Cyber Ranges

Cyber Range: definition (NIST)

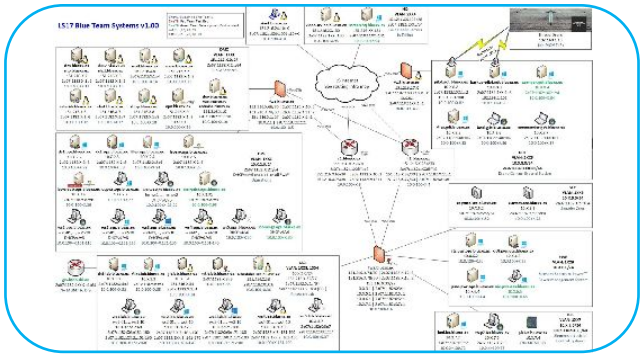
- CR can be termed as responsive simulated depiction of an institution’s local network, system, tools, and applications that are connected to a simulated network environment

- They ensure safety and provide a legal environment to implement cybersecurity skills and security testing.

Cyber Range: definition (NIST)

- CR can be termed as responsive simulated depiction of an institution's **local network**, **system**, **tools**, and **applications** that are connected to a simulated network environment

- They ensure safety and provide a legal environment to implement cybersecurity skills and security testing.

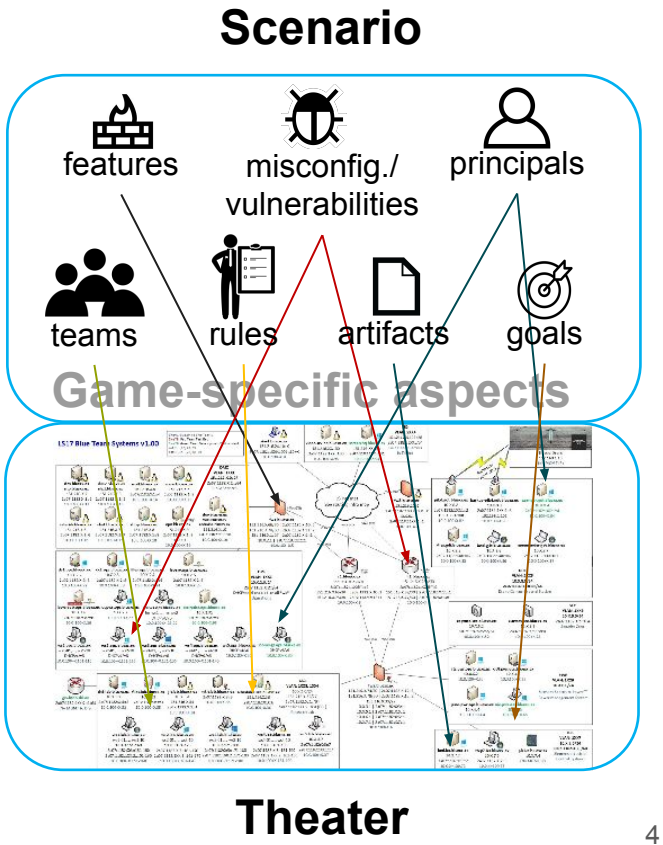


Theater

Cyber Range: definition (NIST)

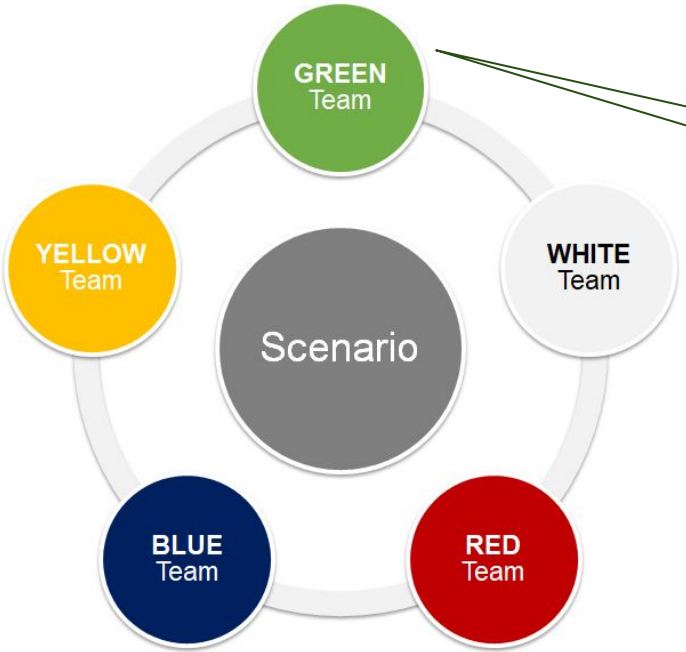
- CR can be termed as responsive simulated depiction of an institution's local network, system, tools, and applications that are connected to a simulated network environment.

- They ensure safety and provide a legal environment to implement **cybersecurity skills** and **security testing**.



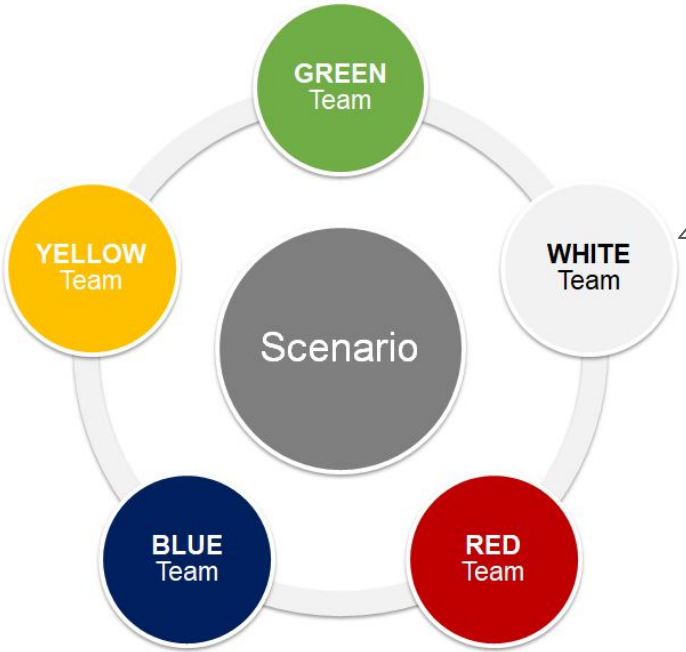
Teams

GREEN Team (GT)



