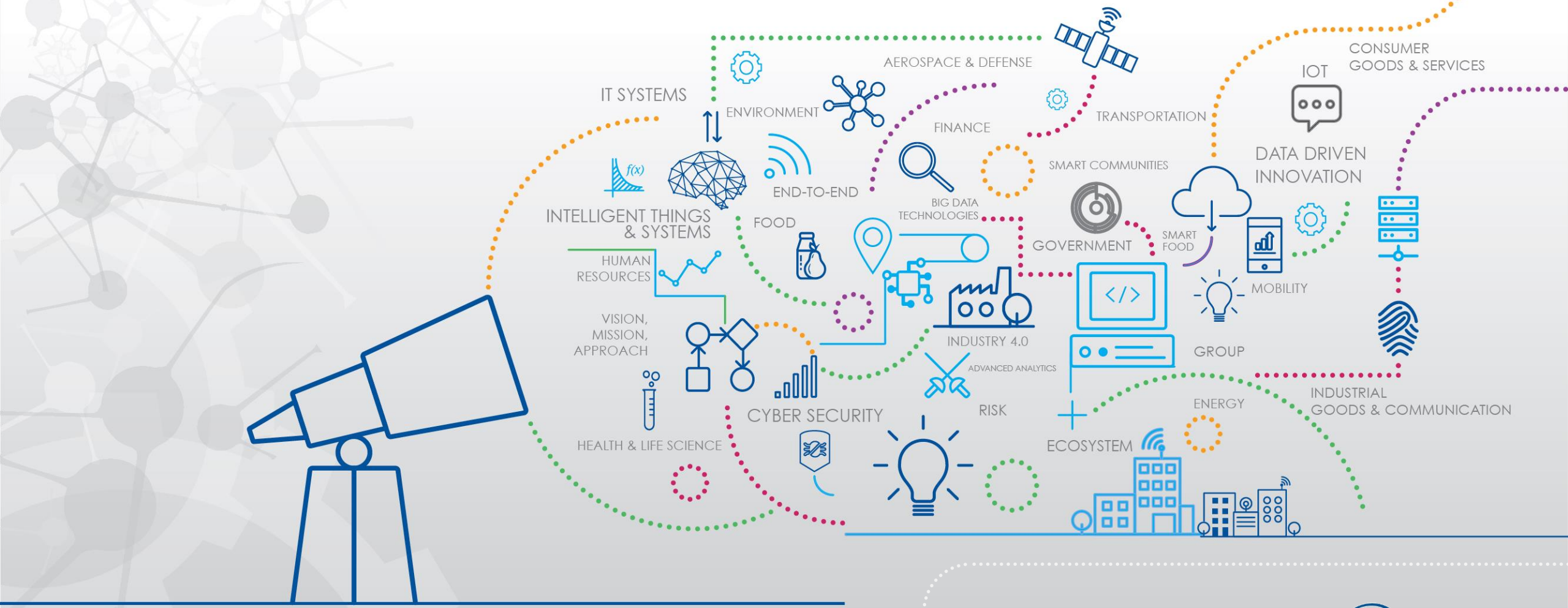
Cyber Range: Virtual Hacking Warfare



DANILO MASSA, Cyber Security Division CTO

ECS EUROPEAN CYBER SECURITY ORGANISATION

aizoon® TECHNOLOGY CONSULTING

AUSTRALIA
EUROPE
USA

Agenda

- ✓ **Nuovi scenari** del **cyber crime** e **nuove competenze da acquisire**
- ✓ **CTF vs CTF Attack and Defence**
- ✓ **Cyber Exercise**
  - Organizzazione
  - Team coinvolti
  - Tools di attacco e difesa
  - Regole di ingaggio
  - Scoring
- ✓ **Lessons learned:** misurare la **"cyber posture"**

Group profile

AIZOON IS

aizoOn è una società di **consulenza tecnologica** di **innovazione**, **indipendente**, che opera a livello **globale**

AIZOON GROUP

Copriamo l'intero processo di **creazione di valore per il cliente**, anche con le nostre partecipate:

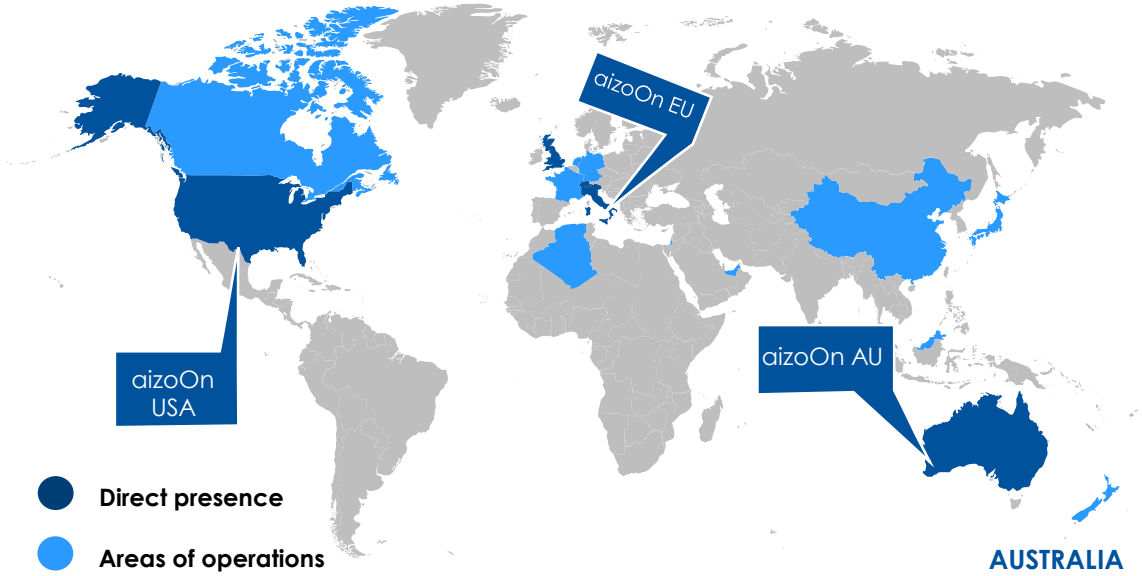
CSP organismo di ricerca per l'IoT e l'IoD
Trustech micro-bio e nanotech
K-Now social data intelligence

VISION/ MISSION

Abbiamo fatto nostro l'approccio **ecosistemico**:
l'innovazione si realizza attraverso un processo di **co-creazione** con le istituzioni, i cittadini, le organizzazioni pubbliche e private

la nostra visione: applicare diffusamente **l'approccio scientifico e quantitativo**, per una società più responsabile e sostenibile

la nostra missione: sostenere il futuro dei nostri clienti nell'era digitale, apportando **competenza di tecnologia e di innovazione**



AUSTRALIA
Sydney NSW

EUROPE
Torino ITA | Cuneo ITA | Milano ITA | Genova ITA
Bologna ITA | Roma ITA | Bari ITA | Sheffield UK | Zürich CH

