Cyber Test Systems

Cyber Test Systems

Build Cyber Range Cyber Defense Training Center to run Cyber Exercises

Gregory FRESNAIS
Co-founder
+ 33 6 72 51 09 22
gregory.fresnais@cybertestsystems.com

Company Introduction

- Privately Founded the 10 of June 2014 at La Defense in Courbevoie, France.
- Co-Founders Gregory FRESNAIS 38 years old and Laurent CHABENET 37 years old.
- More than 17 years working in test and measurement industry (7 Years Spirent, help NSS Lab and BroadBand Testing to build their tests, BreakingPoint 5 Years, 2 Years IXIA, 3 Years Cyber Test Systems).
- Winner of FIC International Cybersecurity Forum’s 2016 Innovative SME Award from among almost 60 startups.

- Cyber Test Systems provides affordable Network Traffic Generator CTS-NTG solutions able to help you to run functional, performance, security, stability and high-availability tests on your network infrastructure replicating real world by generating legitimate and malicious traffic.
- **Cyber Test Systems designs Cyber Range Cyber Defense Training Center for education, service providers, system integrators, enterprises, defense contractors and governments in North America, South America, Europe, Middle East, Africa and Asia Pacific. We can help you to build your Cyber Range in your country.**

Our Main Activities

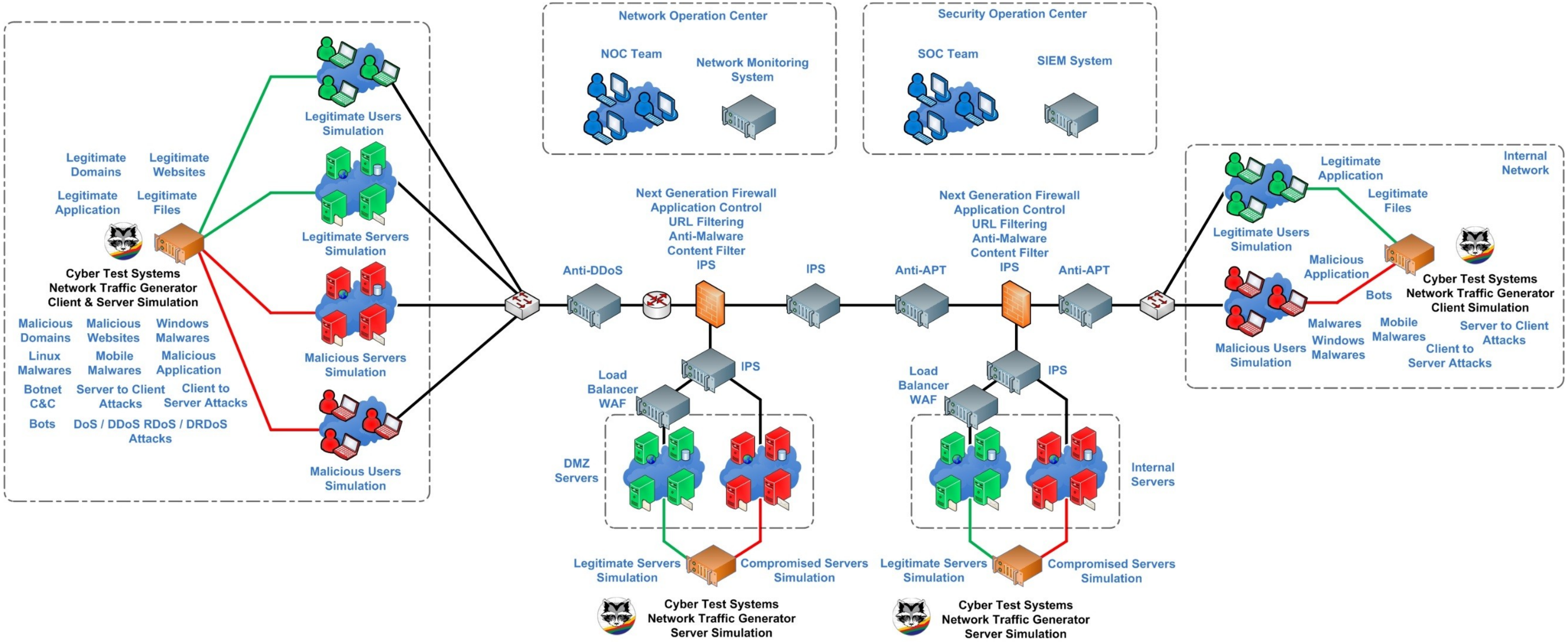
- Cyber Test Systems - Network Traffic Generator CTS-NTG Appliances
  - 1 Mbps to 400 Gbps traffic generation capabilities in 1U
  - CTS-1004-A, CTS-1008-A, CTS-1016-A with 1 GigE interfaces
  - CTS-1020-B, CTS-1040-B, CTS-NTG-1080-B with 1/10 GigE interfaces
  - CTS-1080-C with 40 GigE interfaces
  - CTS-NTG-1200-D, CTS-NTG-1400-D with 100 GigE interfaces

- Cyber Test Systems - Cyber Range Defense Training Center
  - Build entire Cyber Range Defense Training Center for governmental and non governmental organizations.
  - Deliver Cyber Range Cyber Defense Training Session hands-on (Green/Red/Yellow/Blue/White teams).

- Cyber Test Systems - Professional Services
  - Help to run functional, performance, security, stability and high-availability tests on network infrastructure replicating real world by generating legitimate and malicious traffic.

What is a Network Traffic Generator ?

Cyber Test Systems



- Cyber Test Systems Network Traffic Generator CTS-NTG is an hardware equipment able to replicate real world by generating clients, servers, IoT devices and ICS/SCADA systems generating legitimate and malicious traffic.

