
CYBER DEFENCE PROJECTS
CD SDP 2016
28 April
INTERNATIONAL CONFERENCE
LISBON, Portugal
MULTINATIONAL
Malware Information
Sharing Platform (MIS
MULTINATIONA
MN CD2 - Cyber Defe
Capability Developm
MN CD E&T
NATO SMART DEFENCE

Multinational Cyber Defense Education & Trainning Cyberlab

PORTUGAL

Military Academy, Lisbon, 28 April 2016

Marcio Silva Santos
marcio.silva.santos@novabase.pt

Agenda

1 – Strategic Objectives

2 – What is

3 – Technical Objectives

4 - Organogram

5 - Cyberdefense - Lifecycle

6 - Teams

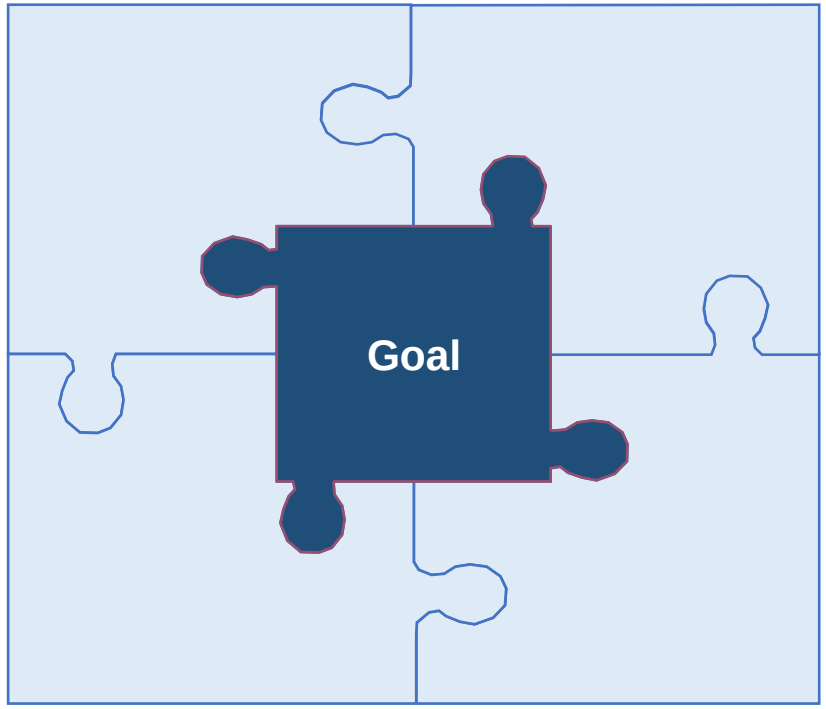
7 - Architecture

8 - Infrastructure

9 - Equipment

10 - Chronogram

Strategic Objectives



“Develop a simulator for activities and operations at Cyberspace (Cyberlab)”

Provide a way to grow the knowledges of cybersecurity teams to increase the ability in responding to complex attacks

MNCDE&T – Cyberlab

What is

The Cyberlab is a cybersecurity and cyberdefense simulation environment

It can replicate real configurations in a controlled scenario

It was designed to create and simulate tests for educational purposes

It is multifunctional and modular

What is not

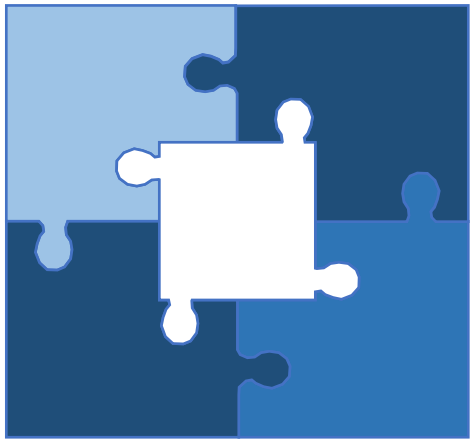
It was not designed to be part of a production environment

It was not developed to work out of a controlled environment

It is not a platform to test real systems

It is not dispensed of updated and reviews

Technical Objectives

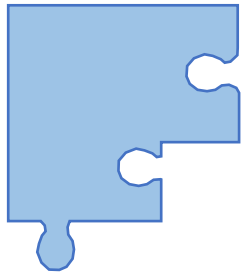


Servers to host virtual systems

Network LAN and WAN into a controlled environment

Central e Unified Management

Technical Objectives



Operational

- Traffic
- Events
- Logging
- Access Control
- Virtualization
- Networking
- Connectivity