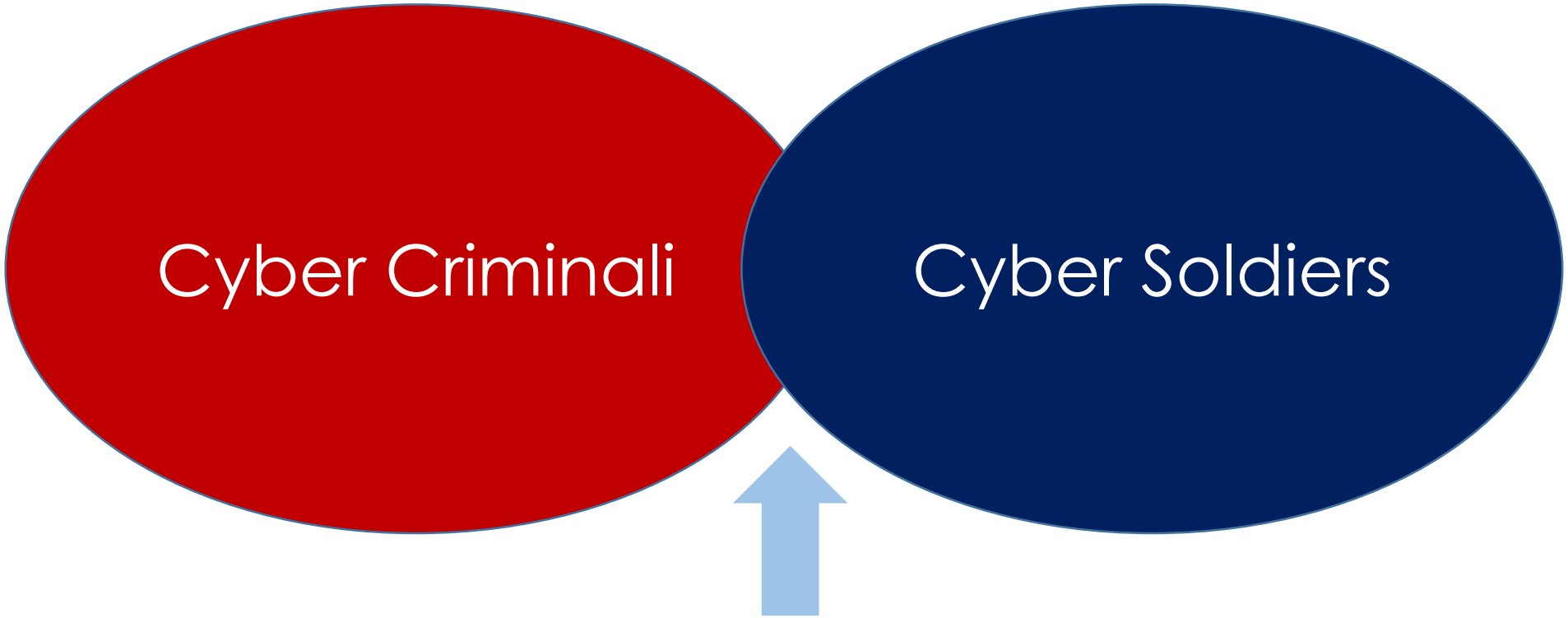
USA
New York NY | Troy MI | Cambridge MA | Lewiston ME

La divisione Cybersecurity

La **divisione Cybersecurity** di **aizoOn** opera su diveri mercati erogando servizi e soluzioni mirate a:

- Prevenzione (Awareness, Compliance);
- Auditing tecnico (VA e PT);
- Gestione post-incident (IH & Forensic);
- Formazione e Addestramento (Corsi & Unavox);
- Nuove tecnologie (ARAMIS, AMEE, MITHRIL, ADEngine, Cyber Range)
- Tecniche offensive (Unavox & altri).

Lo scenario di riferimento cyber-adversary



Cyber Soldiers of Fortune
(mercenari)

Cybercrime

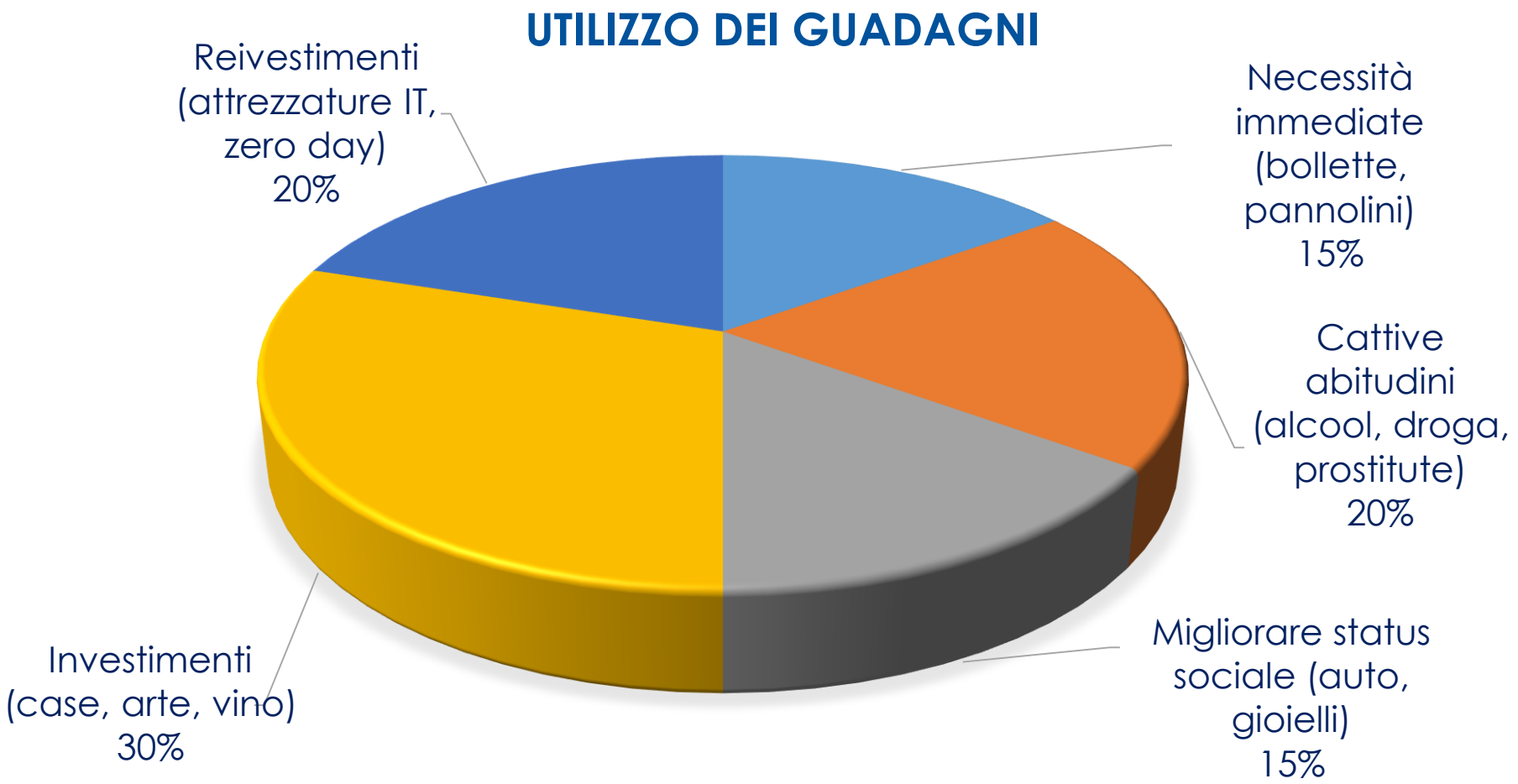
- Sempre **in aumento** ed i **criminali** sono sempre **più specializzati**.
- **Dark net in forte evoluzione**:
  - Market B2C per prodotti vietati (es. droghe ed armi);
  - Exploit zero day;
  - Identità reali (dalla patente di guida al passaporto);
  - Company exploit kit (mirati ad aziende specifiche);
  - CAAS (Crime-As-A-Service).
- **L'impatto**, in termini di **costi**, del cybercrime a livello mondiale è stimato intorno ai **6 trilioni di USD.**