GREEN Team is responsible for the physical and online infrastructure

WHITE Team (WT)

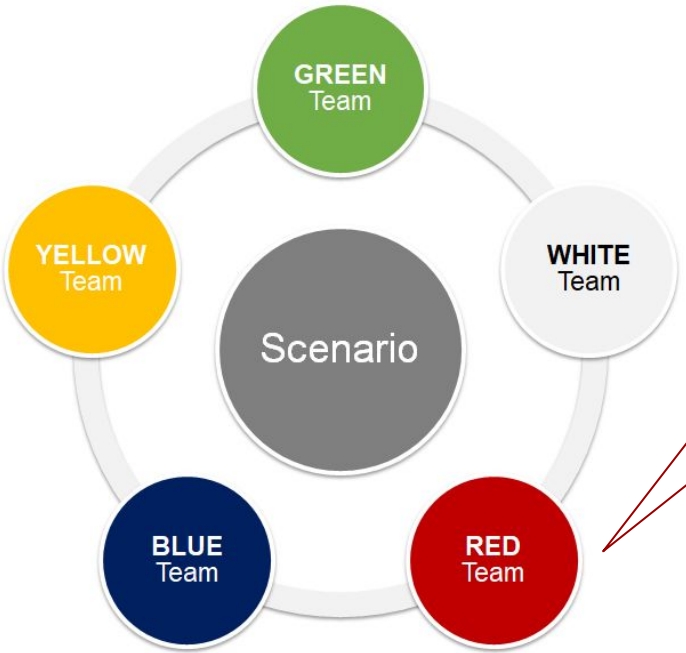


WHITE Team represents exercise managers, referees, organizers, and instructors.

The team is responsible for:

- monitoring the actions of players
- coordinating and driving the scenario storyline
- producing the final scoreboard

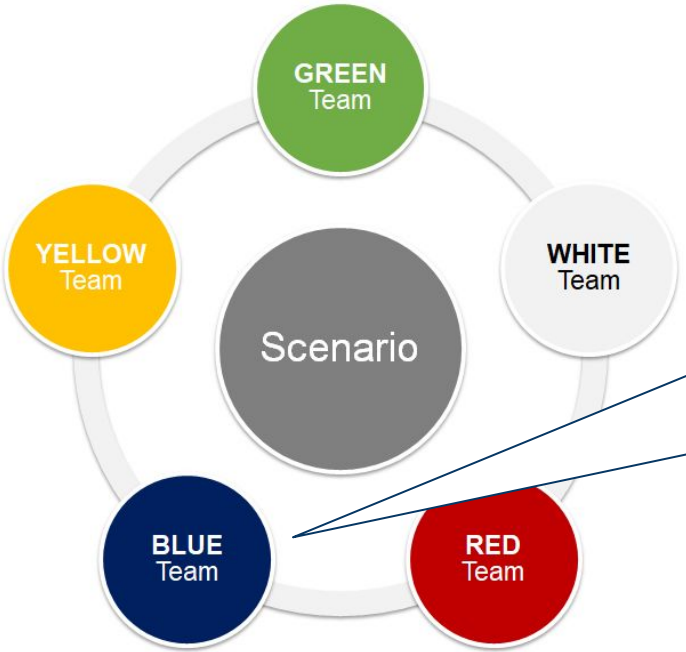
RED Team (RT)



RED Team plays the role of attackers.

Attacks aim at achieving a specific goal (e.g., accessing a specific data or compromising a specific resource)

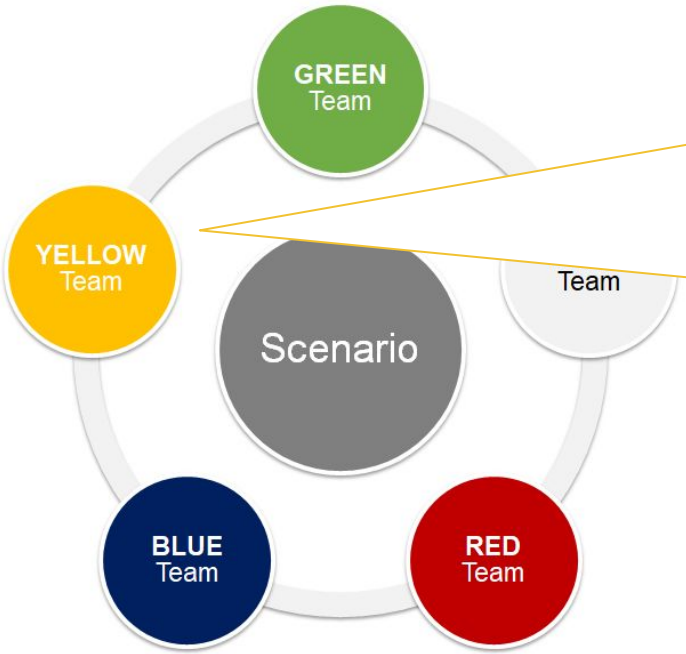
BLUE Team (BT)



BLUE Team has the task of defending the infrastructure.

Their main goal is to identify and protect the assets in the scenario.

YELLOW Team (YT)



YELLOW Team (aka ***Blondies***) makes legitimate interactions with the environment:

- can be partially simulated by automatic tools
- hides the RED Team activity
- injects events during the execution

NATO Locked Shields exercise

What is Locked Shields?

World’s largest International technical live-fire cyber defence exercise

What is Locked Shields?

