دائـــرة الـتـمـكـــيـن الـحـــكـــومـــي
DEPARTMENT OF GOVERNMENT ENABLEMENT

CYBER HACKATHON
{Battle of the Elite};

Cyber Hackathon
Battle of the Elite

Exercise Book

CybExer

paloalto NETWORKS

CyberGate AN IHC COMPANY

Table of Contents

Introduction

Department of Government Enablement together with CybExer, CyberGate and PaloAlto will organize cyber hackathon event as a four-day cybersecurity battle of the elite on 14-17 October 2024. During this event the participating team skills will be tested in a Live-Fire exercise on a simulated IT Infrastructure with ongoing cyberattacks.

The Battle of the Elite is an excellent opportunity for technical cyber defence specialists to cooperate with each other and to test their methodology and skills of detection and response to cyberattacks that will be launched on their IT infrastructure. Multiple teams will participate in the event and cooperate with each other to detect attacks against their IT infrastructure performed by a real-life adversary team. Participating in this event is an excellent way to test and develop the skills in handling incidents by means of detection of cyber attacks, defending and hardening your infrastructure, providing situational awareness, reporting and cooperating with other teams.

During the hackathon teams will also have the chance to solve additional tasks as Capture the Flag format, where participants are faced with several tasks that need to be solved by employing various cybersecurity skills to find clearly defined answers. As the name suggests, the expected answer can be nothing more than a simple “flag” that has no meaning of its own but is just a proof that a participant has been able to reach the desired goal. Participants are also presented with hints to help progress through the task.

The present document describes the event concept, objectives, scenario, control and communication channels, required target audience experience, agenda and systems used during the event.

The “Exercise book” document covers the following topics:

- Introduction
- Hackathon Schedule and Time Plan
- Hackathon Concept & Objectives
- Technical Requirements for Participation
- Overview of the phases
- Hackathon Control and Communication Channels
- Gamenet Description
- Hackathon Rules
- Hackathon Scoring
- Integrated Scoring and Awareness System (ISA) Usage Instructions

Training Schedule & Time Plan

All times are in Dubai Time (GMT+4)

Day 1 (0930 – 1700) MONDAY	
09:30 – 10:00	Registration
10:00 – 12:00	Familiarization Training and Briefing
12:00 – 16:30	Hands-on Preparational Training • Verifying access to Cyber Range Platform tools – visualization & scoring system, documentation, reporting & task submission, green team ticketing system, virtual machine access • Verifying access to communication & cooperation tools – chat, malware information sharing platform (MISP) • Planning team strategy and tactics – divide roles, assign responsibilities & systems
16:30 – 17:00	End of day feedback & QA
Day 2 (0930 - 1700) TUESDAY	
09:30 – 10:00	Registration
10:00 – 16:30	Start of Threat Hunting Exercise Blue Teams must monitor the environment for detecting Red Team attacks and perform post attack investigations on Red Team activities. There is no focus on system hardening and other general defensive tasks.
10:00 – 16:30	Capture the Flag (CTF) Tasks
15:30	Deadline for Blue Team Situation Report I (SITREP I)
16:30	Endex of Threat Hunting
16:30 – 17:00	End of day feedback & QA
Day 3 (0930 - 1700) WEDNESDAY	
09:30 – 10:00	Registration

10:00 – 16:30	Start of Live-Fire Exercise Blue Teams need to keep monitoring and detecting Red Team attacks, but focus is now on defending and hardening of the environment
10:00 – 16:30	Capture the Flag (CTF) Tasks
15:30	Deadline for Blue Team Situation Report II (SITREP II)
16:30	Endex of Threat Hunting
16:30 – 17:00	End of day feedback & QA
Day 4 (0930 - TBD) THURSDAY	
09:30 – 10:00	Registration
10:00 – 12:00	Live-Fire continues
10:00 – 12:00	Capture the Flag (CTF) Tasks
10:00 – 12:00	Start of Hack back
11:30	Deadline for Blue Team Situation Report III (SITREP III)
TBD	Award ceremony & Hotwash Session: • Red Team campaign overview • Exercise Mamagement Team feedback session • Open Discussion

Cyber Hackathon Overview

Roles

The Cyber Hackathon roles are divided between the following teams:

Exercise Management (White Team) - Responsible for overall leading and controlling of the Hackathon. The White Team consists of experts responsible for overall exercise flow, scoring, end-user simulation etc

Participating Team (Blue Team) - Participants in the Hackathon who improve their skills. From the game point of view the Blue Teams acts as the "good guys" who must monitor their networks and detect/defend attacks conducted against them.

Adversary Team (Red Team) - Responsible for conducting offensive activities against the infrastructure that the Blue Team must monitor and defend. From the game point of view, they are the "bad guys".

Infrastructure Support (Green Team) - Responsible for the Cyber Range and Gamenet infrastructure during the Hackathon and will provide technical support to Blue Teams for accessing the Cyber Range and Blue Team infrastructure services necessary for the exercise.

Roles of the Blue Team Members

The following roles should be divided between the blue team members during the Hackathon:

Leadership (Manager / SOC Team Lead)	The team should have a leader who can guide them and coordinate efforts with other parties when needed.
Reporting and Cooperation	The team needs to investigate and document incidents that happen in systems under team's responsibility and use appropriate cooperation tools to share information with other teams. Additionally, the team shall compose situation reports for executive leadership or other parties that may include key findings, monitoring and incident summaries, threat assessments and recommendations.

System and Network Administration	System and network administration skills to handle incidents in technical domains (e.g., Unix based routers and firewalls, Windows & Unix based IT systems, commonly used web platforms like WordPress, Drupal)
Computer Network Defence	The team shall monitor, detect, analyse and report security incidents. They should have experience with common security and cooperation tools such as Arkime/Moloch, Security Onion, MISP.

Blue Team and Red Team Activities During the Hackathon

Activities by the Blue Team:

- Solving tasks about various incidents happening on the Gamenet
- Detecting and preventing of attacks;
- Either using pre-configured monitoring tools or deploying their own to detect Red Team attacks;
- Investigating & handling cyber incidents;
- Reporting & cooperating with other teams;
- Optional activities:
    - Scanning & searching vulnerabilities from their own infrastructure;
    - Planning technical defenses against Red Team attacks;
    - Hacking back on specified time.

Activities that can be undertaken by the Red Team:

- Conducting attacks against web applications, network services and end user workstations;
- Performing DoS attacks against various services;
- Installing various backdoors and using other methods for persistence;
- Deleting logs and hiding their activities;
- Conducting attacks against Active Directory domain;
- Exfiltrating sensitive information;
- Disruption of simulated critical infrastructure operations.

Computer Requirements for Participation

Blue Team members will use their own computers to participate at the Hackathon. All common workstation operating systems like Windows, Linux and macOS can be used. It is preferable that blue teams have full administrative access to their workstation. If administrative access is not possible, then blue team workstation should meet the following minimum requirements:

1. OS: MS Windows 10 x64 (or newer), GNU/Linux Ubuntu 18.04 x64 desktop (or newer) or macOS 11 (or newer)
2. CPU: Intel i5 or equivalent (recommended – Intel i7 or equivalent), Apple M1 or newer
3. HDD: 50 GB of free space (recommended SSD based storage)
4. RAM: 8GB (recommended - 16GB)
5. NIC: physical or dongle based RJ45 10/1000 (If no other option, then WiFi adapter will also work)
6. Ability to use the internet
7. Ability to use workstation without active connections to corporate network (always on VPN, Active Directory, web proxy etc.) – 10.0.0.0/8 network will be routed to cyber range
8. Ability to use Chrome or Firefox web browser
9. Ability to accept self-signed SSL certificates
10. Ability to connect to non standard ports with web-browsers
11. Have SSH and SCP software installed
12. Have Remote Desktop Protocol (RDP) client software installed

Additional Notes

Please note that the whole 10.0.0.0/8 private IP address space is routed over VPN to cyber range. There is a big chance that blue team internal corporate IT resources (AD domain controllers, DNS, web proxies, file servers, intranet sites etc.) will fall into the same range and thus cannot be used while connection to Cyber Range is active. Computers used by hackathon participants should be configured in a way that they do not need active access to internal IT resources to be usable.

Threat Hunting Overview

Threat Hunting mode is a technical task driven response & investigation collaborative effort designed for practicing response to a cyber crisis according to pre-defined scenario.

The digital threat environment (Gamenet) is hosted on CybExer Cyber Range and it will be played on a specially configured Gamenet. The Gamenet provided for the participating teams (Blue Teams) is insecure and contains several vulnerabilities that will be actively exploited by the adversary team (Red Team). Blue teams must monitor the environment for detecting red team attacks and also perform post attack investigations and reporting on red team activities.

There will be friendly competition between blue teams - score is awarded for solving incidents by providing relevant details about attacks. Composing accurate situation reports will also result in awarded positive points. Additional bonus points can be gained from cooperation initiatives among blue teams mostly related on sharing helpful information via Malware and Information Sharing Platform (MISP).

Provided Gamenet represents generic IT organization. Besides regular business IT systems it includes a fully virtualized CCTV control room that is used to manage security monitoring cameras and SCADA system that is used for Energy Company control room

Please note that systems hardening, patching and other defense activities that would technically interfere or mitigate Red Team attacks are not in the scope of this exercise. Implementing such defenses could impact teams' ability to solve tasks and conduct post incident investigation.