Cybercrime

Totale: 1.6 trilioni di USD

©Bromium (HP) – Into the Web of Profit – Dr. Mike McGuire

Cybercrime



©Bromium (HP) – Into the Web of Profit – Dr. Mike McGuire

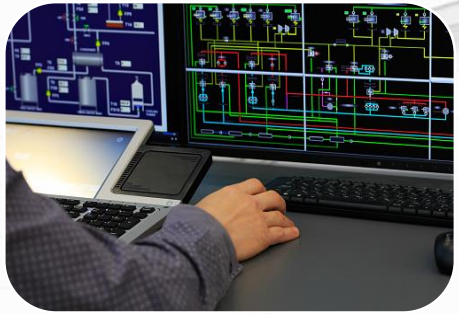
Cyberdefense

- Dal **2016** il **cyber-spazio** è considerato **teatro operativo dalla NATO**.
- **Tutti gli stati si stanno organizzando** per:
  - Addestrare truppe per la difesa e l'attacco;
  - Effettuare esercitazioni (Cyber Range);
  - Finanziare ricerche militari;
  - Sviluppare tecnologia proprietaria (principalmente di attacco).
- **Organismi sovra-nazionali** sponsorizzano attività di **ricerca e sviluppo**, tra i quali:
  - NATO CCD-COE (Cooperative Cyber Defence Centre of Excellence);
  - Unione Europea – EDA (European Defece Agency).

… ovviamente con molta cautela …

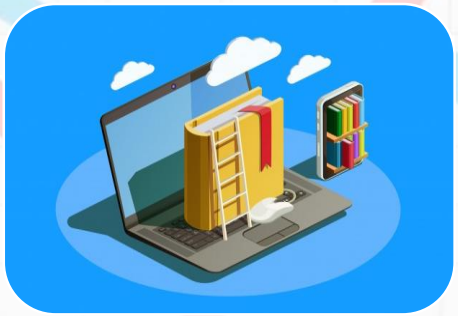
Le sfide del futuro

IOT industriale/building automation



SCADA e sistemi legacy

Embedded (automotive, droni)



Formazione Cyber Awareness

Compliance & Best-practice

Le sfide del futuro

- **Prodotti** sempre meno «signature-based» ma **che utilizzano algoritmi di:**
  - **Machine Learning**;
  - **Intelligenza artificiale**;
  - **Ibridi**.
- **Prodotti di cyber security in grado di trattare reali big data** in termini di:
  - **Quantità**;
  - **Frequenza di ricezione (streaming)**;
  - **Qualità**.
- Attività per la **definizione di roadmap** (e relativo project management) **per la resilienza** delle organizzazioni ai cyber-attacchi.

CTF vs CTF Attack and Defense

COME COSTRUIRE UNO SCENARIO REALE

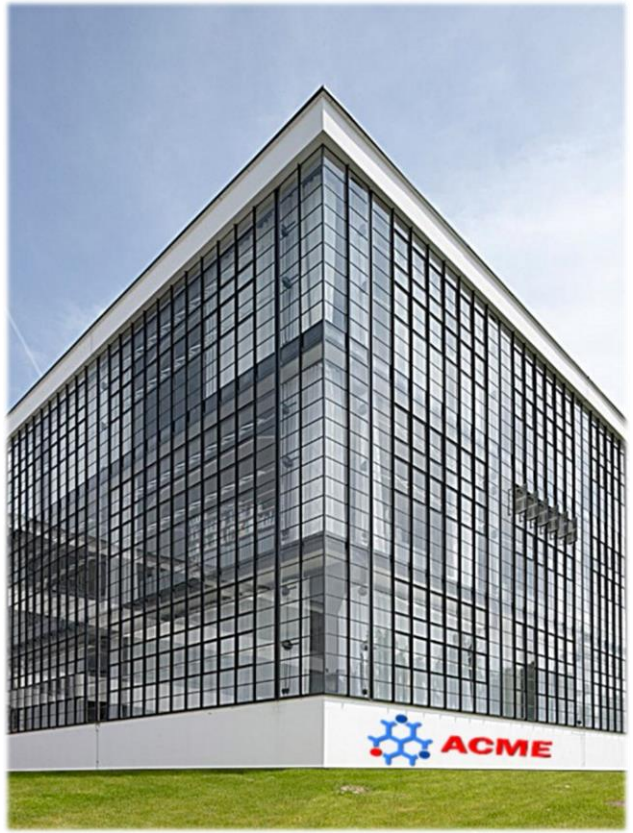
CTF (Capture The Flag)

- Scopo: valutazione Red team
- Scoring: sottomissione di flag
- Blue team inesistente
- Challenges poco realistiche

CTF - Attack and Defence

- Scopo: valutazione dei team coinvolti
- Scoring: comportamentale, team, organizzativo, tecnico
- Presenza del Blue e spesso anche di ulteriori teams
- **Simulazione di uno scenario reale**

Caso d'uso: ACME Corporation



Chi Siamo

La **ACME Corporation**, è stata fondata negli anni '70, oggi è una multinazionale di successo che opera nel campo delle tecnologie innovative applicate a: armi, robotica, attrezzature mediche, aeronautica, genetica, telecomunicazioni, energia. È la principale fornitrice di armamenti per l'esercito americano e per altri governi "allineati".

La sede principale è locata a Cameron (Arizona). **Dal 2017, l'azienda è presente anche in Italia con un nuovo centro di ricerca e sviluppo a Nera Montoro**.

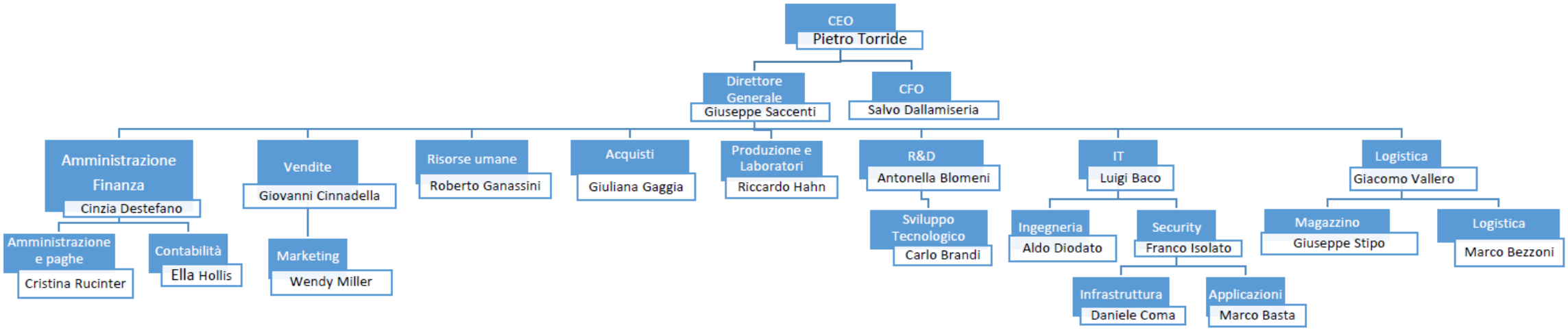
Blue team Mission

Il gruppo ACME necessita di una nuova struttura di specialisti dedicati alla **Cyber Security**…

Organigramma

ACME

ORGANIGRAMMA AZIENDALE



I 2 portali web

ACME

Benvenuti sulla pagina di ACME corporation.
Presto saremo online con una nuova versione del sito.

