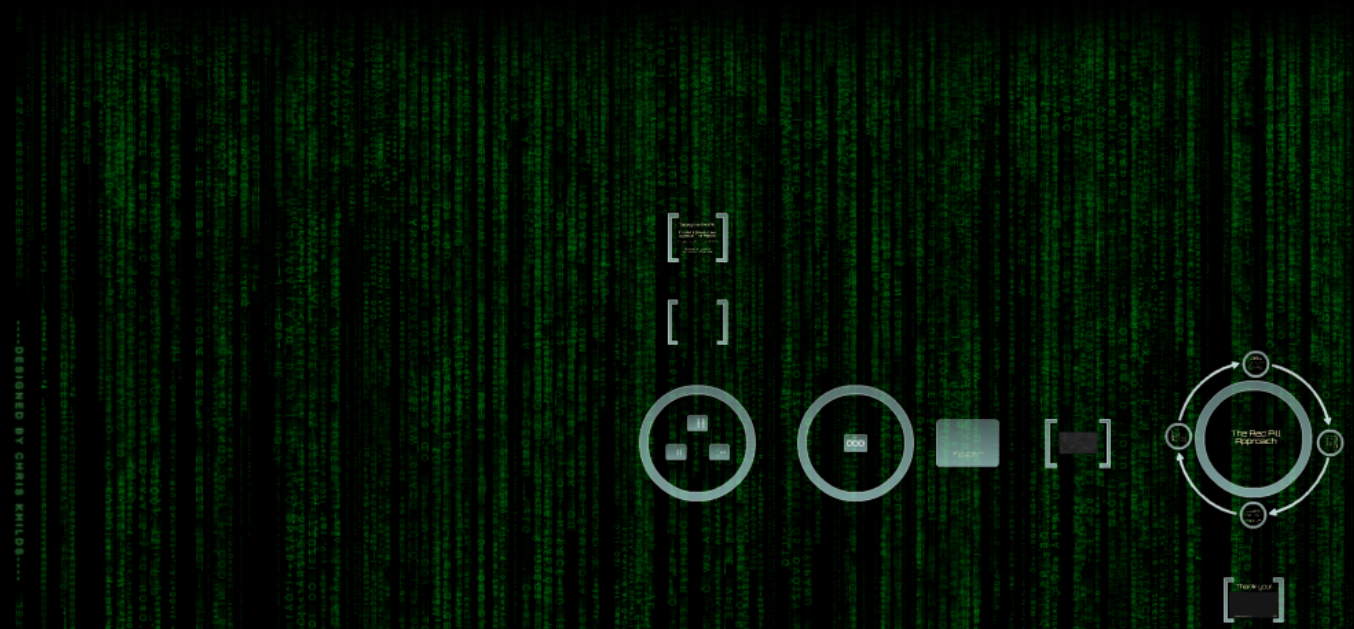

The Red Pill Approach

Taking the Red Pill

Incident Response outside The Matrix

Thank you!