The goal of the Threat Hunting activities is to improve skills and prepare the participants in following areas:

- Detection of attacks and reporting;
- Providing situational awareness;
- Handling cyber incidents;
- Cooperation between the blue teams;
- Teamwork: delegation, dividing and assigning roles, leadership.

Live-Fire Overview

Live-fire mode is a deep, technical Red vs Blue battle designed for practicing response to a cyber crisis according to a realistic pre-defined scenario. The main goal of the scenario is to give the participants a realistic experience in defending IT-systems under intense cyber-attacks. The structures and environments used are standardized and, in addition to providing effective training experience, the scenarios have been designed to allow scoring, benchmarking and effective data capture.

The goal of the exercise is to provide the participants a standardized gamenet environment that would allow fair scoring, as well as be comprehensive and manageable by the blue teams and not to simulate precise structures and environments of specific real-world organizations.

The goal of the live-fire battle is to improve skills of the participants in following areas:

- Detection and Prevention of attacks
- Network monitoring
- Situational awareness and control
- Handling cyber incidents
- Teamwork: delegation, dividing and assigning roles, leadership
- Reporting for higher level managers
- Reporting in Threat sharing platform MISP

Capture the Flag Overview

Capture the Flag (CTF) mode is designed to provide cybersecurity specialists with a foundational understanding of offensive techniques in cyber operations. The tasks included focus on real-world scenarios that showcase common vulnerabilities and attack methods. Participants will gain hands-on experience in areas such as website reconnaissance, SQL injection, buffer overflows, network traffic analysis, and cryptoanalysis.

The tasks also emphasize the importance of understanding risks like unsanitized input, outdated software, unencrypted connections, and how attackers exploit these weaknesses. By practicing these techniques, participants will sharpen their skills in areas like reverse engineering, steganography, exploitation of well-known vulnerabilities, and more.

Exercise Control and Communication Channels

Full accesses to training control and communication channels will be given to all Blue Teams on the day 1 of the hackathon.

Collaborative Training Ticketing & Green Team Support System

URL: https://support.cybexer.com/

Ticketing system is meant to let organizers know about the infrastructure problems in the game network or if there are issues with the connection to the gamenet. Use “Technical Exercises” category to submit new tickets. Make sure to include your team number and use real-world functional e-mail address. Ticket updates and responses will be sent to this email.

Integrated Scoring and Situational Awareness System (ISA)

URL: https://isa.i3.cybexer.io/

Integrated Scoring and Situational Awareness System (ISA) is a tool that provides information for the Blue Teams about scoring and organizers how the training is going. Blue Teams will receive their tasks and will provide answers to the tasks via ISA. ISA is also used for submitting situation reports.

ISA also provides Blue Teams access to virtual machine consoles and allows them to perform limited operations with VM-s – revert to snapshot.

More information how to use the system can be found from Annex I - Integrated Scoring and Awareness System (ISA) Usage Instructions.

Details and requirements on how to write Situation Reports can be found from Annex II - Situation Reporting Instructions.

Also, example of very good SITREP is included in Annex III - Example of Good SITREP.

Technical Documentation

URL: https://collab.i3.cybexer.io/

This site is used to host technical information regarding Blue Team systems, gamenet system's access credentials and Blue Team rules.

Chat Server

URL: https://chat.i3.cybexer.io/

Chat server is the main communication channel between Blue Teams and training organizers. There are dedicated chat rooms for each blue team so this chat server can be used for team internal communications too. Chat service is based on Rocket.Chat and it has web based and desktop clients available.

MISP Servers

URL: https://misp.i3.cybexer.io/

MISP servers can be used by the participants for cooperation purposes - to share technical information about incidents etc.

Description of The Gamenet

The Gamenet represents generic IT organization and consist of about 55 different virtual machines. Blue teams have full administrative access to all the systems. The following network segments are used:

- **Routing Services (WAN)** – Upstream routers of the environment
- **Demilitarized Zone (DMZ)** - DMZ hosts internet facing publicly available services of the Blue Team.
- **Internal Servers Segment (SRV)** – Internal office network servers and services
- **Internal Office Segment (INT)** - INT or internal office network hosts Blue Team end user workstations.
- **Security and Monitoring Segment (SEC)** - SEC host various security tools that the Blue Teams can use for monitoring purposes.
- **WiFi Segment (WiFi)** - This network segment should be considered as guest WiFi network. Hosts inside WiFi network are not under the Blue Team management.
- **Security Monitoring Network (SM)** - This network segment hosts Security monitoring cameras (CCTV) and recorder system.
- **Critical Infrastructure Control Center (CI**) - This network segment hosts Energy Company control room related systems that are used to manage energy distribution network.
- **Business Services (BUSINESS-SRV)** – Hosts company business services, running on Kubernetes.
- **Azure Cloud -** hosts one different Azure services which are managed by Blue Team

In addition to above, every blue team environment is connected to the Gamenet Simulated Internet. Various support systems and malicious parties are located in Simulated Internet segment.

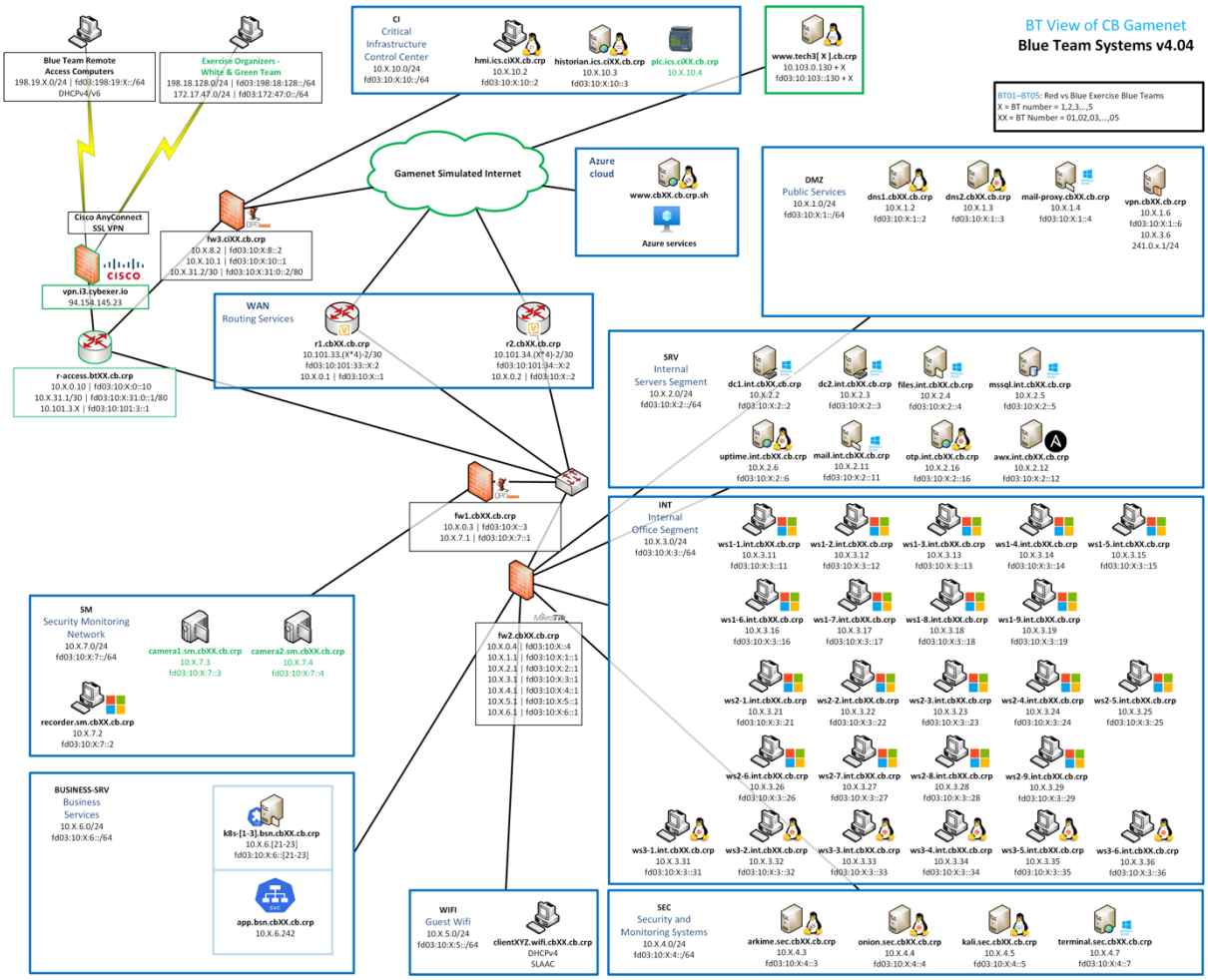
Gamenet Access

Preferred way to access Gamenet Systems is using operating system native management protocols (RDP, SSH, web ui etc.) and connecting directly to hosts IP number or DNS name. In some cases, blue teams might require access to VMs consoles, perform revert to snapshot operations. This can be done using ISA.

Network Diagram

X or XX in IP numbers and DNS names refers to blue team number.