Information Security Management ISO 27001 Certified

SITO **ATTIVO** DAL **30/10/18**

ACME

Home Lavora con noi **Chi siamo** Dove siamo Contatti

Chi siamo

La ACME Corporation, è stata fondata negli anni '70 da William Bell. Oggi è una multinazionale di successo che opera nel campo delle tecnologie innovative nei settori armi, robotica, attrezzature mediche, aeronautica, genetica, farmaceutica, telecomunicazioni, energia, trasporti e intrattenimento. È la principale fornitrice di armamenti per l'esercito americano e per altri governi "allineati". La sede principale è locata a Cameron (Arizona). Dal 2017, l'azienda è presente anche in Italia attraverso un nuovo

ARTICOLI RECENTI

- Nera Montoro (Terni) Acme Corporation investe 25 milioni nella ricerca oncologica
- Bioupper: selezionati i 3 progetti vincitori del voucher di 160mila euro
- Acme Corporation completa l'acquisizione di TRUSTVITA, un'azienda biofarmaceutica focalizzata sull'oncologia

SITO **ATTIVO** DAL **10/11/18**

Le componenti tecnologiche

Theatre components	Defense components	Target components
▪ Network topology • Server VLAN • Client VLAN • DMZ VLAN • Management VLAN ▪ External firewall ▪ Domain Controller • Default users' profiles • DNS Server • DHCP Server	SIEM system	Mail server
	IDS server	Showcase website
	Service monitoring	FTP host
	Honeypot	Internal CRM
	NSM system	Internal NAS
	Web application firewall	Internal collaboration system
	... and more ...	External collaboration system
		IoT system
		CRM system
		... and more ...

Lo scenario

Sistemi IT: portali web, ftp, collaboration, active directory, gestione documentale, NAS, CRM

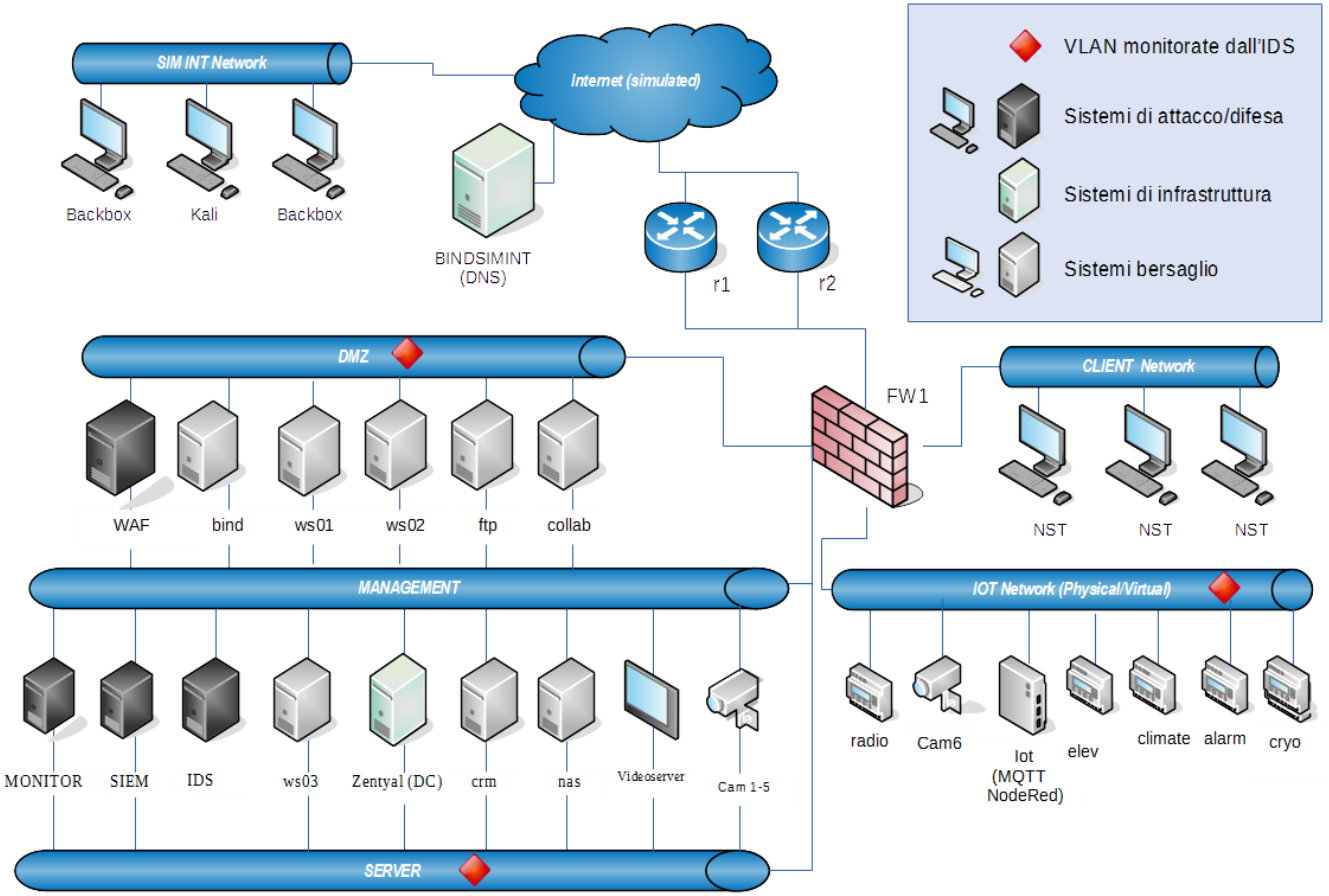
Videosorveglianza: telecamere, sistema per visualizzazione stream video

Iot (building automation)

Sensori

- Meteo
- Inquinamento/radioattività
- Allarmi anti-intrusione
- Ascensori
- Criogenici

Dashboard per la gestione degli allarmi



Componenti infrastruttura

- Web Application Server → **Apache HTTP, Apache Tomcat**
- Web Framework → **Wordpress**
- IoT → **Node-RED, Alpine Linux**
- Videosorveglianza → **OpenWrt**
- Business → **EspoCRM**
- Collaboration → **Collabtive, Zentyal Mail + XMPP**
- NAS and File Sharing → **FreeNAS**
- Domain Controller → **Zentyal**
- FTP & DNS → **ProFTP & Bind (Ubuntu 18.04)**

Strumenti di difesa

FIREWALL	→	**OPNsense**
IDS	→	**Suricata (Selks)**
WAF	→	**Apache mod_security**
SIEM	→	**Elasticsearch Logstash Kibana + Filebeat**
MONITORING	→	**Nagios**
VA	→	**OpenVAS**
HONEYPOT	→	**ARAMIS Deception System**
NST	→	**Network Security Toolkit**

I team

BLUE TEAM

Difesa dell'infrastruttura

Individuazione vulnerabilità

Fix vulnerabilità

Incident response

YELLOW TEAM

Simulare il comportamento dei **dipendenti** della ACME corporation

Simulare il comportamento dei **Clienti/Fornitori della ACME** Corporation

Segnalare disservizi nei sistemi

RED TEAM

Conseguire **obiettivi specifici**

GREEN TEAM

Monitorare il **funzionamento dell'infrastruttura**

Reset macchine

WHITE TEAM

Direzione gaming

Interloquire con i Blue Team

Valutazione dei Blue Team

Adversary simulation (purple team)