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


whoami


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

swisscom

Business

- 2.5 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

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

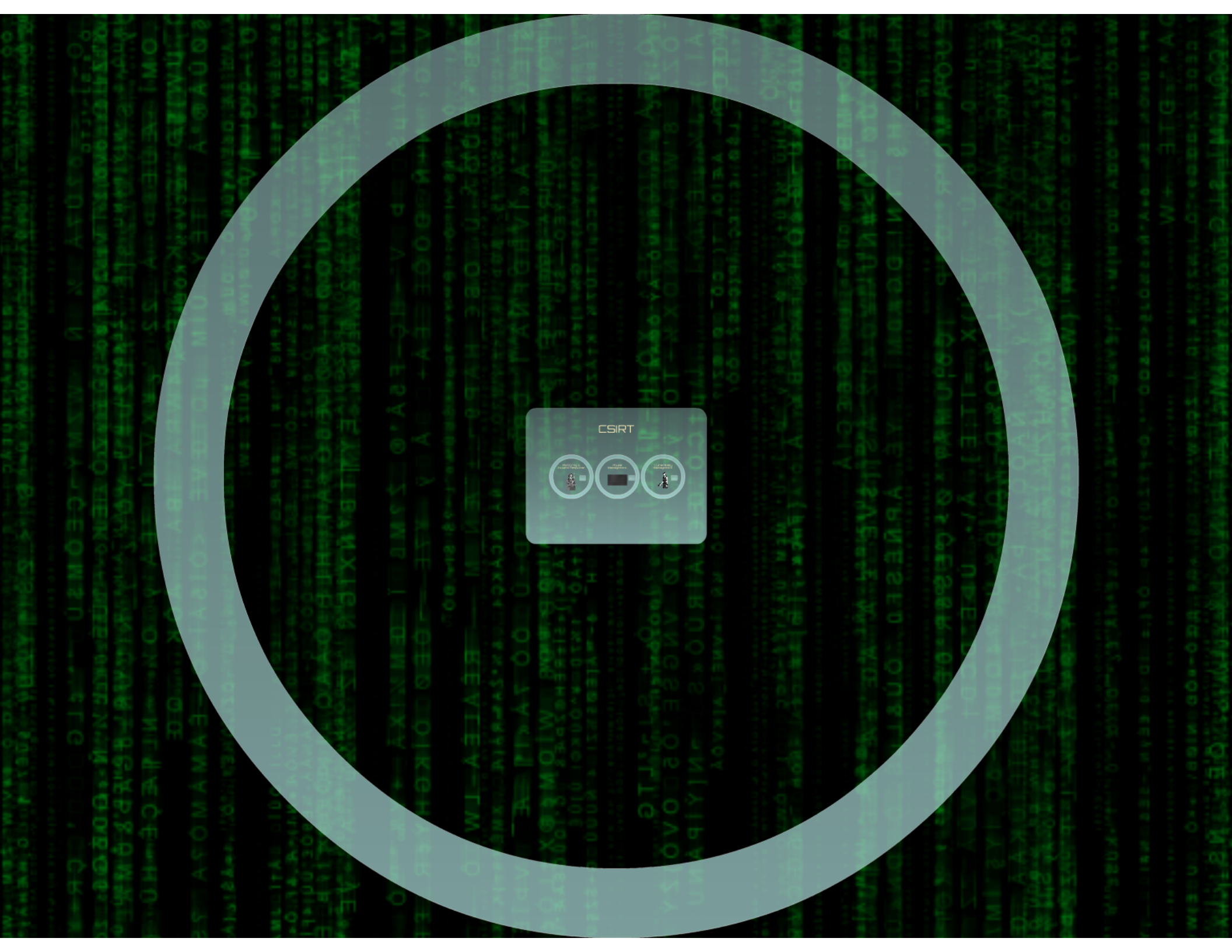
Vandals

Hacktivists

Criminals

Terrorists

Governments