- Live-fire = real-time Red Team vs. Blue Team exercise
- Involves regular business IT, critical infrastructure and military systems
- Integrates technical and strategic decision-making exercise
- More than 1200 cyber defence experts from nearly 30 nations
- Runs on Cyber Range, a platform managed by the Estonian Defence Forces

Objectives of the Locked Shields initiative

1. Train teams of cyber professionals to collaborate with each other
2. Learn from the activities of Blue and Red Teams
3. Building trust networks, and sharing information and experience
4. Improve the organizers' capability to conduct exercises
5. Experiment with situation awareness solutions
6. Raise awareness for decision makers at all levels

IT Specific Objectives - Technical

1. Understand and protect an unfamiliar environment
2. System administration and prevention of attacks
3. Code review and patching
4. Monitoring networks, detecting and responding to attacks
5. Handling cyber incidents
6. Conducting forensic investigation

IT Specific Objectives - Organizational

7. Teamwork: delegation, dividing and assigning roles, leadership
8. Cooperation and information sharing
9. Ability to convey the big picture
10. Reporting
11. Crisis communication
12. Time management and prioritization

Teams

- Blue Team(s) National Teams
  - x25, one per nation
- Red Team NATO Team
- Yellow Team Students from Tallinn
- Green Team NATO SysAdmins
- White Team NATO Referees

Locked Shields 2017, Blue Team 14 - Italy

Scenario

Actors

- **Berylia** – a fictitious island state, in the middle of the North Atlantic Ocean
- **Crimsonia** - a fictitious island state neighbouring Berylia
    - Political and military tensions with Berylia
- **Anti-Berylia Community** - Crimsonian minority living in Berylia
- **[NATO nation]** - helps Berylia in dealing with attacks

Scenario - State of Berylia

Situation

- One third of the Berylian population is ethnically Crimsonian
- Anti Berylian Community is formed by Crimsonian Berylian to
  - Undermine Berylian government and change regime
  - Create instability through division of Berylian population
  - Tactics such as fostering fear and hate of immigrants (Berylia recently hosted more refugees)
- The average Berylian is dissatisfied with their current government

Scenario - State of Berylia

Events leading to “Locked Shields”

- **27/03** - Crimsonia concluded a large naval near Berylia’s territorial waters
  Crimsonia states that the number of forces is high to conduct a turnover of troops
- **01/04** - Elections in Berylia. Jones from the Party of Crimsonian Friendship wins
- **03/04** - An electronic post-election audit shows that results were wrong. Jones did not win
- **04/04** - Results of post-election audit leads to protests
- **05/04** - Major flooding and landslides damage IT systems and critical infrastructure
  Berylian military is deployed to provide humanitarian aid to citizens in need
- **08/04** - Accusations your advisers for accepting money in exchange for helping refugees to Berylia

Game aspects

Dynamic component

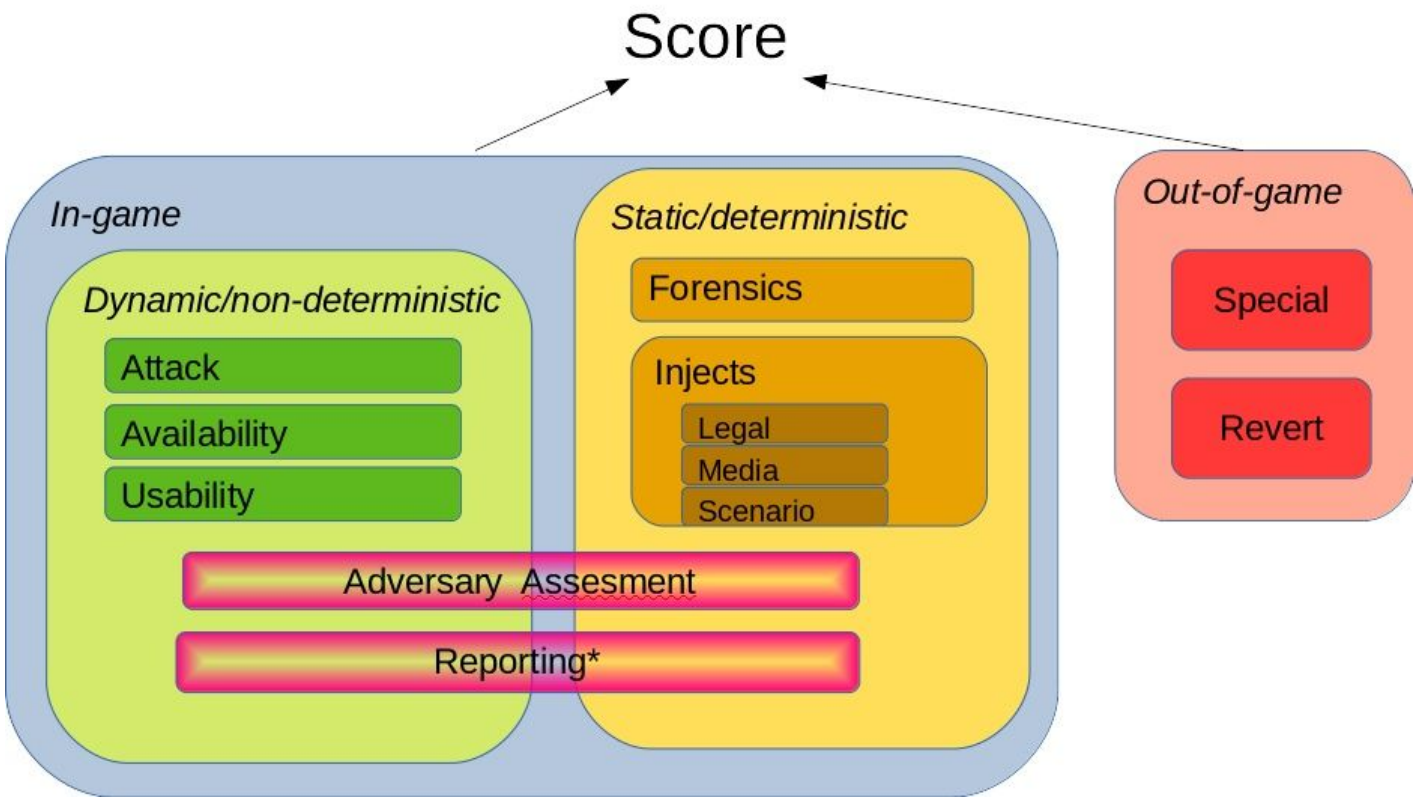
- Attack
- Availability
  - Services are automatically checked
- Usability
  - Services are manually checked