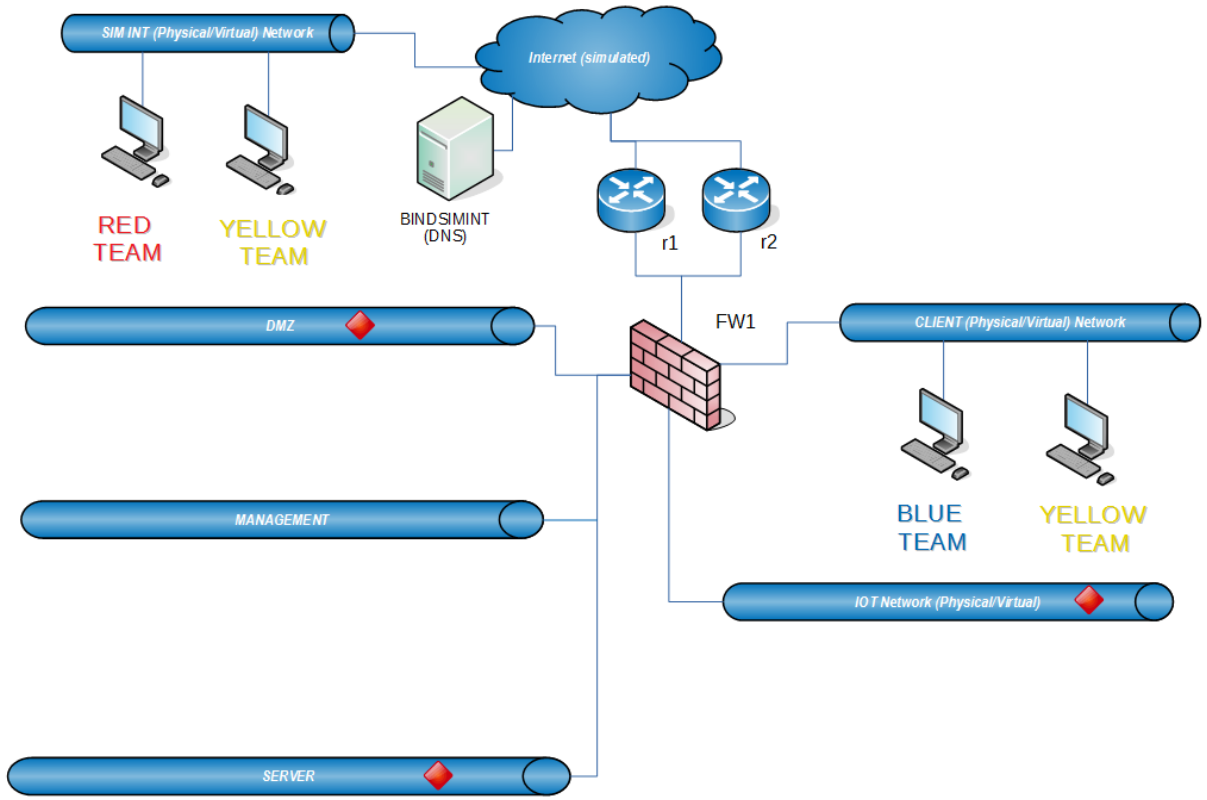
- **Processo cooperativo** tra Red Team e Blue Team
- **Purple team** unione tra i due mondi
- Il Red Team simula le operazioni di un vero attaccante allo scopo di evidenziare le debolezze del team difensore (tecniche, organizzative, strategiche)
- Il Red Team conosce a fondo i difensori
- Attività **white box**

Operation red flag

Posizionamento team: YELLOW TEAM

Azioni

- Iterazione con portali web
- Caricamento documenti su server ftp
- Inserimento e modifica progetti
- Accesso documenti aziendali (nas)
- Monitoraggio sistema videosorveglianza
- Controllo allarmi sistema IoT



Posizionamento team: **RED TEAM**

- **Personale altamente qualificato**
- Esecuzione di **campagne di attacco** pre-programmate

OBJECTIVE ID	OBJECTIVE STEP SCORE		OBJECTIVE DESCRIPTION	NETWORK_ZONE INVOLVED	LIST OF OBJECTIVE TARGET NODES	ATTACK EXIT EVIDENCE_DESCRIPTION
	STEP 1	STEP 2				
OBJ_1.1	100	300	Compromissione macchina in DMZ tramite scansione dei servizi attivi sui bersagli e attacco mediante vulnerabilità specifiche o credenziali di default	DMZ	ws01	screenshot on XMPP server; priviledge, time, IP on EtherPad
OBJ_1.4	100	300	Controllo e Neutralizzazione WAF (ipotesi WAF attivo)	DMZ - MGT	waf-vm	WAF Terminal window screenshot on XMPP server, time, IP on EtherPad
OBJ_1.6	300		Deface sito istituzionale internet	SERVER	ws03	screenshot on XMPP server, time on EtherPad
OBJ_1.8	300		Data Theft documento "IoT TechSpec" su NAS relativo alla specifica tecnica della rete IoT	SERVER	nas	hash del documento, o documento uploaded su XMPP
OBJ_1.9	200		Manomissione stream video videosorveglianza della telecamera su rete IoT	IOT	cam6	time on EtherPad
OBJ_1.10	600		Manomissione stream video videosorveglianza di almeno 2 telecamere su rete server	SERVER	camX (X=1..5)	time on EtherPad

Posizionamento team: **BLUE TEAM**

Studenti Universitari con diverse partecipazioni a eventi e CTF

Blue Team A, **Network e infrastructure**

- Gestione e configurazione apparati

Blue team B, **Application**

- Configurazione e gestione delle componenti applicative

STRUTTURA

- **1 responsabile Comunicazioni strategiche**
- **1 responsabile Comunicazione Informazioni Tecniche** (comunicazione verso White team, verso Green team nel caso di malfunzionamenti o richieste speciali)
- **5-6 Security Expert**

Le regole di ingaggio: **BLUE TEAM**

Salvaguardare il normale funzionamento dei servizi

- Eventuali **blocchi massivi** (es. un'intera subnet) comportano penalizzazioni sullo scoring. **Blocchi persistenti** oltre i 5 minuti vengono puniti con il reset delle macchine;
- **Tracciare ogni azione** eseguita sull'infrastruttura sui **report**;
- E' concesso **richiedere il reset di una singola macchina**. La macchina verrà riportata allo stato iniziale dell'esercitazione.

Informazioni disponibili

RED TEAM 

Prima [acquisisce informazioni]

- Conoscenza architettura
- Conoscenza vulnerabilità
- Esercitazione sull'infrastruttura precedente all'evento

BLUE TEAM 

Prima [essere preparati ed esperti]

- Conoscenza dei tool di difesa

Evento

- Architettura dettagliata del sistema
- Documentazione e credenziali accesso macchine

Scoring

La **valutazione del Blue team** avviene mediante la **somma pesata di diversi fattori**. I **pesi dei fattori non sono noti al Blue Team.**

AVAILABILITY DEI SERVIZI DI TEATRO

- Ogni disservizio comporta una penalità
- Blocco traffico legittimo
- Lo yellow team effettua una valutazione periodica dell'usabilità dei servizi

