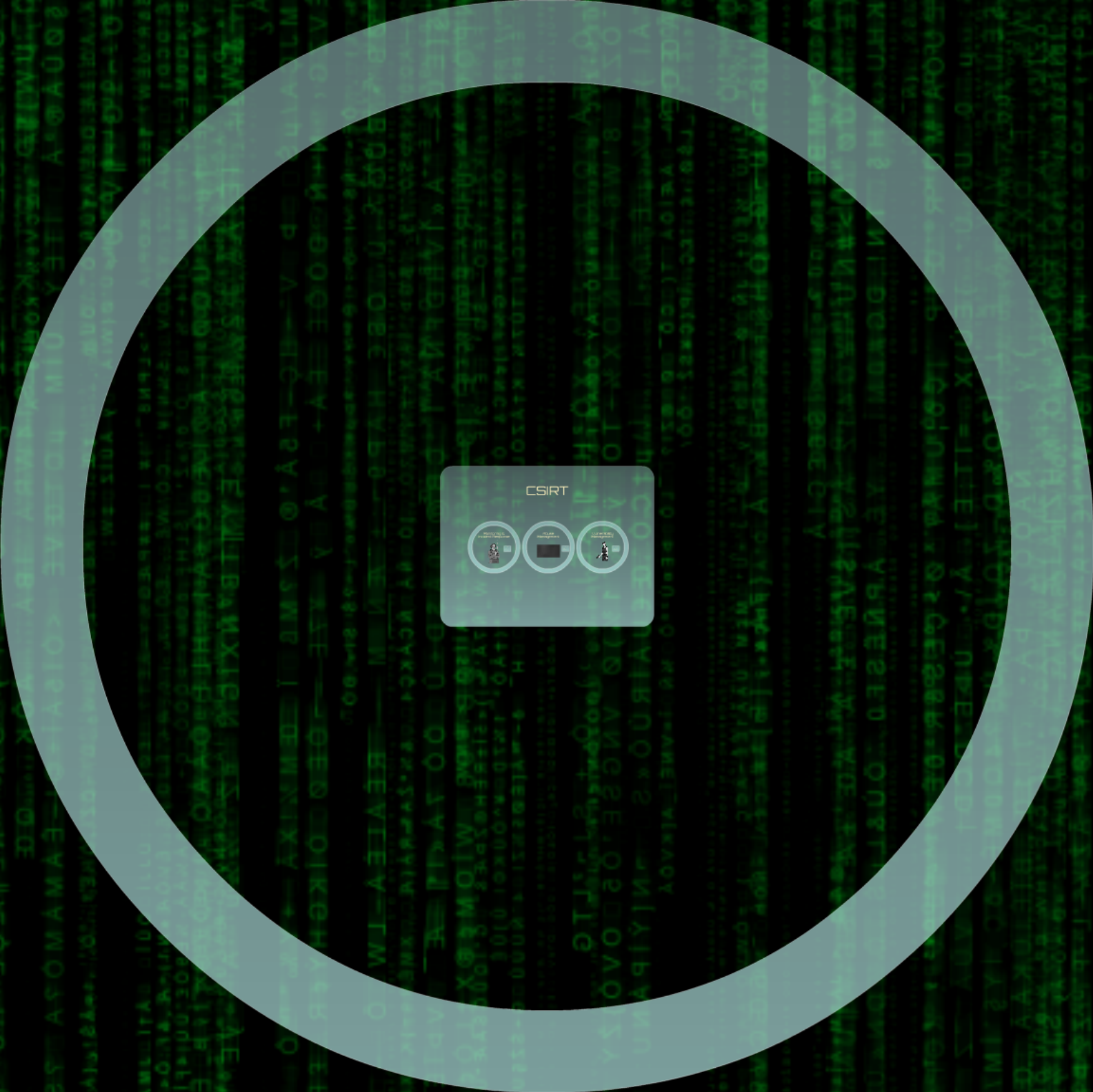
- Sandboxing of infected wireline customers
- Spam
- Phishing
- Abuse Handling

# Vulnerability Management



- Vulnerability Scanning
- Bug Bounty Program
- Emergency Patching
- CVSS Management
- CrowdSecurity Projects

- Vulnerability Scanning
- Bug Bounty Program
- Emergency Patching
- CVSS Management
- CrowdSecurity Projects



CSIRT





We were compliant and satisfied... until...





# The Red Pill Approach

**Innovative Detection**

- Based on human intelligence
- Threat intelligence in context
- Dark Web/Deep Web
- Open Source Intelligence
- Threat Hunting
- MITRE ATT&CK