- X = Blue Team Number = 1,2,3 etc.
- XX = Blue Team Number = 01,02,03 etc.



List of Blue Team Managed Gamenet Systems

X or XX in IP numbers and DNS names refers to blue team number.

- X = Blue Team Number = 1,2,3 etc.
- XX = Blue Team Number = 01,02,03 etc.

Routing & Firewall VMs

Hostname	**IP**	**IPv6**	**Description**	**Required Services**
r1.cbXX.cb.crp	10.103.33.(X*4)-2/30; 10.X.0.1	fd03:10:103:33::X:2; fd03:10:X::1	VyOS router #1	SSH (TCP 22); BGP (TCP 179); OSPF
Additional Details:	• **OS**:: VyOS • BGP on WAN side • OSPF on LAN side • Administration is done over ssh or from console. • Authentication is done against DC1. User administrator has full administrative rights. • Local administrator username is admin			
r2.cbXX.cb.crp	10.103.34.(X*4)-2/30; 10.X.0.2	fd03:10:103:34::X:2; fd03:10:X::2	VyOS router #2	SSH (TCP 22); BGP (TCP 179); OSPF
Additional Details:	• **OS**:: VyOS • BGP on WAN side • OSPF on LAN side • Administrations is done over ssh or from console. • Authentication is done against DC1. User administrator has full administrative rights. • Local administrator username is admin			

fw2.cbXX.cb.crp	10.X.0.4; 10.X.1.1; 10.X.2.1; 10.X.3.1; 10.X.4.1; 10.X.5.1; 10.X.6.1	fd03:10:X::4; fd03:10:X:1::1; fd03:10:X:2::1; fd03:10:X:3::1; fd03:10:X:4::1; fd03:10:X:5::1; fd03:10:X:6::1	MikroTik firewall	SSH (TCP 22); HTTP (TCP 80); OSPF
Additional Details:	• **OS**:: MikroTik RouterOS • OSPF on WAN side • Administration GUI: http://10.X.0.4/ • Local administrator username is admin			
fw1.cbXX.cb.crp	10.X.0.3; 10.X.7.1;	fd03:10:X:0::3, fd03:10:X:7::1	OPNsense firewall	SSH (TCP 22); HTTPS (TCP 443); OSPF
Additional Details:	• **OS**:: OPNsense • OSPF on WAN side • Administration GUI: https://10.X.0.3/ • Local administrator username is root • Authentication is done against DC1. User “Administrator” has full administrative rights.			
fw3.ciXX.cb.crp	10.X.8.2; 10.X.10.1; 10.X.31.2/30	fd64:10:X:31:0::2/80 ; fd64:10:X:10::1, fd64:10:X:8::2	OPNsense firewall	SSH (TCP 22); HTTPS (TCP 443); OSPF
Additional Details:	• **OS**:: OPNsense • OSPF on WAN side • Administration GUI: https://10.X.8.2			

DMZ Zone VMs

Hostname	**IP**	**IPv6**	**Description**	**Required Services**
dns1.cbXX.cb.crp	10.X.1.2	fd03:10:X:1::2	Authoritative master & recursive DNS server based on PowerDNS	SSH (TCP 22); DNS (UDP 53); DNS (TCP 53); HTTP (TCP 80); HTTPS (TCP 443)
Additional Details:	• **OS**:: CentOS • Administration GUI: http://dns1.cbXX.cb.crp • Operating system and web GUI authentication is done against DC1. User “Administrator” has full administrative rights.			
dns2.cbXX.cb.crp	10.X.1.3	fd03:10:X:1::3	Authoritative slave & recursive DNS server based on PowerDNS	SSH (TCP 22); DNS (UDP 53); DNS (TCP 53)
Additional Details:	• **OS**:: Ubuntu 18 • Operating system user authentication is done against DC1. User “Administrator” has full administrative rights.			
mail-proxy.cbXX.cb.crp	10.X.1.4	fd03:10:X:1::4	Email proxy for SMTP located in DMZ	IMAP/s (TCP 143,993); SMTP (TCP 25); HTTP (TCP 80); HTTPS (TCP 443)
Additional Details:	• Provides email transport with headers rewriting according to microsoft design guidelines.			
vpn.cbXX.cb.crp	10.X.1.6; 10.X.3.6; 241.0.X.1/24	fd03:10:X:1::6	CB Organization OpenVPN based VPN server for remote access	SSH (TCP 22); HTTPS (TCP 443); VPN (UDP 1194)

Additional Details:	• **OS**:: OpenVPN Access Server (Ubuntu 18) • Administration GUI: http://10.X.1.6/admin/ • Authentication is done against DC1. User "Administrator" has full administrative rights. • Local ssh username: root • Regular user Access: • Open https://vpn.cbXX.cb.crp and login with your INT Active Directory credentials. You can download suitable OpenVPN client (supported OSX, Windows, Linux) after login.

SRV Zone VMs

Hostname	**IP**	**IPv6**	**Description**	**Required Services**
dc1.int.cbXX.cb.crp	10.X.2.2	fd03:10:X:2::2	Primary domain controller for INT domain	AD DS Web (TCP: 9389); DFS (UDP: 138); DNS (TCP: 53; UDP: 53); Kerberos (TCP: 88; UDP: 88; TCP: 464; UDP: 464); LDAP (TCP: 389; UDP: 389); LDAP GC (TCP: 3268); LDAP GC SSL (TCP: 3269); LDAP SSL (TCP: 636); NTP (UDP: 123); NetBIOS (TCP: 139); NetBIOS (UDP: 137); RDP (TCP: 3389); RPC (TCP 135); SMB (TCP: 445; UDP: 445); File Replication (TCP: 5722)
Additional Details:	• **OS**:: Windows Server 2016			

dc2.int.cbXX.cb.crp	10.X.2.3	fd03:10:X:2::3	Secondary domain controller for INT domain	AD DS Web (TCP: 9389); DFS (UDP: 138); DNS (TCP: 53; UDP: 53); Kerberos (TCP: 88; UDP: 88; TCP: 464; UDP: 464); LDAP (TCP: 389; UDP: 389); LDAP GC (TCP: 3268); LDAP GC SSL (TCP: 3269); LDAP SSL (TCP: 636); NTP (UDP: 123); NetBIOS (TCP: 139); NetBIOS (UDP: 137); RDP (TCP: 3389); RPC (TCP 135); SMB (TCP: 445; UDP: 445); File Replication (TCP: 5722)
Additional Details:	• **OS**:: Windows Server 2016 Core			
files.int.cbXX.cb.crp	10.X.2.4	fd03:10:X:2::4	INT domain file server	SMB (TCP: 445); RDP (TCP: 3389)
Additional Details:	• **OS**:: Windows Server 2016 Core			
mssql.int.cbXX.cb.crp	10.X.2.5	fd03:10:X:2::5	SQL Server for various web applications	SSH (TCP 22); RDP(3389)
Additional Details:	• MSSQL provides database services for the INT segment.			

uptime.int.cbXX.cb.crp	10.X.2.6	fd03:10:X:2::6	Uptime based monitoring server	SSH (TCP 22); HTTP (TCP 80); HTTPS (TCP 443)
Additional Details:	• Uptime monitoring server which monitors different services			
awx.int.cbXX.cb.crp	10.X.2.12	fd03:10:X:2::12	Ansible control node to manage IT infrastucture.	SSH (TCP 22); HTTP (TCP 80); HTTPS (TCP 443)
Additional Details:	• **OS**:: Ubuntu • Ansible AWX is Ansible Tower based open-source Ansible user interface			
mail.int.cbXX.cb.crp	10.X.2.11	fd03:10:X:2::11	Microsoft Exchange mail service	SMB (TCP: 445); RDP (TCP: 3389); HTTPS (TCP: 443); SMTP (TCP: 25)
Additional Details:	• Microsoft Exchange 2019 running on Windows Server 2019 GUI. • Provides mail, calendar services for INT segment users. • Webmail service: https://mail.int.cbXX.cb.crp/ • Exchange Control Panel: https://mail.int.cbXX.cb.crp/ecp			
otp.int.cbXX.cb.crp	10.X.2.16	fd03:10:X:2::16	OpenOTP Authenticatio n server	SSH(TCP: 22); HTTP (TCP: 80); HTTPS (TCP: 443)
Additional Details:	• Provides 2FA for OpenVPN Server (vpn.cbXX.cb.crp), consisting of OTP token and credentials from Active Directory • Administrator user from DC has administrative rights			

INT Zone VMs

Hostname	**IP**	**IPv6**	**Description**	

ws1-X.int.cbXX.cb.crp	10.X.3.[11-19]	fd03:10:X:3::[11-19]	INT domain Windows 10 workstations for regular organization staff members	SMB (TCP: 445); RDP (TCP: 3389)
Additional Details:	• **OS**:: Windows 10			
ws2-X.int.cbXX.cb.crp	10.X.3.[21-29]	fd03:10:X:3::[21-29]	INT domain Windows 10 workstations for regular organization staff members	SMB (TCP: 445); RDP (TCP: 3389)
Additional Details:	• **OS**:: Windows 10			
ws3-X.int.cbXX.cb.crp	10.X.3.[31-39]	fd03:10:X:3::[31-39]	INT domain Ubuntu Linux workstations for regular organization staff members	SSH (TCP 22); RDP (TCP: 3389)
Additional Details:	• **OS**:: Ubuntu			

SEC Zone VMs

Hostname	**IP**	**IPv6**	**Description**	**Required Services**
arkime.sec.cbXX.cb.crp	10.X.4.3	fd03:10:X:4::3	Full network traffic capture server based on Arkime	none

Additional Details:	• **OS**:: CentOS 7
	• Web UI is located at http://10.X.4.3:8005
	  ○ Username: admin
	  ○ Traffic is received from firewalls			

onion.sec.cbXX.cb.crp	10.X.4.4	fd03:10:X:4::4	Security Onion intrusion detection, network security monitoring and log management server	none

Additional Details:	• **OS**:: Security Onion
	
	Security Onion is a free and open source Linux distribution for threat hunting, enterprise security monitoring, and log management.
	