ATTACCHI ESEGUITI CON SUCCESSO

- Ogni obiettivo conseguito dal Red Team comporta una penalità

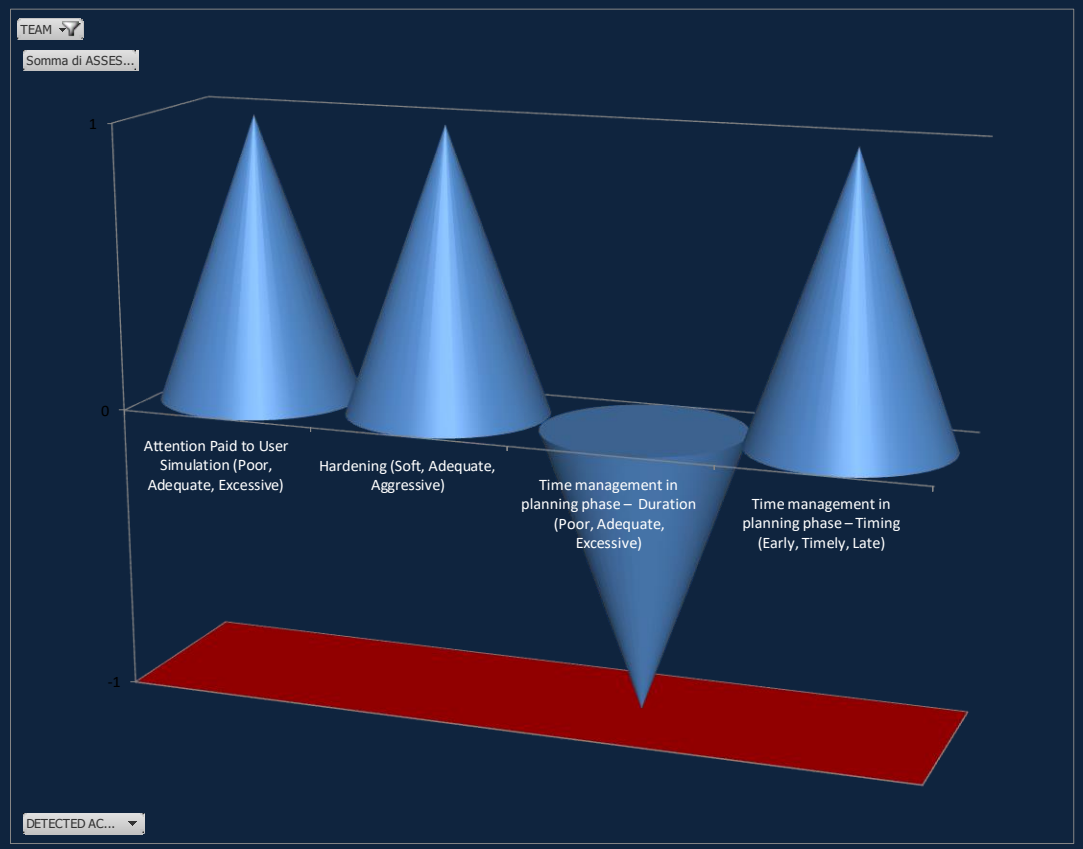
REPORTING

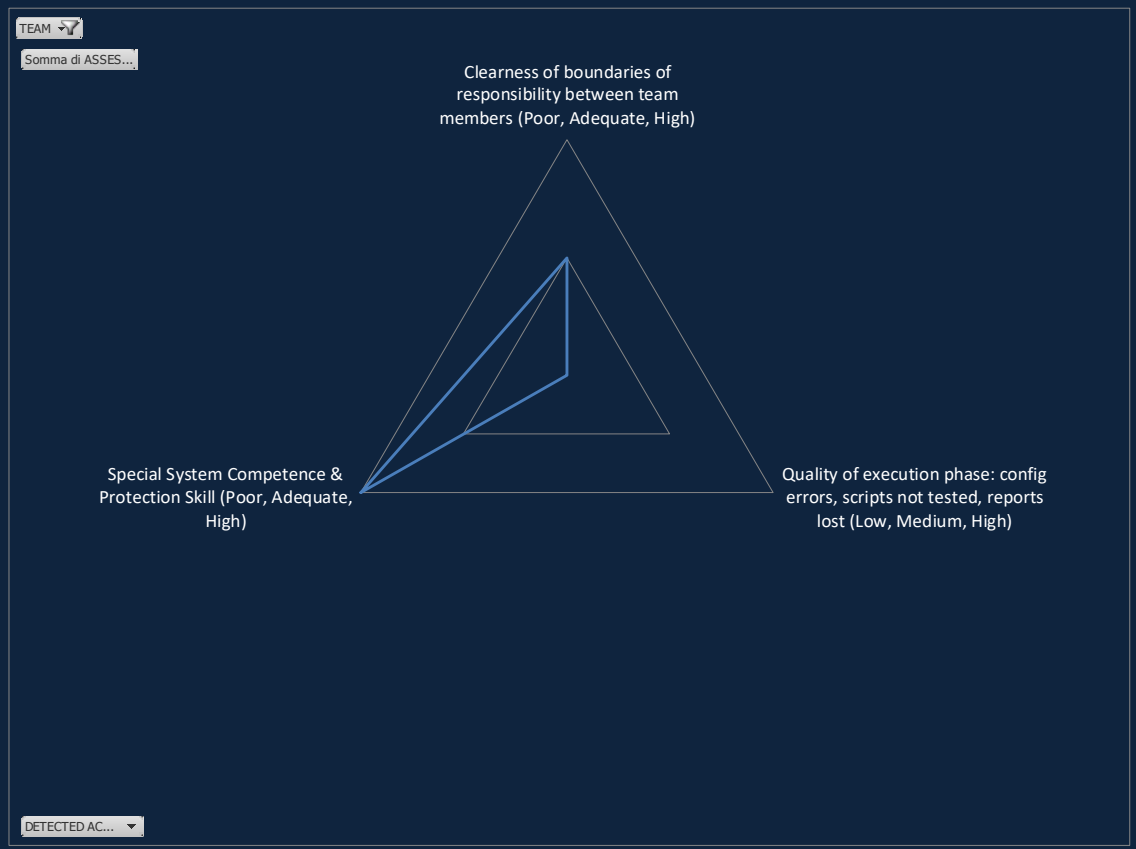
- Valutazione della qualità tecnica e dello stile comunicativo dei report
- Rispetto del ruoli assegnati, lavoro in team

RICHIESTE DI AIUTO

- Esempio reset delle macchine

Visual scoring





Organizzazione gaming

- Familiarizzazione ambiente di gaming
- Difesa preliminare (90 minuti)
- Reporting
- Attacco in linea fase 1 (90 minuti)
- Reporting 1
- Attacco in linea fase 2 (90 minuti)
- Reporting 2
- Debriefing

Difesa preliminare

- Durata **90 minuti**
- **Tempo a disposizione insufficiente** rapportato alla complessità dello scenario
- Solo il blue team aveva accesso all'infrastruttura
- Familiarizzare con gli strumenti
- **Individuare le vulnerabilità** (applicative, misconfiguration, rete, default password)
- **Risoluzione vulnerabilità**
- **Configurazione** degli strumenti di difesa

Attacco in linea

Fase 1 (90 minuti) + Reporting 1 (30 minuti)

Fase 2 (90 minuti) + Reporting 2 (30 minuti)

RED TEAM

- Conseguire obiettivi specifici

VS

BLUE TEAM

- Bug fixing
- Security monitoring
- Incident response
- Team coordination

Technical reporting

- Minaccia
- Quando
- Componenti interessate
- Impatti
- Azioni intraprese

THREAT DETECTION REPORT	
EXERCISE	Cyber_Exercise
PHASE	
BLUE TEAM	
ISSUER (TAG)	
REPORT ISSUEING TIME	
REPORT TEMPLATE VERSION	v1.0.0
REPORT ID	
REPORT TITLE	
THREAT DESCRIPTION	
AFFECTED NETWORK ZONES	
DETECTED/DECLARED IOC	
BEHAVIOURAL IOC LIST	
HOST IOC LIST (FILES, COMMANDS, EXE, DLL, REGISTRY DATA, DBRECORDS, ...)	
NETWORK IOC LIST (URL, IP, DOMAINS, HOSTNAMES)	
OTHER NOTES ON THREAT DETECTION	