Tactical

- Trainning
- Testing
- Analisys
- Monitoring

Teams

Blue Team: The defense line

- Traffic Capture
- Monitoring
- Logging
- SIEM

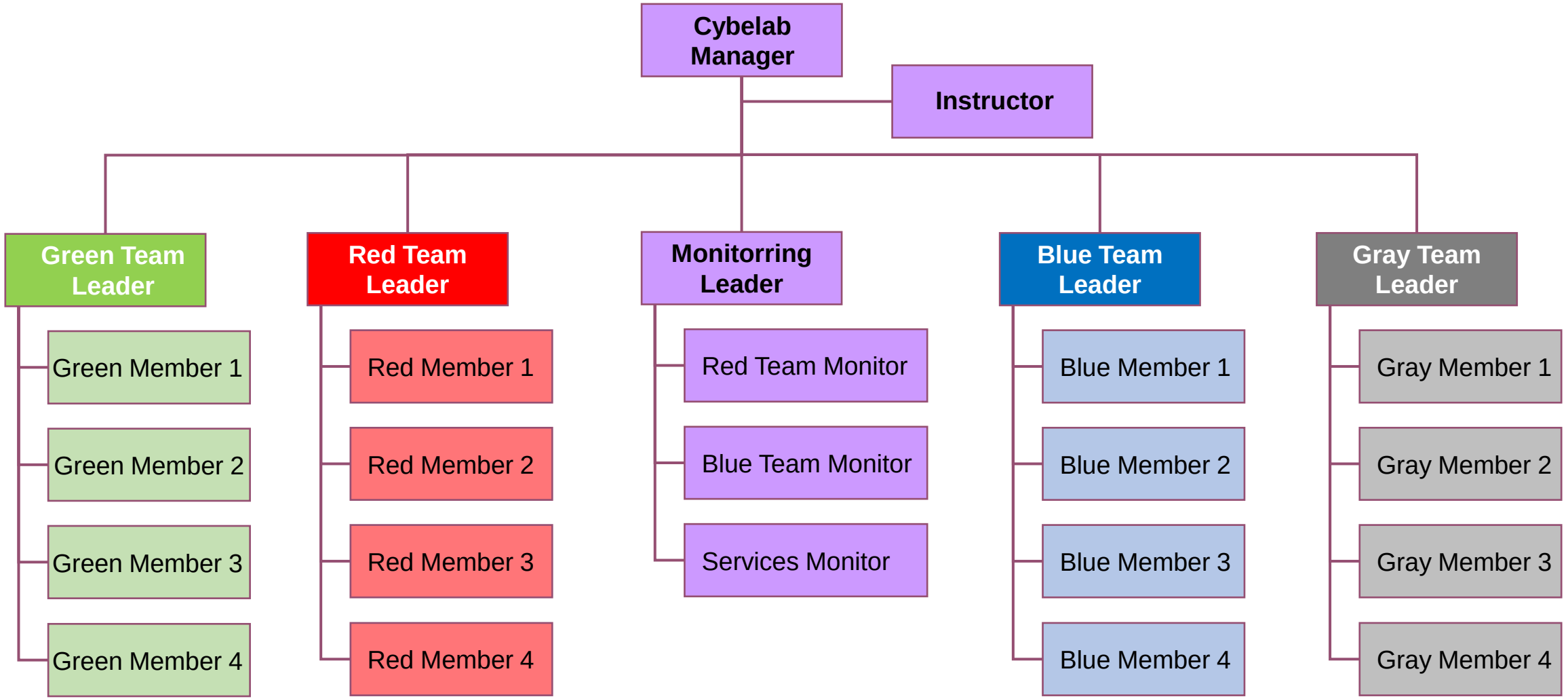
Red Team: The attack line

- Traffic Capture
- Scripting
- Denial of Service

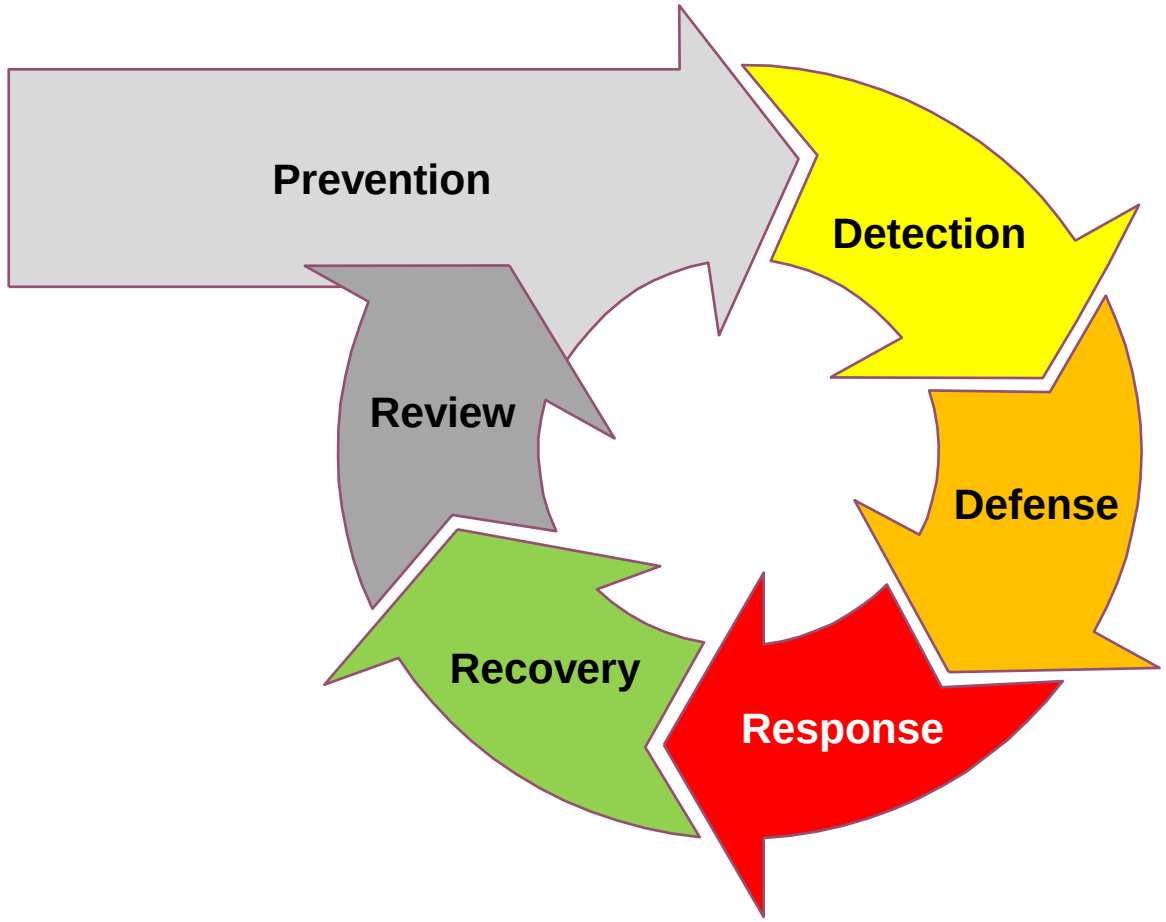
Monitor: Management

- Server Console
- Networking Monitor
- Traffic Capture
- Logging
- SIEM

Organogram Cybelab - Operational



Cyberdefense - Lifecycle



Prevention
Known vulnerabilities, mitigation, workaround

Detection
Monitoring, malicious and unauthorized access

Defense
Grant accesses and services

Response
Reaction, block

Recovery
Data and services restore

Review
Event analysis, new processes and prevention schema

Architecture

War