	• Account name for Web GUI access: admin@cbXX.cb.crp
	• Web GUI: https://onion.sec.cbXX.cb.crp/
	• Windows event log and unix syslog sending is preconfigured to Security onion from other gamenet hosts
	• Network traffic is mirrored from firewalls
	  ○ GRE encapsulated traffic is received on ens224 interface IP
	  ○ Decapsulated GRE traffic is sent to mon1 interface			

kali.sec.cbXX.cb.crp	10.X.4.5	fd03:10:X:4::5	Kali Linux for Penetration Testing and Ethical Hacking	none
Additional Details:	• **OS::** Kali Rolling • Kali Linux can be used by BT for security testing purposes.			
terminal.sec.cbXX.cb.crp	10.X.4.7	fd03:10:X:4::7	Server for Windows based security tools and services	none

Additional Details:	• **OS**:: Windows Server • This host can be used by the blue teams install and use Windows based security solutions.

WIFI Zone VMs

Hostname	**IP**	**IPv6**	**Description**	**Required Services**		
clientXYZ.wifi.cbXX.cb.crp			10.X.5.0/24 (DHCP)	fd03:10:X:5::/64 (SLAAC)	Guest WiFi network, devices are not managed by Blue Team	none
Additional Details:			Blue Team has no administrative access to hosts located in this segment. Regular internet access and services in DMZ and CLOUD segment must be allowed to be accessed for hosts located in this segment.			

SM Zone VMs

Hostname	**IP**	**IPv6**	**Description**	**Required Services**
recorder.sm.cbXX.cb.crp	10.X.7.2	fd03:10:X:7::2	Surveillance video management server	RDP (TCP: 3389); HTTP (TCP: 8081); HTTPS (TCP: 8082)
Additional Details:	The recorder machine is a regular Windows system that is running Milestone XProtect VMS 2022 R3. Video feed is coming from one or more real or simulated cameras. You don't have shell access to the cameras, only HTTP API is available. Credentials are stored in XProtect system. There is no need to reconfigure cameras during training.			
camera1.sm.cbXX.cb.crp	10.X.7.3	fd03:10:X:7::3	Managed by GT	-

Additional Details:	• Camera system, no direct access for blue teams			
camera2.sm.cbXX.cb.crp	10.X.7.4	fd03:10:X:7::4	Managed by GT	-
Additional Details:	• Camera system, no direct access for blue teams			

Critical Infrastructure Control Centre VMs

Hostname	IP	IPv6	Description	Required Services
hmi.ics.ciXX.cb.crp	10.X.10.2	fd03:10:X:10::2	Human Machine Interface (HMI) for Energy Company distribution grid operations	SSH (TCP 22); HTTP (TCP 8080)

Additional Details:	• **OS**:: Debian 8 • Use SSH for operating system admin access. • ScadaBR interface is located at http://10.X.10.2:8080/ScadaBR ○ username: admin • MySQL root user has the default Blue Team admin password **Operating the Power Grid** http://10.X.10.2:8080/ScadaBR/views.shtm?viewId=1 shows layout of a simple power grid. The task is to keep the end users (indicated with light bulbs on right side) powered. http://10.X.10.2:8080/ScadaBR/public_view.htm?viewId=2 is a read-only view of the same grid that can be used for display purposes in the training control room. The schematics displays situation in the Gamenet power grid. Parts that are colored red, are currently without power. Certain parts are accompanied with indication of its current load. Turn ON/Turn OFF buttons are available for operating power plants and breakers on lines. Some backup power lines are controlled automatically by the PLC. The loads generated by end users are picked randomly and change every few minutes. The loads on substations and power plants are calculated based on routing of the current. Note that the substations and power plants have overload protections that will switch them off. The substations recover automatically, but power plants must be switched back on manually.			
historian.ics.ciXX.cb.crp	10.X.10.3	fd03:10:X:10::3	Database server that collects historic process data about energy distribution grid operations	SSH (TCP 22); MariaDB (TCP: 3306)

Additional Details:	• **OS**:: Oracle Solaris • Use SSH for operating system admin access. MySQL root user has the default Blue Team admin password phpmyadmin is located at http://10.1.10.3/admin/ ○ username: pma ○ password: pma(if this does not work, try no password)			
plc.ics.ciXX.cb.crp	10.X.10.4	fd03:10:X:10::4	Green Team managed energy distribution grid substation equipment	ModBUS (TCP 502)
Additional Details:	• This host is managed by training organizers and blue team does not have access to it.			

Business Services VMs

Hostname	**IP**	**IPv6**	**Description**	**Required Services**
k8s-[1-3].bsn.cbXX.cb.crp	10.X.6.[21-23]	fd03:10:X:6::[21-23]	Kubernets cluster node	SSH (TCP 22); HTTPS (TCP 443)
Additional Details:	• **OS**:: Ubuntu • Use SSH for operating system admin access.			
app.bsn.cbXX.cb.crp	10.X.6.242	-	City management portal.	HTTP (TCP 80)
Additional Details:	• Docker pod running on Kubernetes • Uses Postgesql running in Kubernetes in the same namespace			

Azure Cloud VMs

Hostname	**IP**	**IPv6**	**Description**	**Required Services**
www.cbXX.cb.crp.sh	N/A	N/A	CB Organization managed website running in Azure	HTTPS (TCP 443)
Additional Details:	• Azure Managed service • This is 3rd party city web site that is managed by CB organization.			
bastion.cbxx.cb.crp.sh	N/A	N/A	Bastion Host for external partners to access goverment resources	RDP (TCP 3389)
Additional Details:	• Windows Server for hosting a jumphost for external partners			

List of Green Team Managed Gamenet Systems

The following table lists Green Team managed systems that the Blue Team should be aware of.

Hostname	**IP**	**IPv6**	**Description**
www.tech3X.cb.crp	10.103.0.130+X	fd03:10:103::130+X	Internet website
r-access.btXX.cb.crp	10.X.0.10	fd03:10:X:0::10	Green Team managed blue team access router for accessing BT networks over VPN
upload.cb.crp	10.103.0.103	fd03:10:103::103	Upload server for simple and anonymous file sharing
pastebin.cb.crp	10.103.0.107	fd03:10:103::107	Pastebin service for simple link and text sharing
ip.cb.crp	10.103.0.109	fd03:10:103::109	Simple http://whatismyip.com style website displaying clients IP address

ns1.cb.crp	10.103.0.13	fd03:10:103::13	Primary Recursive DNS server for Gamenet clients
ns2.cb.crp	10.103.0.14	fd03:10:103::14	Secondary Recursive DNS server for Gamenet clients
ca.cb.crp	10.103.0.137	fd03:10:103::137	Public Certificate Authority server

Hackathon Technical Rules

1. Blue Team Systems page in https://collab.i3.cybexer.io/ defines for each system what is the general functionality of the host and what services have to be provided. Required services must remain operational and blue teams are not allowed to sabotage or remove these services.
2. During Threat Hunting Phase, Blue teams are discouraged from making configuration changes in the gamenet machines. This is due to the nature of a threat hunting exercise, which is pre-planned and focuses on detection and reporting of attacks by the blue teams. In case hardening changes are implemented by a team, they run the risk of locking themselves out of the content of the training(attacks, data items, data for reporting and so on).
3. During Live-Fire Phase, Blue Teams are free to make any changes to the systems as they see appropriate, while respecting exercise rules. In case the modifications result in a loss of service availability for extended period white team may revert virtual machines in question back to their initial state in order to restore the services availability
4. Blue Teams are allowed to revert VMs to working snapshot via ISA portal. Reverting may not be used as part of “defense plan”, instead it meant to recover a VM if no other option is available. A penalty will be applied.
5. In case the required service is listening on both IPv4 and IPv6 address, the service must remain accessible over both addresses.
6. Changing DNS names or IP addresses of any of the systems is not permitted.
7. All required services running in DMZ and CLOUD network segments are considered to be public and have to be accessible from all networks including (simulated) internet.
    1. Only exception to this rule are the management services running on DMZ and CLOUD hosts (ssh, RDP, administrator web panel etc.). At minimum, management services must be open to INT and SEC segment.
8. Services running on hosts in INT, CI, SRV and SM segment must be accessible for hosts in the same subnet and to all other hosts which are required to guarantee the functionality of services specified under system descriptions. Few examples:
    1. dc1.int.cbXX.cb.crp and dc2.int.cbXX.cb.crp are used by various applications in DMZ segment for user authentication
9. Services required for remote administration (SSH, RDP, web interface etc.) must be available to other hosts inside their Gamenet zone unless different requirements are specified under system description.
10. ICMP/ICMPv6 ping (echo request and reply) must be allowed on all hosts and interfaces. For DMZ and CLOUD ping must be allowed from the whole simulated internet. For internal services, the ping has to be allowed from same segment and also from other segments where that particular host has to be reachable.