ACTION REPORT	
EXERCISE	Cyber_Exercise
PHASE	
BLUE TEAM	
ISSUER (TAG)	
REPORT ISSUEING TIME	
REPORT TEMPLATE VERSION	v1.0.0
REPORT ID	
REPORT TITLE	
AFFECTED NETWORK ZONES	
ACTION	

INCIDENT REPORT		
EXERCISE	Cyber_Exercise	
PHASE		
BLUE TEAM		
ISSUER (TAG)		
REPORT ISSUEING TIME		
REPORT TEMPLATE VERSION	v1.0.0	
REPORT ID		
REPORT TITLE		
INCIDENT SEVERITY		
INCIDENT ASSIGNED OWNER		
IMPACTS	Involved Usernames	
	Involved Client	
	Involved Services	
	Notifying Defense Tool / Platform	
	Detected Signature	
TIME LINE	DATE/TIME	ACTION
ROOT CAUSE ANALYSIS & EVIDENCE GATHERING		
MITIGATION, ERADICATION & IMPROVEMENT PLAN (ACTION, OWNERSHIP,TIMING)		

Management report

Fornire informazioni utili agli organi preposti a prendere decisioni (*decision maker*)

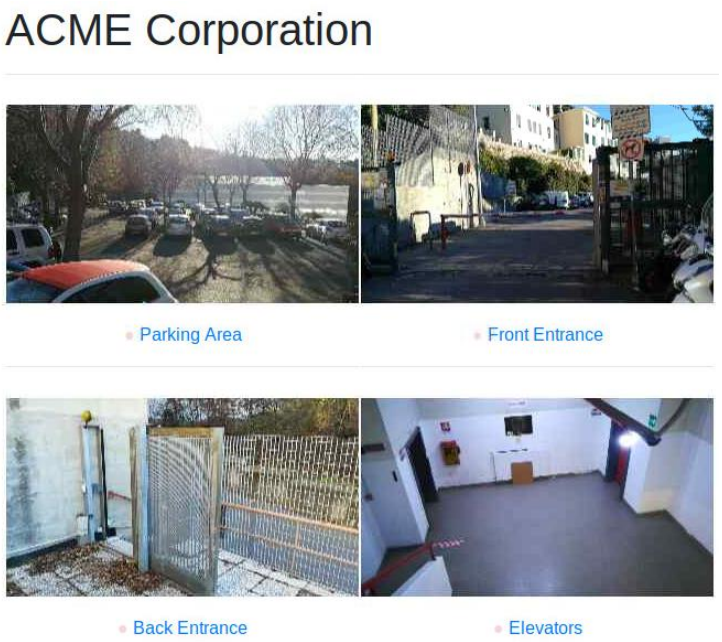
OFF LINE DEFENSE TECHNICAL REPORT	
EXERCISE	Cyber_Exercise
PHASE	0
BLUE TEAM	
ISSUER (TAG)	
REPORT ISSUEING TIME	
REPORT TEMPLATE VERSION	v1.0.0
REPORT ID	
REPORT TITLE	OFF LINE DEFENSE TECHNICAL COMMUNICATION REPORT
TIMELINE	DETECTION / ACTION

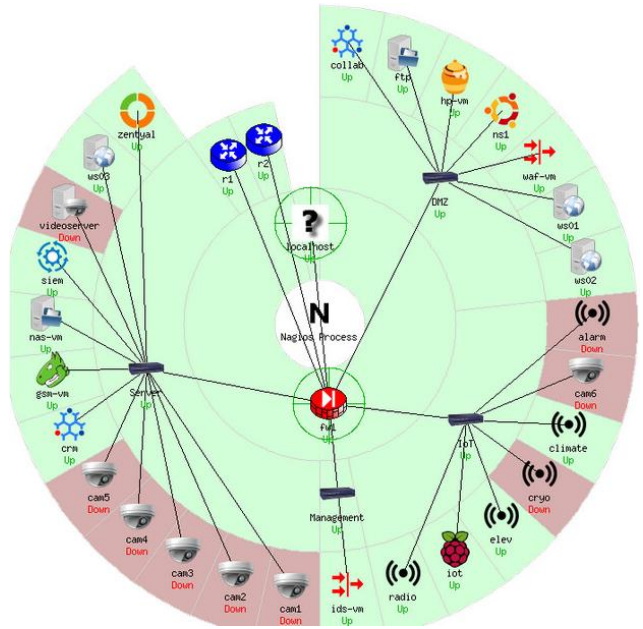
OFF LINE DEFENSE STRATEGICAL COMMUNICATION REPORT	
EXERCISE	Cyber_Exercise
PHASE	0
BLUE TEAM	
ISSUER (TAG)	
REPORT ISSUEING TIME	
REPORT TEMPLATE VERSION	v1.0.0
REPORT ID	
REPORT TITLE	OFF LINE DEFENSE STRATEGICAL COMMUNICATION REPORT
TIMELINE	DETECTION / ACTION

Situational awareness

Fornire una visione di ciò che accade all'interno dello scenario, **effettuare proiezioni** e **valutazione degli eventi** futuri