Static component

- Forensics
- Injects (explicit tasks given to BTs)
  - Legal
  - Media
  - Scenario

Mixed component

- Reporting
- Adversary assessment


Score
In-game
Dynamic/non-deterministic
Attack
Availability
Usability
Static/deterministic
Forensics
Injects
Legal
Media
Scenario
Adversary Assesment
Reporting*
Out-of-game
Special
Revert

Code Review subteam - Preparation

Timeline

- Day 0
  - Offline preparation
- Day 1
  - 9.00-23.59 - Gamenet opens
- Day 2
  - 0.00-14.00 - Gamenet closes
  - Systems are reverted
- Day 3+
  - Offline analysis

Tasks

- Understand the analysis infrastructure
  - Debian with i3wm (a hit or miss choice, but it mostly missed)
- Understand the game infrastructure
  - Software versions
  - Frameworks
  - CMS (e.g. Wordpress/Joomla/Drupal)
- Gather services
  - Code
  - Configuration

Code Review subteam - Execution

Timeline

- Day 0
  - 9-17 - Gamenet is open
  - No attacks
  - Systems are reverted
- Day 1
  - 9-16 - Gamenet is open
  - Attacks start (defacement + exploits)
- Day 2
  - 14.00 - Gamenet closes
  - Destructive attacks start
- Day 3
  - Hotwash
  - Lesson learned

Tasks

- Patch vulnerable services
  - Remove backdoors
  - Remove vulnerabilities
- Maintain the game infrastructure
  - Answer to tickets from Yellow Team
  - Restore attacked services
- Detect attacks
  - Help understanding and reporting attacks

LS17 Blue Team Systems v1.00

Blue01-Blue20: LS Blue Teams
Blue78: Red Team Test Bed
Blue79: Green Team Development Environment
X=1,2,...,20, 78, 79
XX=01,02,...,20, 78, 79

sinet.bluexx.ex
151.216.24.10+X
2a07:1182:1000:1001::10+X
10.0.100+X.8

video-srv.hq.bluexx.ex
151.216.XX.130
2a07:1182:1XX::130
10.0.100+X.93

screen.hq.bluexx.ex
151.216.XX.131
2a07:1182:1XX::131
10.0.100+X.94

HQ
VLAN: 2XX4
151.216.XX.128/28
2a07:1182:1XX::/64
Blue Headquarters
in Tallinn

Threod Drone
192.168.1.10
(No MGMT IP)

Radio Link
VLAN 2XX3

DMZ
VLAN: 1XX1
151.216.X.0/27
2a07:1182:X:1::/64
Public Services

dns.bluexx.ex
ntp.bluexx.ex
151.216.X.2
2a07:1182:X:1::2
10.0.100+X.12

dns2.bluexx.ex
ntp2.bluexx.ex
151.216.X.3
2a07:1182:X:1::3
10.0.100+X.13

mail.bluexx.ex
151.216.X.4
2a07:1182:X:1::4
10.0.100+X.14

www.bluexx.ex
151.216.X.5
2a07:1182:X:1::5
10.0.100+X.15

asterisk.bluexx.ex
151.216.X.6
2a07:1182:X:1::6
10.0.100+X.16

chat.bluexx.ex
151.216.X.7
2a07:1182:X:1::7
10.0.100+X.17

shop.bluexx.ex
151.216.X.8
2a07:1182:X:1::8
10.0.100+X.18

vpn.bluexx.ex
151.216.X.9
2a07:1182:X:1::9
10.X.0.0
10.0.100+X.19

dev.bluexx.ex
wiki.bluexx.ex
redmine.bluexx.ex
151.216.X.10
2a07:1182:X:1::10
10.0.100+X.10

LS Internet
See routing infra map

fw1.bluexx.ex
51.216.X.66/30 | 2a07:1182:X:10::2
51.216.X.70/30 | 2a07:1182:X:11::2
151.216.X.1/27 | 2a07:1182:X:1::1
10.X.2.1 | 2a07:1182:X:2::1
10.0.100+X.5

VLAN 2802

fw3.bluexx.ex
151.216.27.X
2a07:1182:1000:1004::X
10.X.8.1
2a07:1182:1XX:1::1
10.0.100+X.7

VLAN 2XX7
VLAN 2XX1
VLAN 2XX2
VLAN 2XX6

pilot.gdt.bluexx.ex
10.X.8.2
2a07:1182:1XX:1::2
192.168.1.100
10.0.100+X.82

backup-pilot.gdt.bluexx.ex
10.X.8.3
2a07:1182:1XX:1::3
192.168.1.101
10.0.100+X.83

cam-gen.gdt.bluexx.ex
10.X.8.4
2a07:1182:1XX:1::4
10.0.100+X.84

files.gdt.bluexx.ex
10.X.8.5
2a07:1182:1XX:1::5
10.0.100+X.85

intel.gdt.bluexx.ex
10.X.8.6
2a07:1182:1XX:1::6
10.0.100+X.86

commander.gdt.bluexx.ex
10.X.8.7
2a07:1182:1XX:1::7
10.0.100+X.87

GDT
VLAN: 2XX5
10.X.8.0/24
2a07:1182:1XX:1::/64
Drone Control Ground Station

OPS
VLAN: 1XX2
10.X.2.0/24
2a07:1182:X:2::/64
DHCPv4/v6 enabled on all *ws*
Operations