CSIRT

CSIRT

Monitoring & Incident Response

Abuse 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

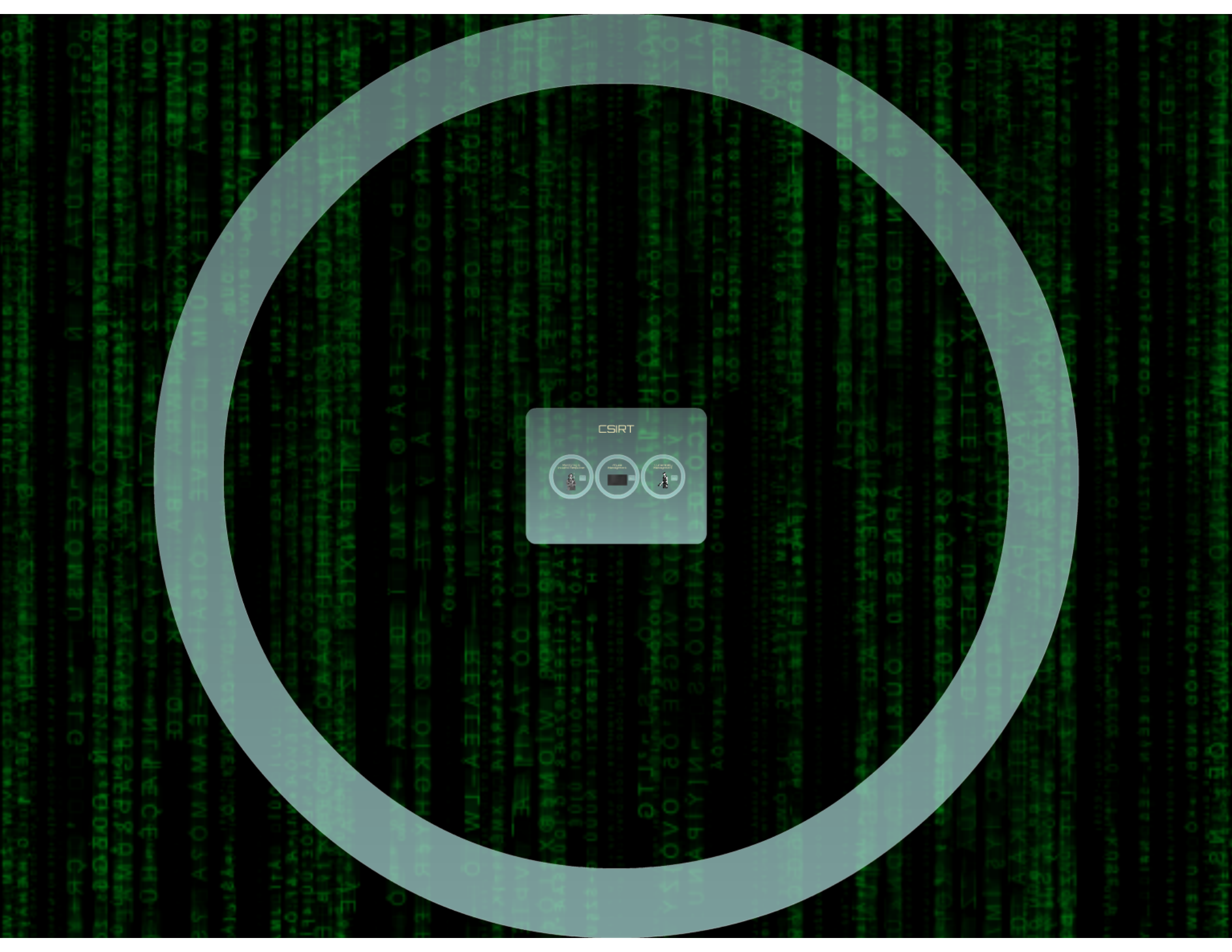
- Sandboxing of infected wireline customers
- Spam
- Phishing
- Abuse Handling

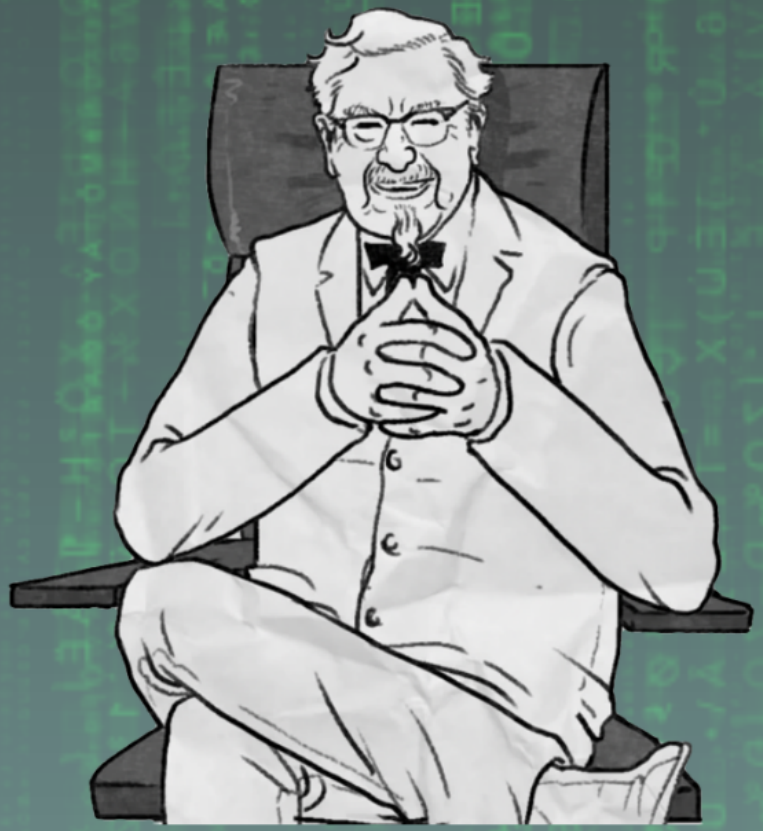
- Sandboxing of infected wireline customers
- Spam
- Phishing
- Abuse Handling