Provide an access infrastructure to the cyberlab

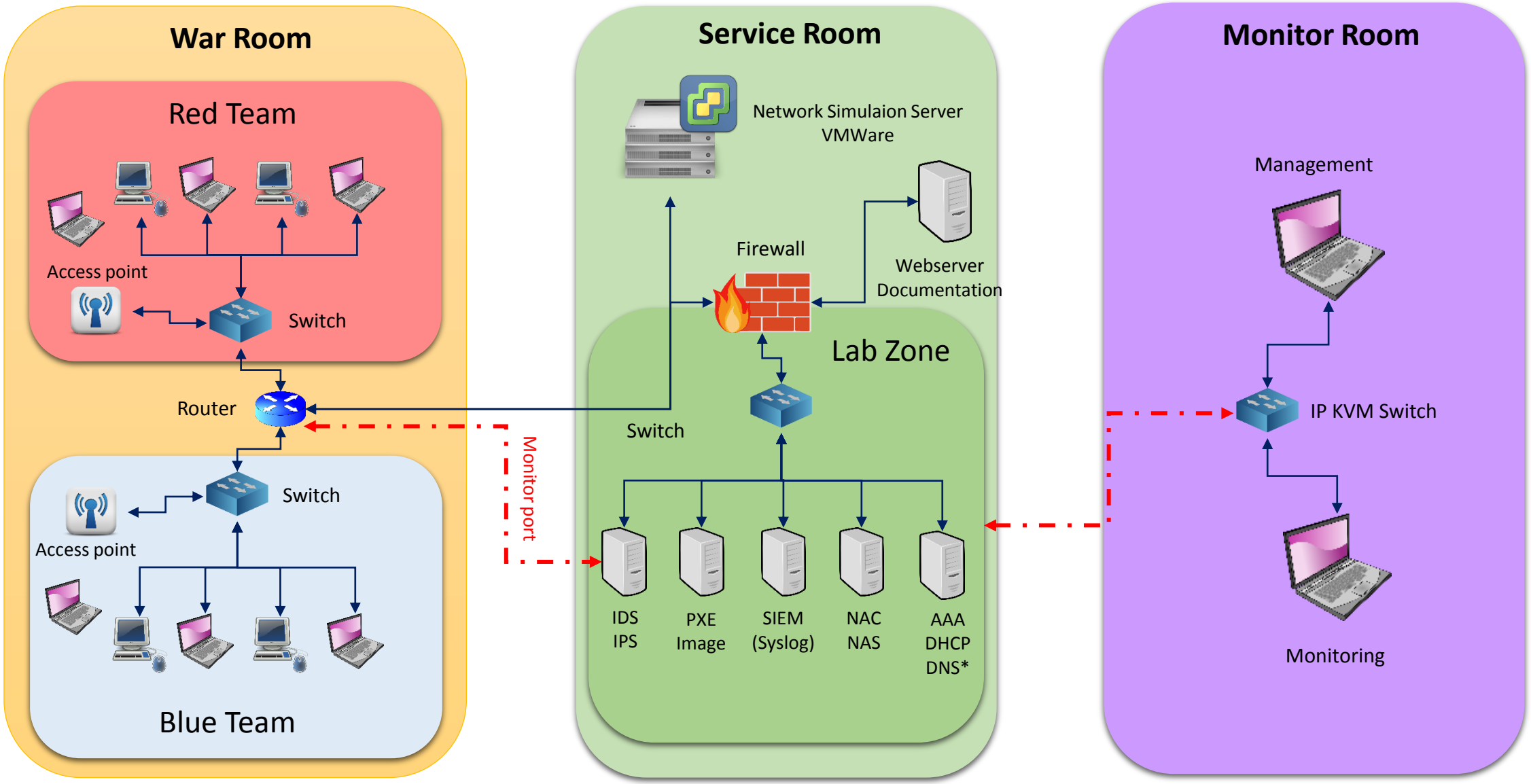
Service

Servers and security appliances

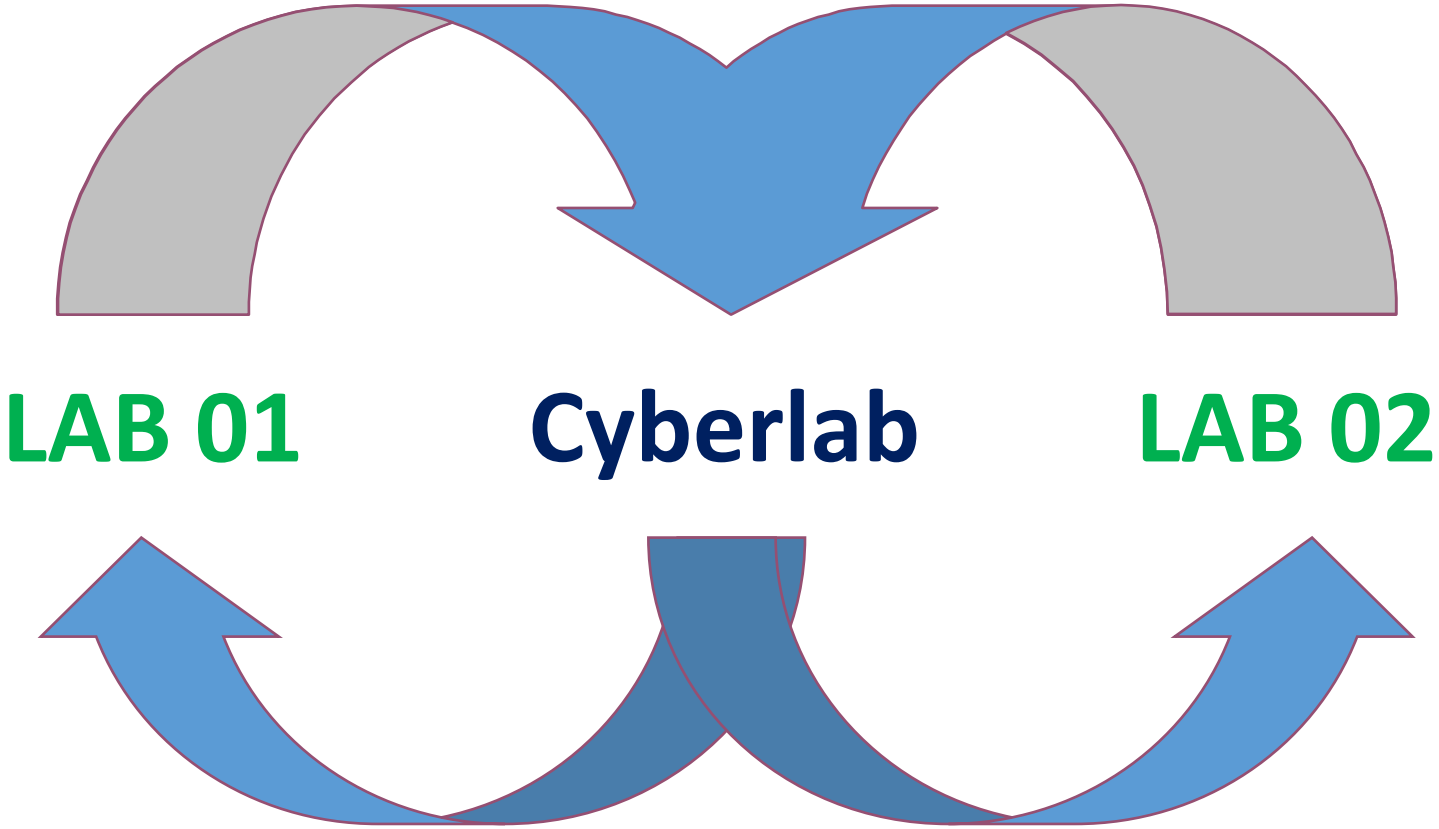
Monitor

Command and Control

Architecture



Architecture



The architecture was designed to permit an integration with other simulation environments.

It will permit the Cyberlab to be part of another context of tests and also provide interfaces to external platforms.

Infrastructure

War Room

Switch - Catalyst 3750X 24 Port PoE IP Services
Access Point - Cisco Aironet 1832i
Router - Cisco 4000 Series

A replicated infrastructure for Red and Blue Teams

Infrastructure

Services Room

Server - Cisco M4308
Switch - Catalyst 3750X 24 Port PoE IP Services
Host Operational System - VMware ESXi