11. Blue Team is not allowed to shutdown, remove or abuse VMWare tools or open-vm-tools in any way
12. All workstations that were initially joined to INT Active Directory domain must remain joined in the domain.
13. Workstations in INT and WIFI segment must be allowed to use the following services (outgoing traffic) on the the (simulated) internet:
    1. SSH, HTTP(s), HTTP-ALTERNATIVE (8080), SMTP, POP3, IMAP, ICMP ping. Both IPv4 and IPv6 traffic must be allowed.
14. Pre-installed software on INT workstations, which is needed for daily business of regular users has to remain fully functional. At minimum the following software has to remain in place:

    1. Microsoft Office (Word, Excel, Powerpoint, Outlook) or LibreOffice alternative.
    2. Software for reading PDF documents
    3. Selection of different web browsers - Mozilla Firefox, Google Chrome and Internet Explorer on Windows workstations
    4. Media player software (VLC or similar)
    5. Putty and WinSCP on Windows workstations
    6. Software for archive manipulation (7zip, WinRAR, WinZip or similar)
    7. Notepad++ or similar
15. End users have the priority of using their workstations. Administrators cannot limit their access for extended period of time.
16. Accounts gt, greenteam and scoringbot are use by Green Team members for support and monitoring purposes system. Blue Team is not allowed to:

    1. disable, restrict, mimic, replace, modify or use these accounts in any way
    2. kick out Green Team members or any other way disturb Green Team from using these accounts
    3. remove these accounts from administrator or sudo groups
    4. remove above mentioned accounts ssh keys from authorized_keys file if they are present

       green team ssh public key is:
       ssh-rsa
       AAAAB3NzaC1yc2EAAAADAQABAAACAQCrijB4VjbTOwQvNh6bjRbwuYz3a6KS3bj
       oShIXEgaOoyLqx7ZievBP75n6z82L6tFZKqeuZVs0D+XusGkb9c2zXH2aIccEcO
       mp6vX9Pj5fIydT+noVAzLHdKgOfIk5ngaRiwTcUSNzRO3wy1m3C66hpiNYkW60p
       ISMfhnhtbvpNTuoX8EDZykohP+x3r0syP+Xc4HhS0Gw+PwgUJpAlGDDiTkdrY/7
       YzR4xABY66KAnVDRopxxQ2+lf4s7d3UR7FplSdSSt4CRo0dE82N5d/DyKjZgiih
       ToYTBmCHbpMNPEls5hFHpumiKHBNIJObPwQoJNbzE0AnW3b6i9Mlz/vXcqRae6l
       u2mrTu1SvQ9xvKjE4ou9wthNxEMu9Uwr0erIa8jod4pTKWuuKJdIELDEQND4Bcj
       0vshntUi25C+rHgdhfP68vWAJiYHHxemIOflHbxoWGIu+JlkpsKvNHDLOtaWC9+
       YByh5WHRJPx8sQMvHEQN37rVNk8rvHng9J2xB+OnDC9NeJef1z18SinnVYijsHv
       n+kR3OrCr1dh36yxquSPozXhbwzESf3V/q3csVhnj8AldO5UvOyGel+K9U/sLXz
       tVmgacVnivUDRxyyVhrKqS5Yp6SB+3HmobgCEqgsTYtqqq/rbFxTiBZ3fLxFZfi
       HoJTyL/fX/C8pPwDuCz/Q== cb_gt

5. scoringbot ssh public key is:
   ssh-rsa
   AAAAB3NzaC1yc2EAAAADAQABAAABAQDNYTiXw4f2esa+f0KYsqOfVlcmE+M55ge
   iwz1rT5pLyUhG48KoyabulmsrNPO/cVIMAIWqcW4br60aNkaG9OJiGf5HtlQDUD
   F3TKs8UZvxjpbAiTVyJuZCu5RmS/TG/okhPvtrsHwHuEpQjpzH4dRlOxCG0dOZd
   uXPRavDD+r8uwdsbHTfaioaFv3uvkkX6w0MUdHHgJ2lA17qu5gd+2eUuOWG/EpH
   o604Qf7fdPMwhH7c0SN8SM0UuP56nVUjw8fWVulJk6/oLSmbH/Tluz91tqshkiv
   Mz2P/URoo9JNtePqatsT1+hWCusBDbSU9NqNdt77fxCsCooRSOotZpD4z
   scoringbot
17. Blue team is free to change, modify or delete any other account used to administer the systems (root, Administrator, admin etc.)
18. Regular user accounts of the Blue Team personnel are listed under User Accounts in http://collab.i3.cybexer.io/ . The users are working all the time and they are expecting to experience as few inconveniences as possible during their workday. In case a password reset of end user is deemed necessary, Blue Teams are required to document new password and brief reasoning on the User Accounts page.

Scoring Categories

Blue Team scoring depends on 7 categories:

- **Solving Tasks** – positive points are gained by solving various tasks via ISA including the CTF and Hack back tasks.
- **Situational Reports** – positive points are granted on valid Blue Team's SITREPs (validated by the White Team). SITREPs are expected once per day on specific times.
- **Incident Reports** - positive points are granted on valid Blue Team's Incident Reports (validated by the White Team). Incident reports will be enabled during live fire mode.
- **Availability** - positive score for maintaining services availability during classic live fire mode.
- **Special Scoring** – negative or positive points given by White Team. Positive points can be awarded for good and useful cooperation initiatives via MISP.
- **Attacks** - penalty score for failing to defend against Red Team attacks during classic live fire mode.
- **Virtual Machine Reverts** - penalty score for restoring systems from backup (revert VM to snapshot)

User Simulation and Automated Scoring

To make the training realistic then user simulation and traffic generation is used to create close to life like traffic profile in blue team systems and networks. In addition, services that are required to be kept operational can be monitored by the training organizers via automated checks.

Automated Monitoring Checks

Green Team can perform automatic monitoring checks of required services to verify the general health of blue team systems. These checks are conducted as following:

- Public services in DMZ and CLOUD are checked using random IP addresses from (simulated) Internet
- Internal services (INT, SEC etc.) are checked from the same network segment. Monitoring bot uses IP addresses ending with .252, .253 and .254

User Simulation

White team is responsible for simulating regular users. Both automatic and manual means are used to conduct various activities in workstations - read e-mails, browse web, edit documents etc.

Automatic agentless user simulation is performing various tasks via RDP, the actions look for the Blue team as if a real person is performing the actions. ChatGPT is generating Outlook and Word content. The following actions are being done via RDP:

- Web browsing
- Sending internal emails via Outlook 2016
- Creating Word documents
- Creating notepad files
- Running PowerShell scripts if the user used in sim “works” IT Department.

User Simulation team will use accounts listed under User Accounts page. If blue team changes regular user password, then new passwords must be documented.

User Simulation team will use operating system native remote access tools (ssh, rdp) or VM console to access workstations.

Annex I - Integrated Scoring and Awareness System (ISA) Usage Instructions

Introduction

Integrated Scoring and Awareness (ISA) is a solution, which provides a near real-time scoring, and situational awareness visualization and reporting functions during cyber exercises or trainings.

Functionality

This section describes the ISA functionality for Blue Teams.

- Scoring
- Tasks
- Situation reports
- Incident reports
- Situational Awareness

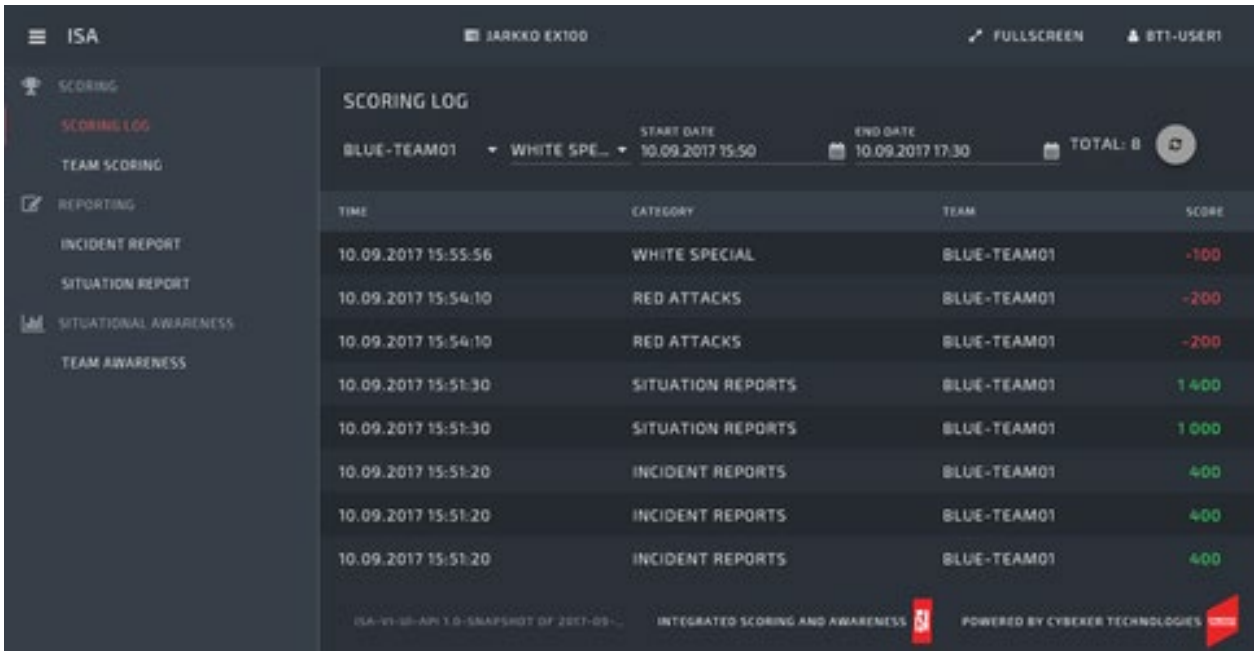
Access During Execution

It is important that you use newest Firefox or Chrome browser version for ISA (other browsers are not recommended).