dc1.ops.bluexx.ex
10.X.2.2
2a07:1182:X:2::2
10.0.100+X.22

dc2.ops.bluexx.ex
10.X.2.3
2a07:1182:X:2::3
10.0.100+X.23

files.ops.bluexx.ex
10.X.2.4
2a07:1182:X:2::4
10.0.100+X.24

icc-srv.ops.bluexx.ex
10.X.2.5
2a07:1182:X:2::5
10.0.100+X.25

icc-oradb.ops.bluexx.ex
10.X.2.6
2a07:1182:X:2::6
10.0.100+X.26

ui.pwr.ops.bluexx.ex
10.X.2.7
10.0.100+X.27

icc-ws.ops.bluexx.ex
icc-ws1,..., icc-ws2
DHCPv4/v6
10.0.100+X.28-29

icc-radar.ops.bluexx.ex
10.X.2.31
2a07:1182:X:2::31
10.0.100+X.95

ws1.ops.bluexx.ex
ws1-01,..., ws1-10
DHCPv4/v6
10.0.100+X.101-110

ws2.ops.bluexx.ex
ws2-01,..., ws2-10
DHCPv4/v6
10.0.100+X.111-120

ws3.ops.bluexx.ex
ws3-01,..., ws3-10
DHCPv4/v6
10.0.100+X.121-130

ws4.ops.bluexx.ex
ws4-01,..., ws4-10
DHCPv4/v6
10.0.100+X.131-140

ws5.ops.bluexx.ex
DHCPv4/v6
10.0.100+X.20

icc-ws-gt.ops.bluexx.ex
DHCPv4/v6
10.0.100+X.30

r1.bluexx.ex
151.216.X.250/30
2a07:1182:1XX:fffe::2
151.216.X.65/30 | 2a07:1182:X:10::1
151.216.X.73/30 | 2a07:1182:X:12::1
10.0.100+X.3

r2.bluexx.ex
151.216.X.254/30
2a07:1182:1XX:ffff::2
151.216.X.69/30 | 2a07:1182:X:11::1
151.216.X.77/30 | 2a07:1182:X:13::1
10.0.100+X.4

capture.sec.bluexx.ex
10.X.5.2
2a07:1182:X:5::2/64
10.0.100+X.52

custom.sec.bluexx.ex
10.X.5.3
2a07:1182:X:5::3/64
10.0.100+X.53

SEC
VLAN: 1XX5
10.X.5.0/24
2a07:1182:X:5::/64
Security Zone

VLAN 2XX8
VLAN 2XX9

fw2.bluexx.ex
151.216.X.74/30 | 2a07:1182:X:12::2
151.216.X.78/30 | 2a07:1182:X:13::2
151.216.X.33/27
10.X.3.1 | 2a07:1182:X:3::1
10.X.5.1 | 2a07:1182:X:5::1
10.X.6.1 | 2a07:1182:X:6::1
10.X.7.1 | 2a07:1182:X:7::1
10.0.100+X.6

rts.pwr.ops.bluexx.ex
10.X.6.2
10.0.100+X.62

dc4.pwr.ops.bluexx.ex
10.X.6.3
10.0.100+X.63

psos.pwr.ops.bluexx.ex
10.X.6.4
10.0.100+X.64

ui2.pwr.ops.bluexx.ex
10.X.6.5
10.0.100+X.65

PWR
VLAN: 1XX6
10.X.6.0/24
Siemens Spectrum Power™
Power Management System

gw.btXX.dsl.ex
2a07:1182:1XX:2::1/64
(No MGMT to BTs)

dc3.lab.bluexx.ex
10.X.3.2
2a07:1182:X:3::2
10.0.100+X.32

files.lab.bluexx.ex
10.X.3.3
2a07:1182:X:3::3
10.0.100+X.33

git.lab.bluexx.ex
10.X.3.4
151.216.X.34
2a07:1182:X:3::4
10.0.100+X.34

mkit.lab.bluexx.ex
2a07:1182:X:3::5
10.0.100+X.35

scheduler.lab.bluexx.ex
151.216.X.36
2a07:1182:X:3::6
10.0.100+X.36

LAB
VLAN: 1XX3, 1XX4
10.X.3.0/24
151.216.X.32/27
2a07:1182:X:3::/64
2a07:1182:1XX:2::/64 (DSL)
Research Lab

ws1.lab.bluexx.ex
ws1-01,..., ws1-10
10.X.3.151-160
2a07:1182:X:3::151-160
2a07:1182:1XX:2::151-160
10.0.100+X.151-160

ws2.lab.bluexx.ex
ws2-01,..., ws2-10
10.X.3.161-170
2a07:1182:X:3::161-170
2a07:1182:1XX:2::161-170
10.0.100+X.161-170

ws3.lab.bluexx.ex
ws3-01,..., ws3-10
10.X.3.171-180
2a07:1182:X:3::171-180
2a07:1182:1XX:2::171-180
10.0.100+X.171-180

ws4.lab.bluexx.ex
ws4-01,..., ws4-10
10.X.3.181-190
2a07:1182:X:3::181-190
2a07:1182:1XX:2::181-190
10.0.100+X.181-190

ws5.lab.bluexx.ex
10.X.3.7
2a07:1182:X:3::7
2a07:1182:1XX:2::7
10.0.100+X.37

hmi.ics.bluexx.ex
10.X.7.2
2a07:1182:X:7::2
10.0.X+100.72

step7.ics.bluexx.ex
10.X.7.3
2a07:1182:X:7::3
10.0.X+100.73

plc.ics.bluexx.ex
10.X.7.4
(No MGMT IP)