Vulnerability Management

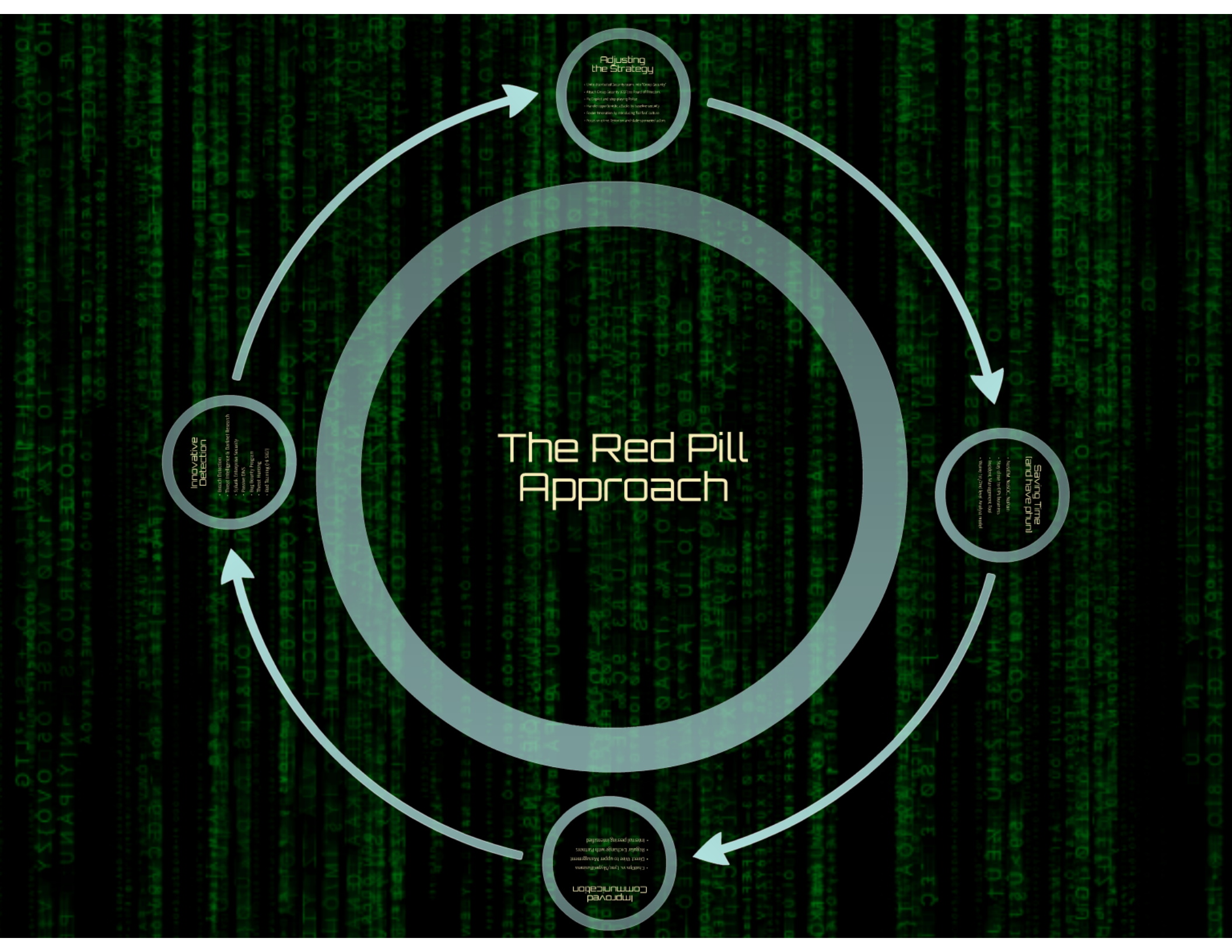
- Vulnerability Scanning
- Bug Bounty Program
- Emergency Patching
- CVSS Management
- CrowdSecurity Projects