Guests OS - Windows Server 2012 and Linux (RedHat/CentOS/Suse/Debian)
Firewall - Cisco ASA – Adaptive Security Appliance
Firewall – Palo Alto – PA3060

Infrastructure

Networking Equipment List*

Item	Descrição	Quantidade
Switch	Catalyst 3750X 24 Port PoE IP Services	3
	Catalyst 3K-X 715W AC Power Supply	3
	Catalyst 3K-X Network Module Blank	3
	Catalyst 3K-X Power Supply Blank	3
	CAT 3750X IOS Universal with web base dev mgr	3
Router	Cisco ISR 4300 Series IOS XE Universal	1
	AC Power Cord (Europe), C13, CEE 7, 1.5M	1
	4-port Layer 2 GE Switch Network Interface Module	1
	Cisco ISR 4331 Sec bundle w/SEC license	1
Access Point	Cisco Aironet 1832i	2
Firewall*	ASA 5525-X with SW, 8GE Data, 1GE Mgmt, AC, DES	1
	ASA 5525-X Botnet Traffic Filter License for 1 Year	1
	ASA 5500 20 Security Contexts License	1
	AC Power Cord (Europe), C13, CEE 7, 1.5M	1
	ASA 5500 UC Proxy 50 Session License	1
Firewall*	Fortigate 100D	1
Firewall*	Palo Alto Networks NGFW	1
Servidor	UCS C220 M3	1
	16GB DDR3-1866-MHz RDIMM/PC3-14900	6
	1TB 6Gb SATA 7.2K RPM SFF HDD/hot plug	4
	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	2
Switch IP KVM	1 Analog Console Port + 4 Users, 16 Servers	1

*Review

Chronogram


Month 1
Month 2
Month 3
Task
1
2
3
4
1
2
3
4
1
2
3
4
Kick-off
Cabling + hack
Services Room
Operational Systems
Services + Applications
Monitor Room
Workstations
Switch KVM
War Room
Router
Red Team
Switching
Wireless
Workstations
Blue Team
Switching
Wireless
Workstations
Testing + Comissioning

Thank you

Marcio Silva Santos
marcio.silva.santos@novabase.pt