ICS
VLAN: 1XX7
10.X.7.0/24
2a07:1182:X:7::/64
Siemens Industrial
Control Systems

Day 1 - 10/04

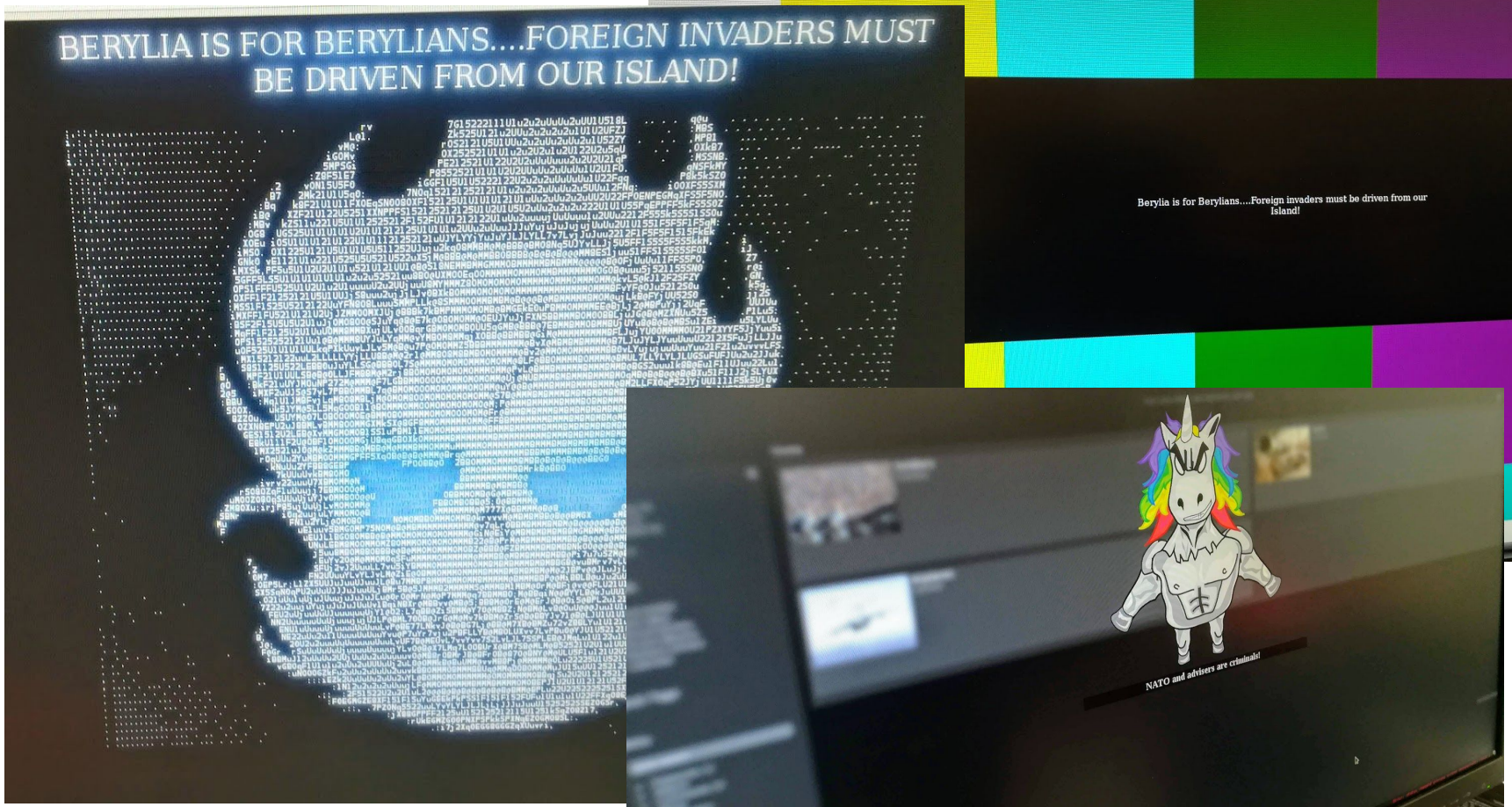
Ship

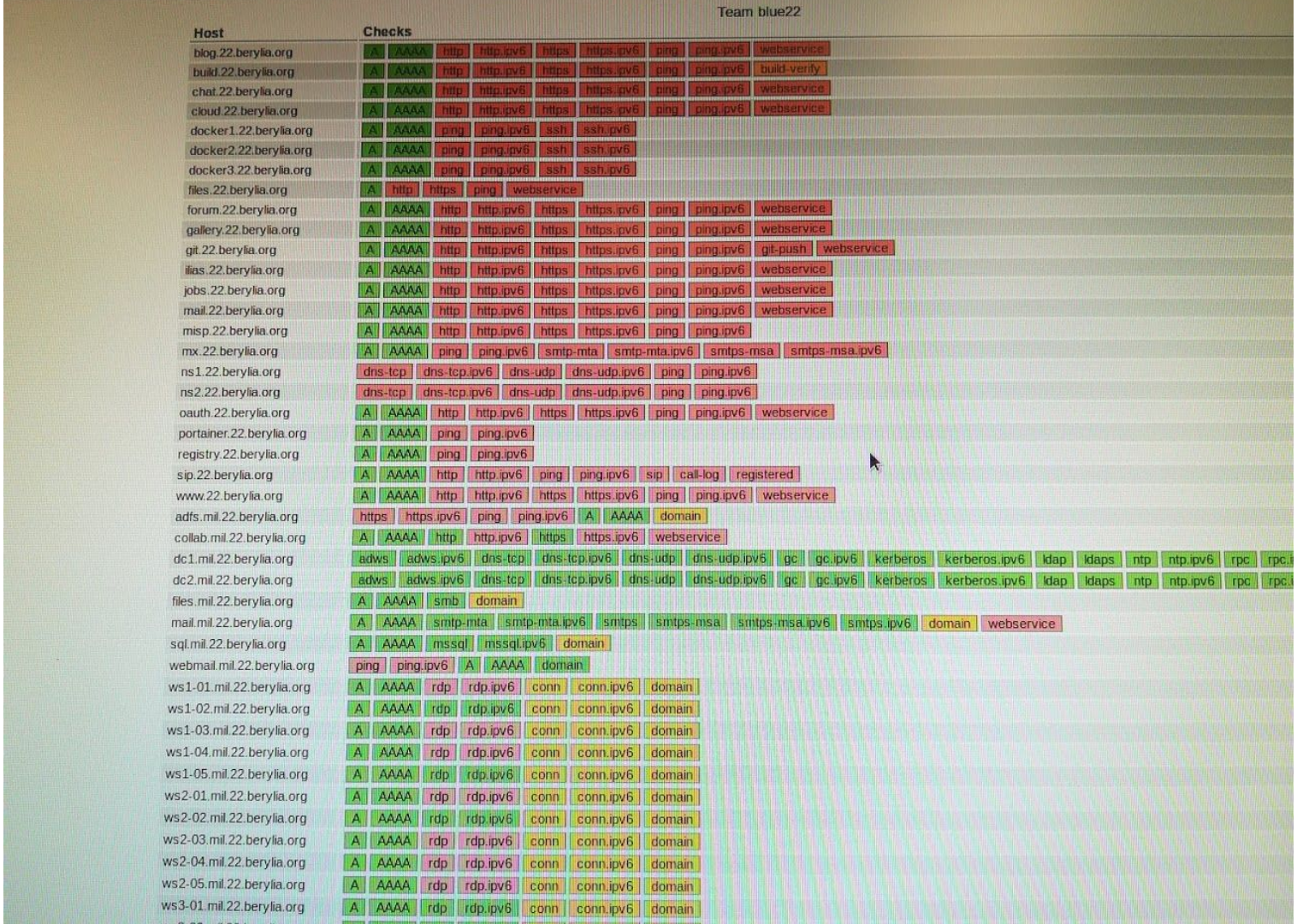
- Morning weather is extremely poor with limited visibility
- The supply ship Vigilance is carrying aid for Berylia
- The Vigilance collides with a Berylian merchant ship

- Investigation shows GPS signals were intermittent in the vicinity of the ships
- There is suspicion Crimsonia may have engaged in jamming the GPS signal

Day 2 - 11/04

Water Plant


BERYLIA IS FOR BERYLIANS....FOREIGN INVADERS MUST BE DRIVEN FROM OUR ISLAND!
Berylia is for Berylians....Foreign invaders must be driven from our Island!
NATO and advisers are criminals!


Team blue22
Host
Checks
blog.22.berylia.org A AAAA http http.ipv6 https https.ipv6 ping ping.ipv6 webservice
build.22.berylia.org A AAAA http http.ipv6 https https.ipv6 ping ping.ipv6 build-verify
chat.22.berylia.org A AAAA http http.ipv6 https https.ipv6 ping ping.ipv6 webservice
cloud.22.berylia.org A AAAA http http.ipv6 https https.ipv6 ping ping.ipv6 webservice
docker1.22.berylia.org A AAAA ping ping.ipv6 ssh ssh.ipv6
docker2.22.berylia.org A AAAA ping ping.ipv6 ssh ssh.ipv6
docker3.22.berylia.org A AAAA ping ping.ipv6 ssh ssh.ipv6
files.22.berylia.org A http https ping webservice
forum.22.berylia.org A AAAA http http.ipv6 https https.ipv6 ping ping.ipv6 webservice
gallery.22.berylia.org A AAAA http http.ipv6 https https.ipv6 ping ping.ipv6 webservice
git.22.berylia.org A AAAA http http.ipv6 https https.ipv6 ping ping.ipv6 git-push webservice
ilias.22.berylia.org A AAAA http http.ipv6 https https.ipv6 ping ping.ipv6 webservice
jobs.22.berylia.org A AAAA http http.ipv6 https https.ipv6 ping ping.ipv6 webservice
mail.22.berylia.org A AAAA http http.ipv6 https https.ipv6 ping ping.ipv6 webservice
misp.22.berylia.org A AAAA http http.ipv6 https https.ipv6 ping ping.ipv6
mx.22.berylia.org A AAAA ping ping.ipv6 smtp-mta smtp-mta.ipv6 smtps-msa smtps-msa.ipv6