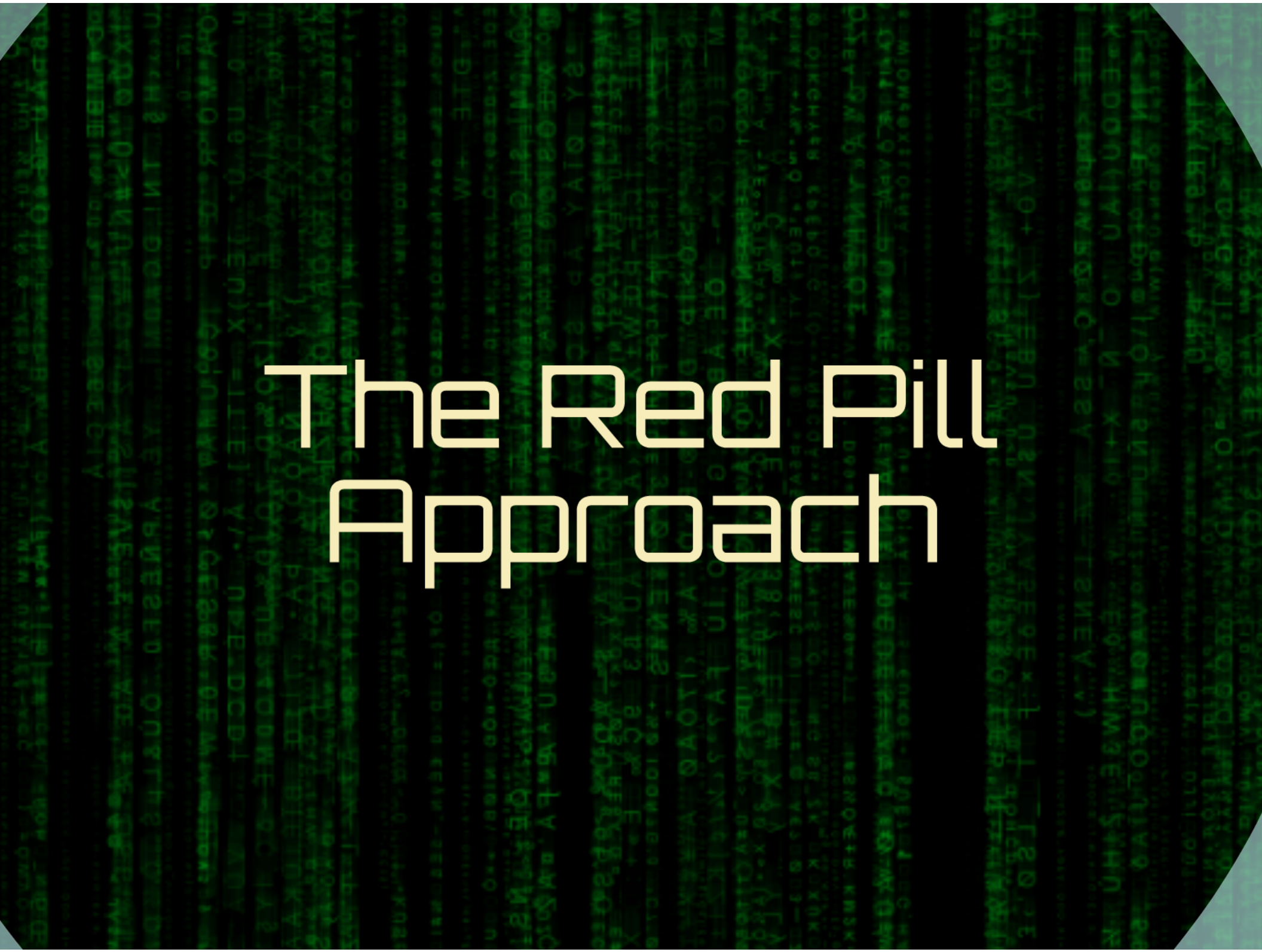
- Vulnerability Scanning
- Bug Bounty Program
- Emergency Patching
- CVSS Management
- CrowdSecurity Projects


CSIRT



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


Adjusting the Strategy
Innovative Detection
Improved Communication
Saving Time and Money
The Red Pill Approach