**Improved Communication**

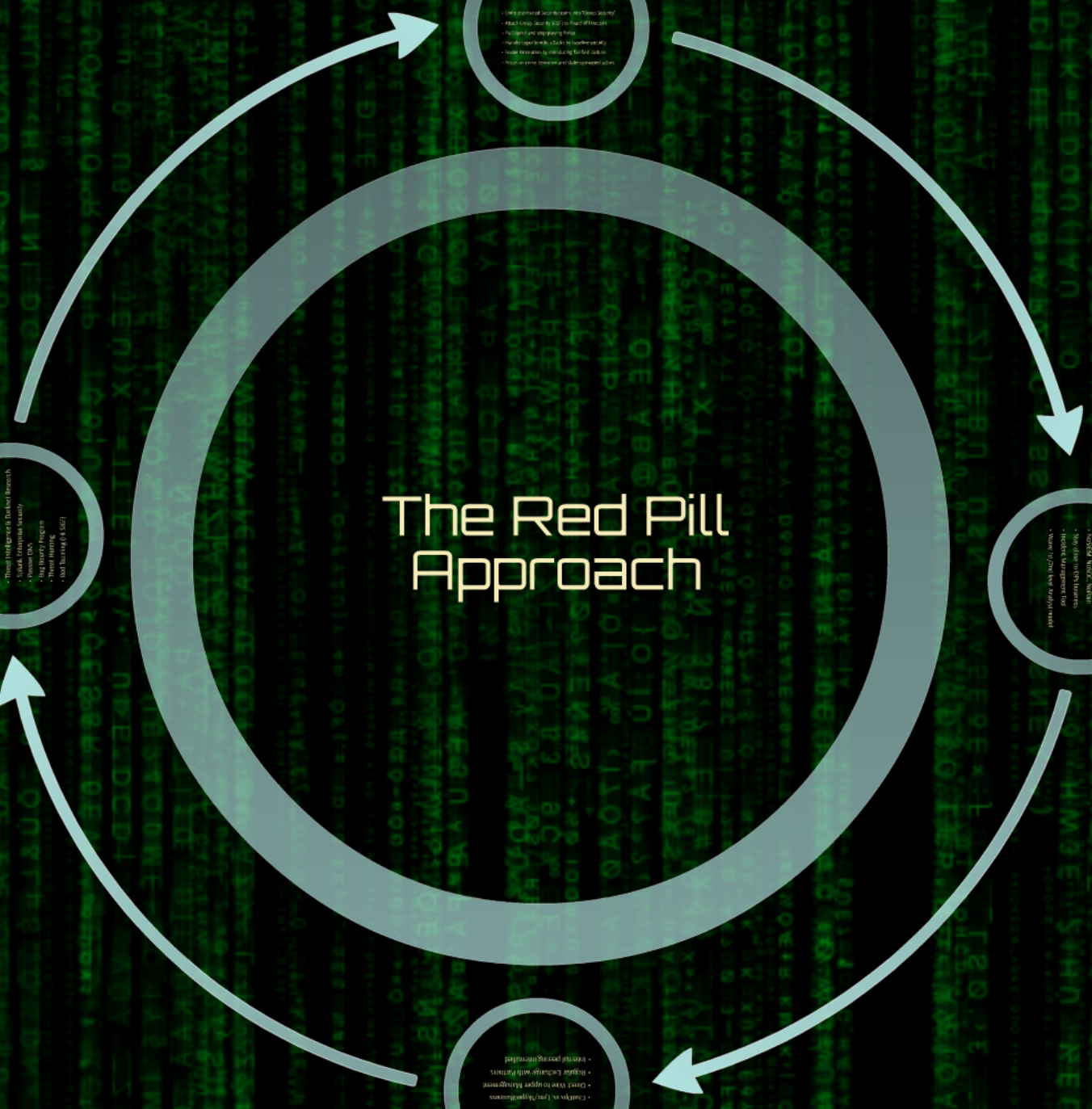
- Security Line/Threatline
- Data type to user language
- Single looking with partners
- Events processing

**Saving Time (and have fun!)**

- Attack Noise Filter
- Simplify triage
- Incident Response for threat hunters

**Adjusting the Strategy**

- Operational assumptions re-visited
- Attack Logic (ATO) to threat detection
- Hypothesis and supporting Proof
- Feedback loops to the user
- User feedback by interacting with system
- Focus on user experience and development



# The Red Pill Approach

# Adjusting the Strategy

- Unite distributed Security teams into "Group Security"
- Attach Group Security (GSE) to Board of Directors
- Be Copilot and stop playing Police
- Handle opportunistic attacks by baseline security
- Foster Innovation by introducing 'fail fast' culture
- Focus on crime, terrorism and state-sponsored actors

# Saving Time (and have phun)

- NoSIEM, NoSOC, NoPain
- Stay close to OPs business
- Incident Management Tool
- Waive 1st/2nd level Analyst model

# Improved Communication

- ChatOps vs. Lync/Skype4Business
- Direct Wire to upper Management
- Regular Exchange with Partners
- Internal peering intensified

# Innovative Detection

- Breach Detection
- Threat Intelligence & Darknet Research
- Splunk Enterprise Security
- Passive DNS
- Bug Bounty Program
- Threat Hunting
- Red Teaming (Hi SIG!)

# The Red Pill Approach

**Innovative Detection**

- Based on human intelligence in network research
- Track, identify and locate
- Identify and track
- Track and identify
- Identify and track
- Track and identify

**Adjusting the Strategy**

- Identify and track
- Track and identify
- Identify and track
- Track and identify
- Identify and track
- Track and identify

**Saving Time (and have fun!)**

- Identify and track
- Track and identify
- Identify and track
- Track and identify
- Identify and track
- Track and identify

**Improved Communication**

- Identify and track
- Track and identify
- Identify and track
- Track and identify
- Identify and track
- Track and identify



# Thank you!



@hakasumi @LorenzInglin

:wq

Taking the Red Pill  
Incident Response  
outside The Matrix.  
<https://www.linkedin.com/pulse/taking-red-pill-incident-response-outside-the-matrix-alexander-berk/>