Scoring Widgets

Scoring Log

- Allows Blue Team to see the list of scoring events for their own team in log view.
- Columns:
    - Time: date and exact time of event
    - Category:
        - White special
        - Red attacks
        - Situation reports
        - Incident reports
        - Solve Task
    - Team: name/number of the Blue Team
    - Score: how many points were given for the event
        - Green: positive points
        - Red: negative points
- It is possible to filter the dates in the upper section
- It is possible to show events by type from a dropdown menu



Team Scoring

Allows all users to see current scores for all teams in graphical view.

- From the picture: upper section shows total score for each team.
- From the picture: lower section shows a breakdown of the scores by category:
    - White special
    - Red attacks
    - Incident reports
    - Availability
    - Situation reports
    - Reverts from snapshots

Reporting

Incident report

When Blue Team detects a service problem or when they restore a service, Incident Report can be submitted. This indicates that Blue Team knows that they were attacked and would get points for that.

The report goes to the White Team or analysis and confirmation.

Incident type

- **Compromised** – when target state changes from "good" to compromise. To be sent immediately when compromise is detected, these mark targets as compromised for the blue team (does not negatively affect availability score).
- **Not compromised** – when target state changes from compromised to "good"(target has been secured).

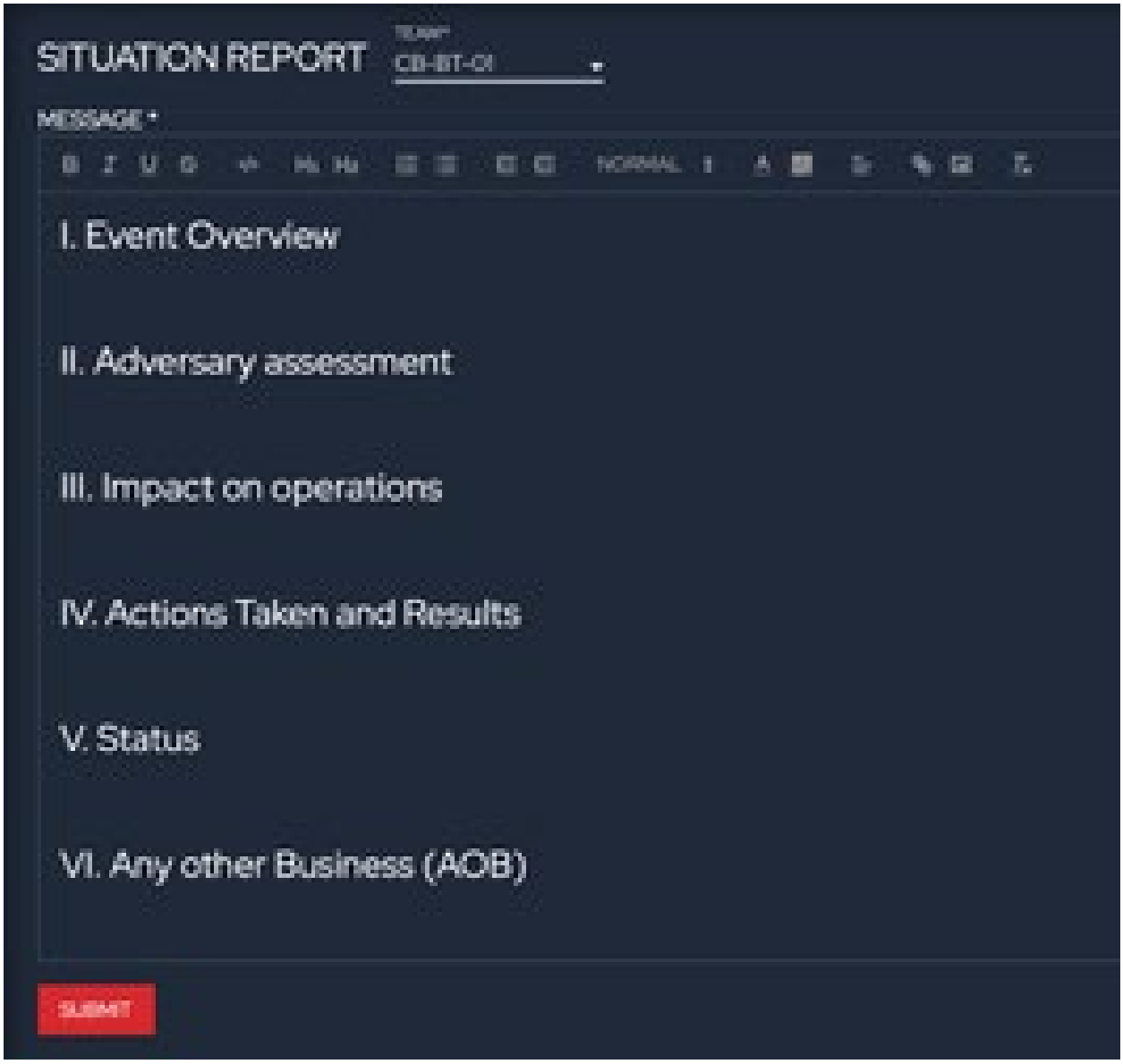
Submit Incident Report

- Go to „Incident report“ section in the left-side panel.
- Choose a target that is affected.
- Choose incident type:
  - Compromised
  - Not compromised

- Write a comment in free form in the „Details“ window. Please insert valuable technical data/information in the system – IPs, work tasks, impact, estimated time of repair.
- Click „Submit “.
- Please take into account that all incident reports have a sequence – compromised → not compromised.

Situation report (SITREP)

The Situation Report allows Blue Team members to insert/report requested situation reports in free format. ISA interface allows rich text editing. The report goes to the White Team judges for analysis after submitting.



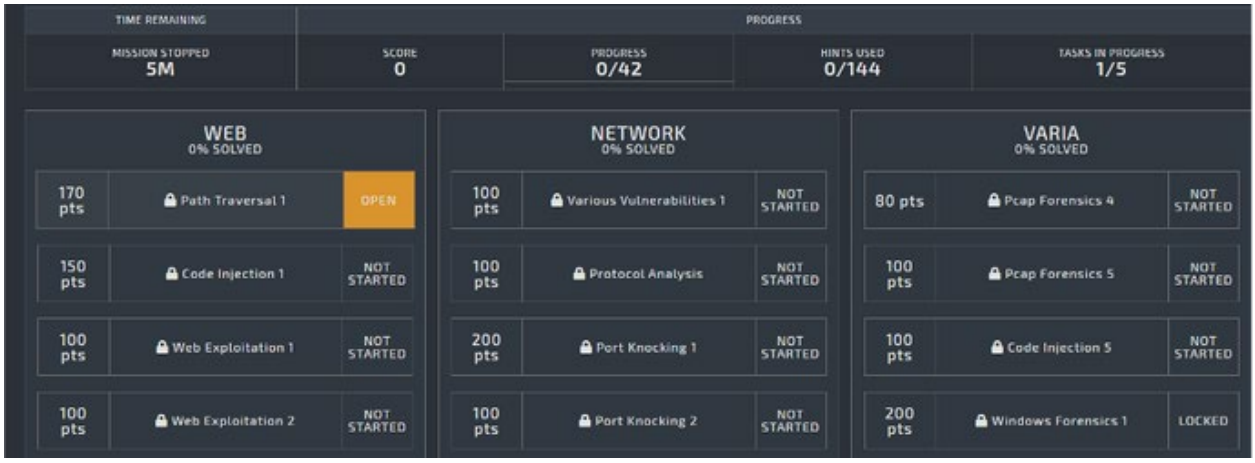
Submit SITREP

- Go to „Situation report" section in the left-side panel.
- Fill in the report according to pre-defined report structure in the „Message" window. You can use many of the most common rich text editing features like bold, italic, underline, bulleting, numbering, linking, inserting images etc.
- Click „Submit", when the report is completed.