- **Team in gioco**
- **Spettatori** che osservano l'esercitazione





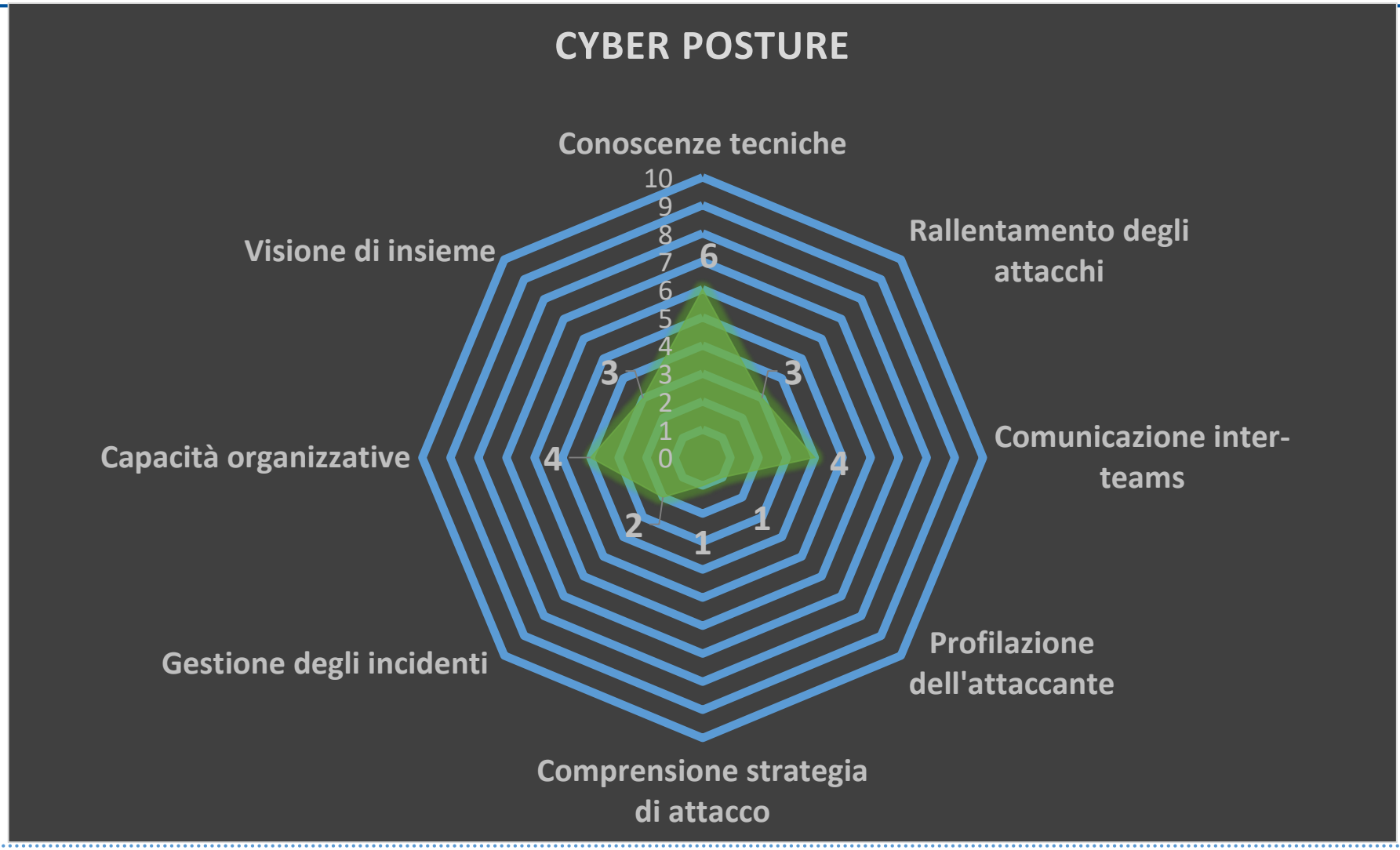
Cyber posture

La **cyber posture** misura la **capacità** dell'organizzazione **di difendersi**

"The security status of an enterprise's networks, information, and systems based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes" **NIST SP 800-128**

- Valutazione del **grado generale di sicurezza** di un infrastruttura
- **Elementi principali**: persone, hardware, software, policy
- **Rapid response**

Valutazione della cyber posture



Debriefing

- Conoscenze Tecniche
- Competenze Comunicative
- Competenze Strategiche
- Attack profiling
- Gestione incidenti

Conoscenze tecniche

I partecipanti hanno mostrato una **buona preparazione sul fronte tecnico**:

- Metodologie hardening
- Firewalling
- Networking
- It operation

Firewall, WAF, IDS, dispositivi di protezione devono essere visti come **l'estensione delle capacità umana** e non come unico e autonomo elemento su cui basarsi

Modalità comunicative e lavoro di squadra

Competenze comunicative

- **Poca attenzione alle comunicazioni** per lo **Yellow team**. Esempi: cambio password della dashboard per il monitoraggio sistema IoT, modifica impostazioni con impatto sullo Yellow team;
- **Discreto interscambio di informazioni** tra **Blue team A** e **Blue team B.**

Competenze strategiche/ Visione di insieme

- **Mancata richiesta degli asset sensibili** dell'infrastruttura;
- **Honeypot non sfruttata al meglio**. Mancata redirection del traffico malevolo verso l'Honeypot:
  - Rallentare gli attacchi;
  - Valutare accuratamente la strategia difensiva.

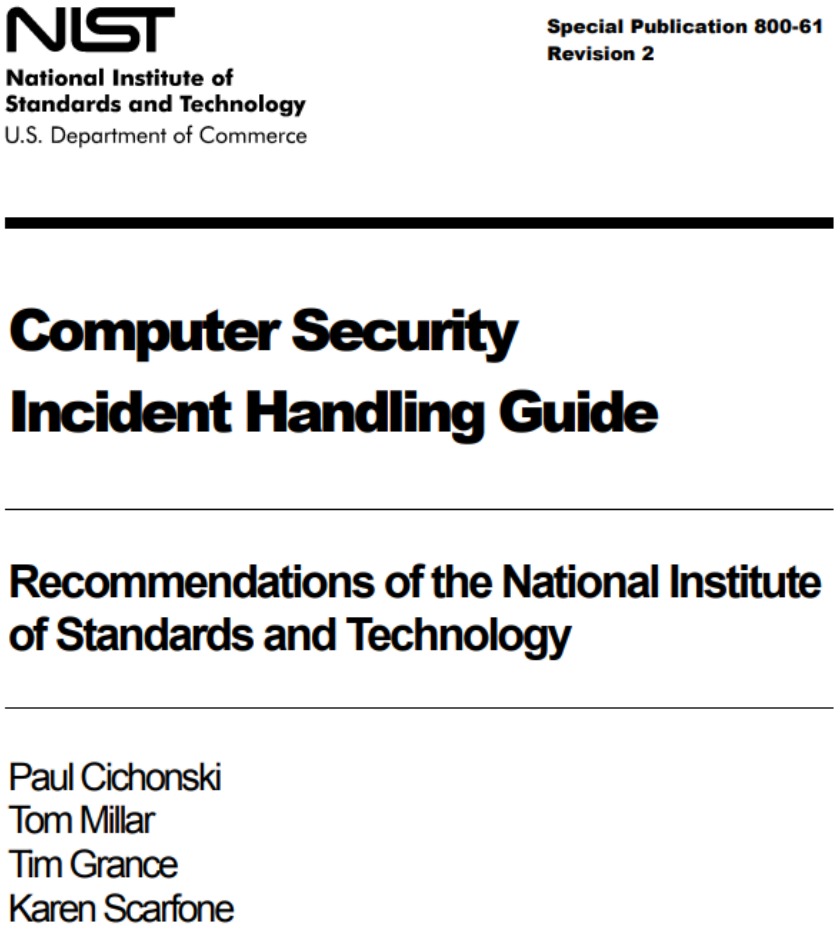
CONOSCERE L'ATTACCANTE: Attack profiling

Scarsa attenzione

- Tools utilizzati
- Scopo
- Motivazioni
- Skills

Gestione degli incidenti

- Preparazione
- Bassa capacità di identificare l'attaccante
- Limitata capacità di protezione
- Assenza di reazione integrata
- NIST 800-61 / Assenza di linee guida


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security
Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

Lessons learned

- Per **contrastare il Cybercrime** sono necessarie **nuove competenze**, metodologie e **processi di apprendimento**
- Le **conoscenze tecniche** sono la **base di partenza** su cui formare i nuovi esperti di Cyber Security, ma non sono sufficienti
- **Necessario** migliorare le capacità comunicative, gestionali, strategiche, **acquisire un nuovo mindset (agire)**
- La **carenza di competenze strategiche e tattiche**, come evidenziate nell'esercitazione, rispecchiano le lacune che si riscontrano quotidianamente nelle **organizzazioni reali**
- La **formazione** e **l'addestramento** in ambienti virtuali rivestono un **ruolo fondamentale** per raggiungere livelli elevati di consapevolezza e adeguata cyber posture

aizoon® AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

AUSTRALIA
Sydney NSW

EUROPE
Torino ITA | Cuneo ITA | Milano ITA | Genova ITA
Bologna ITA | Roma ITA | Bari ITA | Sheffield UK | Zürich CH

USA
New York NY | Troy MI
Cambridge MA | Lewiston ME

www.aizoongroup.com
aizoon@aizoongroup.com
aizoon Technology Consulting
@aizoongroup