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-sponsered actors

Saving Time (and have phun)

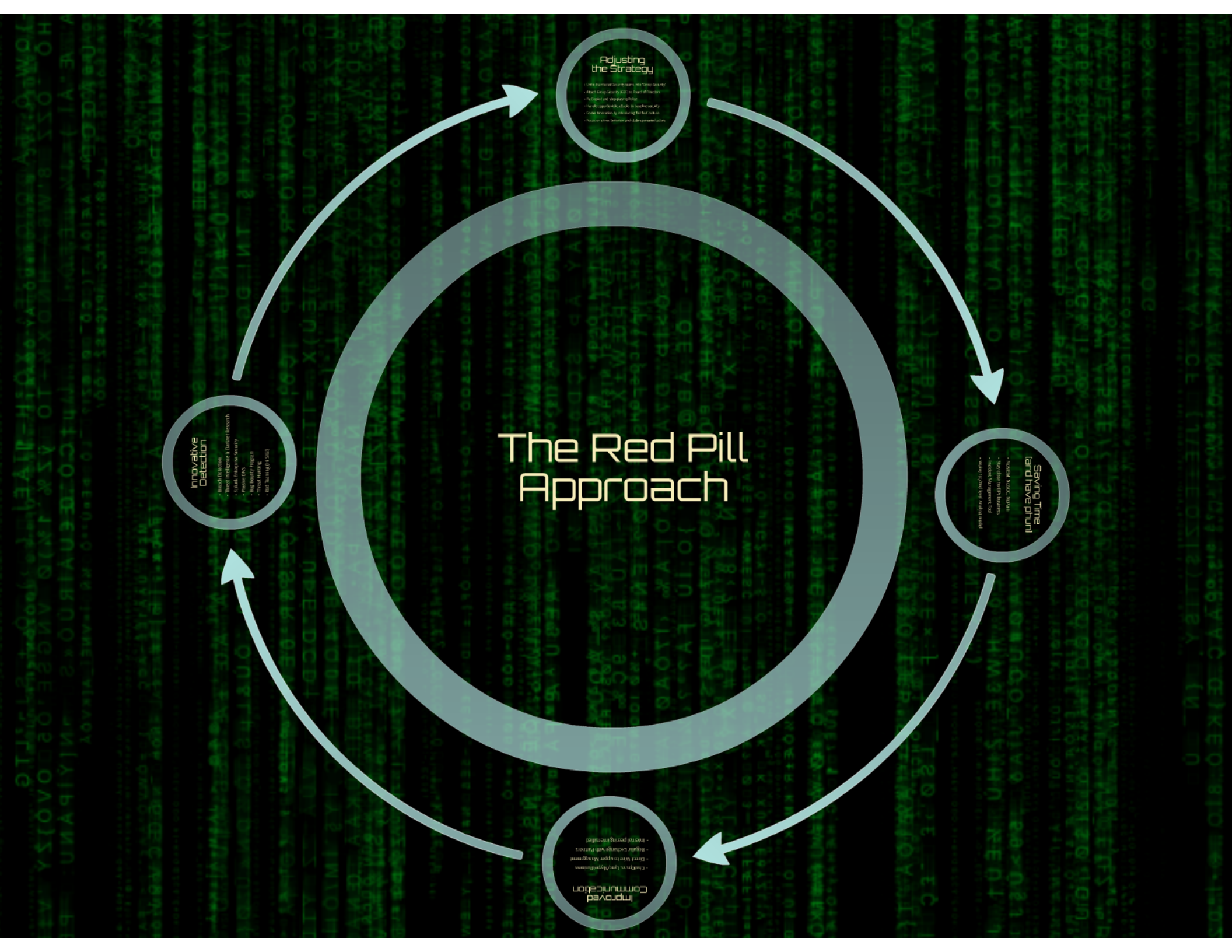
- NoSIEM, NoSOC, NoPain
- Stay close to OPs business
- Incident Management Tool
- Waive 1st/2nd level Analyst model

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!)


Adjusting the Strategy
Innovative Detection
Improved Communication
Saving Time and Money
The Red Pill Approach

Thank you!

@hakasumi @LorenzInglin

:wq

Taking the Red Pill

Incident Response outside The Matrix

Thank you!