ISA tasks

During the hackathon the ISA mission board tasks will be used for one of two purposes:

1. CTF tasks
2. Threat Hunting tasks
3. Live-Fire tasks
4. Hack back task
5. Bonus tasks



Mission board gives the user an overview of tasks. The tasks are categorized and can be unlocked/locked by the organizers. To see the contents of a task, click on the task. To start solving, press "Start Solving". There will be 5 options available:

- Submit Answer
- Stop Solving (can result in negative points)
- Use Hint (can result in negative points)
- Feedback
- Close

Team Awareness View

Team Awareness provides network segment overview for a Blue Team, based on situational state indexes. The information comes from Blue Team's incident reports.

Segment Status View

Segment Status show the live status of the Gamenet targets. ISA checks all the targets required services with 1 minute interval.

There are two statuses visible to Blue Team:

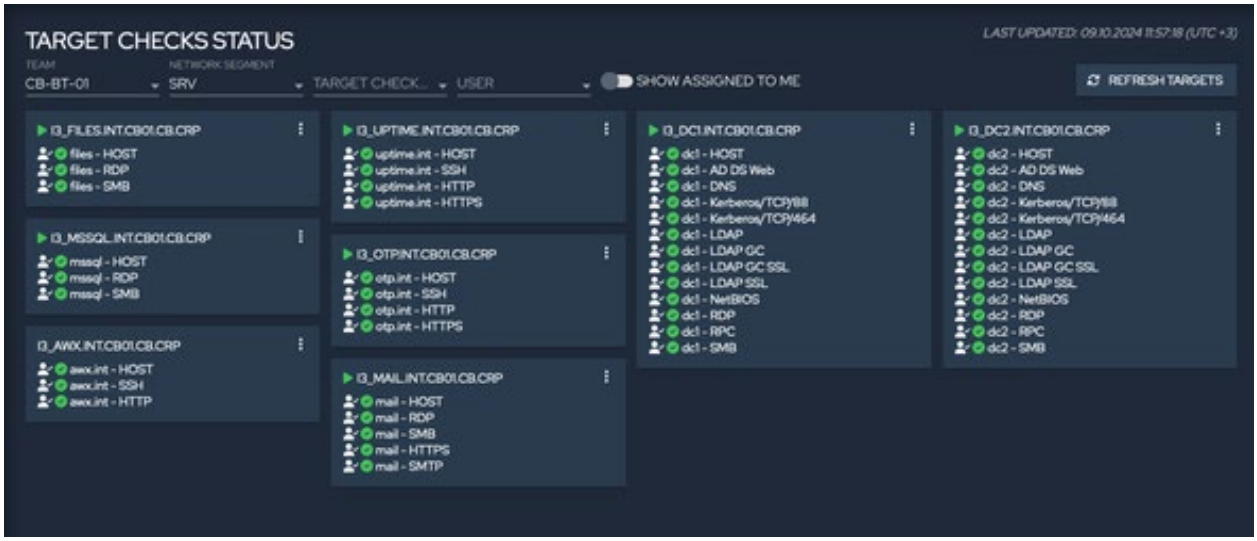
- Green (Available)
- Red (Not Available)

Target Check Status View

Target Check status drills down the availability information to specific targets in a network segment

There are two statuses visible to Blue Team:

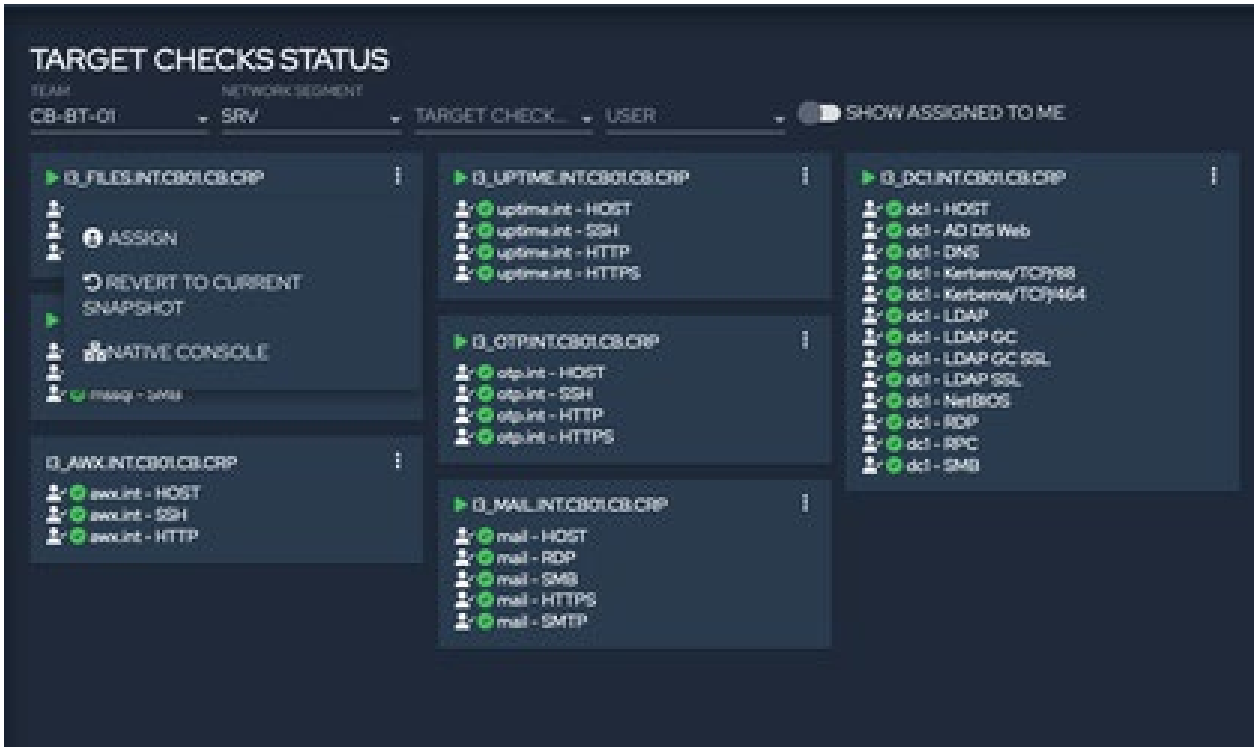
- Green (Available)
- Red (Not Available)



Accessing Virtual Machine Consoles and Reverting to Snapshots

From the Target Check Status View, Blue Teams can access the consoles of the Virtual Machines and also revert the Virtual Machines back to initial states (with penalty).

The VM console can be used in emergency situations, when network is not available to the target (in case on over hardening the target or the firewall).



Annex II - Situation Reporting Instructions

Situation Report (SITREP) serves the primary purpose of keeping higher headquarters and adjacent organizations informed of changes in the situation, or critical events. Reports must be complete and accurate; at the same time, leaders must ensure that their reports are not overly complex. The SITREP outlines the Team's situation, the Team leader's recommendation of a course of action (COA) in response to an ongoing event, or a summary of actions already taken and their affect. If the team is presenting a COA for approval from higher and it's approved, after executing the approved COA, the Team leader sends an update in the next scheduled SITREP (in this case, a closure report) to inform the higher headquarters of the result of the operation (success, failure, impact, additional follow-on COA, etc).

General Guidelines

The Blue Teams are expected to write a SITREP directed to their imaginary supervisory authority that oversees managing the given crises. The SITREPs must be compiled on the ISA site using the standard reporting format and cover the period since the previous report (since STARTEX for the first one).

The White Team will read and judge the reports exactly on the time marked in the schedule.

Please note that you just can't be late with completing the SITREP. Meaning, it makes absolutely no sense to edit the report after deadline, because a half-ready report has already been automatically submitted for the evaluation exactly at the given deadline.

To be kept in mind:

- SITREP audience is the Blue Teams' supervisory authority in charge of managing crises.
- Do not include too much technical details (IP addresses, ports, code snippets, tech jargon, etc...)
- SITREP should describe the major activities of the reporting period
- Users must remember that timely reporting, especially of enemy activity, is critical in fast-moving tactical situations. Recommend keeping your SITREP up-to-date during the day so that you are not rushing at the last minute to complete it. This could result in mistakes, incomplete reports, ineffective reports, and a lower scoring gameplay.
- Spell out abbreviations first time they're used, don't assume the audience knows what it means.

Events to Report

- Adversary intrusions to your network
- Service interruptions due to malicious activity (Loss of functionality, website defacement, etc.)
- Suspected malicious activity (even if not confirmed)
- Discovered malware on systems
- User compromise (successful social engineering, phishing, etc.)
- Other relevant information

SITREP Format

The SITREPs should follow the below format and consist of the following core elements. Each element is described below.

Executive summary

The Executive Summary (EXSUM) should describe a summary of issues of major importance or impact on operations. This should be a short and succinct summary of all key points in the SITREP so that if leadership only reads this one paragraph they'll have a general understanding of a given situation.

Key Events

In the key events section, the SITREP should describe the main activities, events, and updates **since the last SITREP**. To ensure accuracy and completeness, use the following outline. Not all elements under each section are required; use the ones that are applicable to the given situation. Every key event should have a unique identifier: BTXX for instance. When listing key events, you can first list events for which something new happened since last SITREP. The closed events can be listed in the bottom with the message: **Closed**. The idea is to have a reference of all events that have occurred since the start of the exercise or training.