ns1.22.berylia.org dns-tcp dns-tcp.ipv6 dns-udp dns-udp.ipv6 ping ping.ipv6
ns2.22.berylia.org dns-tcp dns-tcp.ipv6 dns-udp dns-udp.ipv6 ping ping.ipv6
oauth.22.berylia.org A AAAA http http.ipv6 https https.ipv6 ping ping.ipv6 webservice
portainer.22.berylia.org A AAAA ping ping.ipv6
registry.22.berylia.org A AAAA ping ping.ipv6
sip.22.berylia.org A AAAA http http.ipv6 ping ping.ipv6 sip call-log registered
www.22.berylia.org A AAAA http http.ipv6 https https.ipv6 ping ping.ipv6 webservice
adfs.mil.22.berylia.org https https.ipv6 ping ping.ipv6 A AAAA domain
collab.mil.22.berylia.org A AAAA http http.ipv6 https https.ipv6 webservice
dc1.mil.22.berylia.org adws adws.ipv6 dns-tcp dns-tcp.ipv6 dns-udp dns-udp.ipv6 gc gc.ipv6 kerberos kerberos.ipv6 ldap ldaps ntp ntp.ipv6 rpc
dc2.mil.22.berylia.org adws adws.ipv6 dns-tcp dns-tcp.ipv6 dns-udp dns-udp.ipv6 gc gc.ipv6 kerberos kerberos.ipv6 ldap ldaps ntp ntp.ipv6 rpc
files.mil.22.berylia.org A AAAA smb domain
mail.mil.22.berylia.org A AAAA smtp-mta smtp-mta.ipv6 smtps smtps-msa smtps-msa.ipv6 smtps.ipv6 domain webservice
sql.mil.22.berylia.org A AAAA mssql mssql.ipv6 domain
webmail.mil.22.berylia.org ping ping.ipv6 A AAAA domain
ws1-01.mil.22.berylia.org A AAAA rdp rdp.ipv6 conn conn.ipv6 domain
ws1-02.mil.22.berylia.org A AAAA rdp rdp.ipv6 conn conn.ipv6 domain
ws1-03.mil.22.berylia.org A AAAA rdp rdp.ipv6 conn conn.ipv6 domain
ws1-04.mil.22.berylia.org A AAAA rdp rdp.ipv6 conn conn.ipv6 domain
ws1-05.mil.22.berylia.org A AAAA rdp rdp.ipv6 conn conn.ipv6 domain
ws2-01.mil.22.berylia.org A AAAA rdp rdp.ipv6 conn conn.ipv6 domain
ws2-02.mil.22.berylia.org A AAAA rdp rdp.ipv6 conn conn.ipv6 domain
ws2-03.mil.22.berylia.org A AAAA rdp rdp.ipv6 conn conn.ipv6 domain
ws2-04.mil.22.berylia.org A AAAA rdp rdp.ipv6 conn conn.ipv6 domain
ws2-05.mil.22.berylia.org A AAAA rdp rdp.ipv6 conn conn.ipv6 domain
ws3-01.mil.22.berylia.org A AAAA rdp rdp.ipv6 conn conn.ipv6 domain