Event Overview

- Brief description of the event. Include what, when, where, why, & how the event took place.
- Timeline of the event / incident.
- A brief overall assessment of the situation. This includes circumstances or conditions, which increase or materially detract from the capability and readiness your organization (BT).
- The source of the incident or the vulnerability exploited, if discovered.

Media contacts (if any)

These are not always linked with key events. Media can be addressed in the “Any other Business” (AOB) section if not linked with key events.

Adversary assessment

In real life, the attribution is very difficult and trying to answer to the below if not having real and strong evidence could generate to attribution overkill. Anyway, if you have a reason to believe that you know who caused the incident (the adversary), provide identity and short explanation of how you came to this conclusion including your assessment of the adversary. In other words, try to answer the questions below, explain and describe your rationale behind the assessment.

- **Who** - individuals/organization/state/other. Little or no evidence of state involvement, state-tolerated or sponsored/state executed, names, symbols, etc.
- **Why** - motivations. Objectives as criminal, ideological, political, etc.
- **What** - how skilled is the adversary? Consequence of the exploits or attacks from the adversary and level of sophistication (does the adversary use known exploits and/or custom developed exploits)
- **Where** - location of adversary. If possible, of course.
- **When** - when this happened.

Impact on operations

Describe the Team leader's evaluation about the impact this incident had on your services or on the operations. Consider downtimes, damage to customer basis, negative PR, potential legal actions taken against you, etc. Furthermore, consider the situational impact to the Organization (BT), the significant mission readiness degradation and the current and proposed future mission impacts.

Actions Taken and Results

Describe the major steps you have taken to mitigate the issue and a brief description and results of Defensive Operations undertaken by your organization (BT). Summarize about plans for operations during next 24-hours, including objectives and probable adversary reaction. Report about deviations or variations from previously reported intentions/plans. Eventual request for assistance should be mentioned in this section as well it would be good that an answer, if any, is coming to the BT. Remember, however, that the SITREP is not the right channel to request for assistance.

Status

Report if the system affected are fully operational or with limited functionality, if they are off-line, etc.

Decision or Resource Requirements

Report if you need a higher-level decision. Also report about significant deficiencies and resource requests out of the organization's control, which affect supporting for continued operations. Problem areas beyond the organization's capability to overcome or alleviate in a timely manner could be reported as well.

SITREP Scoring

White team considers the following four categories when scoring the reports:

- **Coverage** - if the relevant events were covered in the report.
- **Details** - amount of details shall satisfy the need of supervisory authority.
- **Analysis** - how well the events are interpreted and analyzed in the report, also the requests for decisions and resources fall into that category.
- **Other** - style, format, structure, readability and any noteworthy comments which do not fall into above mentioned categories.

Annex III - Example of Good SITREP

This is an example of very good SITREP from one of the previous events.

General

For this and further updates, the report contains the old version as well and we explicitly show changes in separate, marked paragraphs to see the development of the situation. The updates were moved to the beginning of each chapter. If not interested in the content from the past report, you can then jump to the next subtitle.

I. Event Overview

Here is a quick overview what has happened / has been identified so far. The events are clustered according to report phases to see updates/development of the situation. If necessary, there is an explanation in between.

Events from Day 1 from noon (12:00h) until afternoon (15:30h):

- Ongoing activity after the social engineering
- Further attacks on network components and infrastructure services
- Identification of signs of previous attack steps of a likely targeted attack

Events from Day 1 start of the SOC team deployment until noon (12:00h):

- Social Engineering against Office users (targeted attack?)
- Website attacks (code injection for financial purposes) on DMZ service (webmail) --> annoyance for users, higher energy bill but no real threat
- Website defacement on main Webserver (under investigation)

II. Adversary assessment

From what was seen so far, there are hints to 3 potential adversaries, which are being described in the next paragraphs. Updates are reported after the initial assessment from the first report to see the development.

CAUTION: Since the SOC team mission has just started, there are still heavy investigations. It's thus likely that information changes as new information is collected and analyzed.

Sophisticated / possible state sponsored actor

Update for 2nd report: The sophisticated/possibly state sponsored actor managed to get administrative credentials quite fast. He has now full control over the INT zone. The techniques used seem at least sophisticated, as initially assessed. The adversary uses a mix of default system tools to hide under "normal system administration", although we identified hints for a possible custom tool.

It seems that the attacker gained access already a week ago (10 Feb 2022) and has highly likely administrative access. See chapter III, Impact on operations, below, for further details)

Original assessment from the 1st report: There are signs of targeted attacks against our office users. A dozen users has received phishing documents. X users downloaded or opened the attachment and got thus likely infected with malware. It's still under investigation what the actor is doing at the moment.

The delivery of the malware is still under investigation, which then will allow us a determination of the sophistication level. At the moment, hints show at least a medium sophistication level as the attack seems targeted.

Financially motivated actor

Update for 2nd report: The were no new "IOCs" (Indicators of Compromise) identified, which we would attribute to this attacker. Thus, it's likely that this adversary hit us incidentally, when broadly deploying the malicious script for financial gain.

Original assessment from the 1st report: A (financially motivated) actor has placed a Cryptominer (abuses visitors computing resources for financial gain) on our webmail service. It's likely that this was an automated attack and no special attack against the national infrastructure or a government/military specific attack, however, cannot be confirmed.

The sophistication level, for the moment, cannot be determined for certain. A Cryptominer per se is "standard". The way how the service was compromised is not known at the moment.

Hacktivist group

Update for 2nd report: The were no new "IOCs" (Indicators of Compromise) identified, which we would attribute to this attacker. Thus, it's likely that this adversary hit us due to a known vulnerability. This is a sign for (medium to) low sophistication and the hacktivist group does not pose a serious threat.

Original assessment from the 1st report: An attack on our main webserver shows hints to hacktivism. A message ("Incredible Computing has false sense of security") on the defaced website tries to influence public opinion on our national ICT industry provider ("IC", Incredible Computing).

At the moment it can not be said for certain if the sophistication level of this adversary is high or low. This is still under investigation.

III. Impact on operations

The impact on operations will be divided in different zones, according to our security model. These will be described in the next following sub sections.

DMZ (Public-facing network services)

Update for 2nd report: We saw several traces for past attacks which can, but not necessarily have to, be connected to the actual attacks. We could not verify so far. Affected are a number of technical infrastructure services in the zone DMZ, as well as an meanwhile decommissioned Gallery-Webserver. It's unlikely that we can fully resolve the issues, as there is not enough evidence to connect the dots for the full picture due to the removed system and insufficient logging.

However, it looks reasonable that the attacks on the infrastructure services in DMZ were used to infect internal users, by tricking them into opening phishing mails with legit-looking, compromised websites on our own systems. This is due to insufficient system hardening.

Original impact from the 1st report: In the DMZ, normal operations is possible at the moment, except the main webserver (www.icXX.jc.crp). This website is defaced and thus unusable at the moment, which causes negative publicity as long as the website is not being fixed.

The Cryptominer on the webmail service is annoying, but the service is still usable and for the moment there are no hints regarding loss of information.

INT (Office environment)

Update for 2nd report: The attacker in the INT zone is still active. Last investigation results show that the adversary could be having access since 10 Feb 2022, so up to 1 week. As the attacker has fully administrative control over the systems, it has to be assumed that the adversary is looking about information regarding the actual missions, as far as these are planned within the office network.

Original impact from the 1st report: The attacks on our users in the office zone show hints of an APT (Advanced Persistent Threat). The attacker is still active within the network, but is closely being monitored.

A timeline is being put together for the next report to show what the adversary tries to achieve (and has already done).

Internet

We detected direct connections and change of system configuration on our main connection to the internet. This was possible due to poor configuration and use of a weak password. We are in contact with the IT provider "GT Systems Ltd" to improve security.

SAT (Satellite Systems)

Update for 2nd report: Partners are reporting connection attempts from possibly malicious systems from the internet to their satellite systems. Due to attacks on our core network systems (see above), it's likely that an attacker is preparing similar attacks on our systems. We are investigating this issue.

It's important to understand that our satellite systems are under attack. If the attacker manages to get access to the systems, he can control our satellite systems.

IV. Actions Taken and Results

Update for 2nd report: We are still investigating the attacks and try to draw the complete picture. As mentioned above, we are missing essential information.

Our contractor "GT System Ltd." is being mandated to fix all identified systems that are compromised.

The attacker is advancing to more critical systems than the INT zone (office) to our military systems (Drone and Defense systems).

Additionally, we improved contact with our international and national partners to directly share critical information about relevant attacks.

Original actions from the 1st report: The incidents have been investigated or (targeted attack on our office users and website defacement) are still under investigation. We will report news twice a day to keep the commander informed about the development of the attacks.

Our contractor "GT" has been mandated to fix the compromised services and to remediate normal operations.

Thus, the services webmail is up and running clean again. Website will be next after full investigation.

V. Status

Status of the SOC team is good at the moment, everything is under control.

We have to recommend critical system improvement, on at least two sides:

- Secure configuration by default
- Improvement of visibility within the network segments and systems

VI. Any other Business (AOB)

NSTR (nothing special to report).