Lesson Learned

- The Incident Response process is more important than avoiding the incident
    - (which is mostly impossible, an incident WILL occur no matter what)
- Communication is key
- Having a trained team is better than having trained individuals

SERICS e ARTIC

Security and rights in the cyber space (SERICS)

- la fondazione SERICS, acronimo di “Security and rights in the cyber space”, è stata inaugurata Il 13 dicembre 2022
- un progetto avviato dall’Università di Salerno (HUB) per alimentare la ricerca nel campo della cybersecurity che coinvolge altri atenei, enti ed aziende
- SERICS riceverà 116,36 milioni di euro dal Ministero dell’Università e della Ricerca (MUR)
- la fondazione rientra in una strategia del MUR per assegnare 1,61 miliardi dei fondi europei del PNRR a ricerca di base e applicata

https://www.serics.eu

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

Spoke 4 e ARTIC

- 10 spoke tematici (https://serics.eu/spoke/)
- Spoke 4 “Sicurezza dei sistemi operativi e della virtualizzazione” è coordinato dall’Università di Genova e include 3 progetti
  - Project: Securing Containers (SecCo), PI: Alessio MERLO, Associate Professor, UNIGE
  - Project: Security in 5G and beyond (5Gsec), PI: Raffaele BOLLA, Full Professor, UNIGE
  - **Project: Affordable, Reusable and Truly Interoperable Cyber ranges (ARTIC), PI: Enrico RUSSO, Assistant Professor, UNIGE**

Contesto e sfide aperte

I **Cyber Range** (CR) rappresentano **asset strategici** per la cybersecurity*

- ✔ Secondo Gartner, entro il 2022, il 15% delle **grandi aziende** li utilizzerà per **sviluppare le competenze** dei propri team di sicurezza
- ✔ Possono essere utilizzati per **molti scopi** e si sono adeguati nel corso degli anni ai **cambiamenti tecnologici**
- ✔ È complesso e costoso che un CR sia in grado di fornire tutte le capacità richieste: più CR, ciascuno con la sua area di specializzazione, devono poter **lavorare insieme**

- ✔ L'uso dei CR conferma un **trend positivo e rapido** ma evidenzia che sono generalmente convenienti e disponibili solo per le **grandi organizzazioni**
- ✔ I CR sono in continua evoluzione: è necessario supportare **nuovi domini di sicurezza** informatica, integrare **nuove tecnologie** o sfruttare le loro capacità in **nuove aree di applicazione**
- ✔ La **cooperazione** tra CR è un requisito fondamentale

SERI SECURITY AND RIGHTS IN TI

*European Cyber Security Organization (ECSO). "Understanding Cyber Ranges: From Hype to Reality." Brussels, Belgium: ECS, 2020

Obiettivi

Ridurre i costi tecnologici e di gestione, i requisiti infrastrutturali e il personale richiesto

Supportare **nuovi domini cyber** (ad es., AI security, sistemi cyberfisici navali o 5G) e scenari cross-dominio

Identificare **nuove tecnologie abilitanti** (ad es. Digital Twins)

Identificare **nuove aree di applicazione** (ad es. Honeypot o Sandbox)

Promuovere la **cooperazione** attraverso l'interoperabilità e la federazione

Attività

Tecniche e strumenti per la progettazione, verifica, test di scenari e runtime injections **UNIGE CINI IMT LEONARDO**	Tecnologie di orchestrazione e virtualizzazione *affordable* **BaC**	Integrare le capacità dei Digital Twins **UNICAL**	Strumenti AI per la sicurezza informatica e Adversarial Machine Learning **UNIGE**	Fake news e campagne di disinformazione **IMT**	Scenari *Hardware-Based* **CINI**	Scenari relativi alle infrastrutture critiche **BaC Fincantieri**
WP1 - Framework per Cyber Ranges			**WP2** - Nuovi domini cyber e aree di applicazione			
Testbed per i progetti dello SPOKE						

Risultati Attesi

- **R1. ARTIC Framework** per design e deployment di CR
  - aperto e rilasciato pubblicamente alla comunità
  - generale
  - sostenibile e scalabile
- **R2. Standards for operation:** Regole e soluzioni di *interoperabilità*
  - design di scenari
  - simulazione di attività utente e attacchi
  - scoring e reporting
- **R3. Cross-domain scenario**
  - inclusivo di diversi elementi e caratteristiche di infrastrutture critiche
  - supportato da tecnologie allo stato dell'arte (ad es. Digital Twins)