Founders background

- 17+ years working in test and measurement industry
- 17+ years experience in networking and programming
- 17+ years experience in delivering professional services
- Hardware expertise : Product management of new hardware platform
- Software expertise : C, Kernel, PHP, Javascript, HTML5/CSS3, Perl, TCL, Bash, SQL
- Automation expertise : Strong experience with test automation and large databases

- Cyber Security expertise:
  - Deliver Cyber Range Cyber Defense Training Session hands-on
  - Design and Build Cyber Range Defense Training Center Infrastructure
  - Design and Build Information Assurance (IA) Infrastructure
  - Design and Build Security Operation Center (SOC) Infrastructure

- Military expertise :
  - Participation to Combined Endeavor from 2003 to 2014
  - Participation to Pacific Endeavor from 2012 to 2016
  - Participation to CYDEX 2016, CDANS UK 2017, DEFNET 2017, LOCKED SHIELD 2017

Testing Expertise

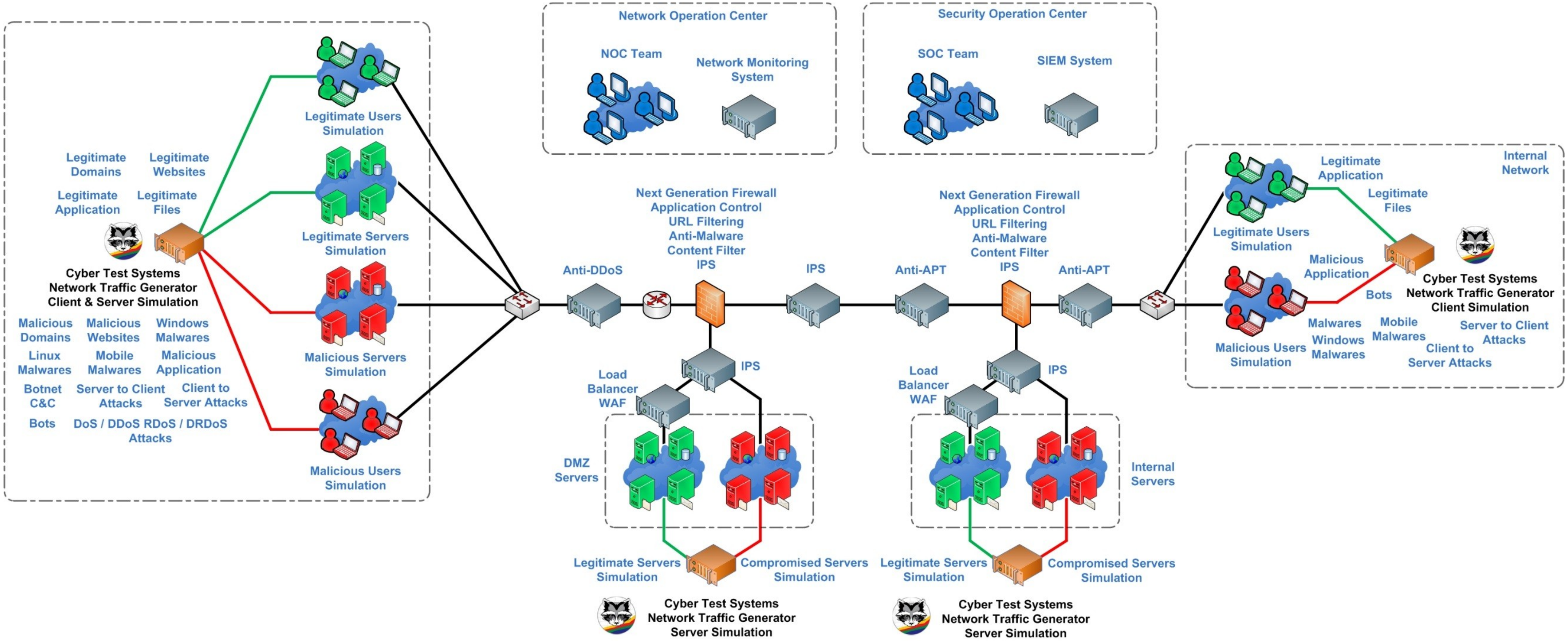
Cyber Test Systems

- Network Traffic Generator
- Application Traffic Generator
- TAP and Aggregator
- Network Packet Broker
- Switch
- Router
- Firewall
- Next Generation Firewall
- IPSec VPN Gateway
- SSL VPN Gateway
- Web Application Firewall (WAF)
- IDS/IPS
- Cache
- Transparent and Explicit Proxy
- Anti-Adwares
- Anti-Virus
- Anti-Malwares
- Anti-Spywares
- URL Filter
- Content Filter
- SMTP Relay
- Anti-Spam
- WAN Accelerator
- Anti-Advanced Persistent Threat (APT)
- Network Data Loss Prevention
- QoS DPI
- Application DPI
- Load Balancer
- Anti-DDOS System
- Anti-Botnet System
- Lawful Intercept System
- Data Retention System / Full Packet Capture System
- Network Monitoring Platform
- SIEM
- Desktop End Point Security
- Mobile End Point Security
- ICS/SCADA Security Solution
- Desktop and Laptop
- Servers
- Mobile and Tablets
- IoT Devices
- ICS / SCADA Devices

What is Traffic Network Generator ?

What is a Network Traffic Generator ?

Cyber Test Systems



- Cyber Test Systems Network Traffic Generator CTS-NTG is an hardware equipment able to replicate real world by generating clients, servers, IoT devices and ICS / SCADA systems generating legitimate and malicious traffic.

Cyber Test Systems Network Traffic Generator CTS-NTG High-Level Product Capabilities

Replicate Traffic of Large Diversity of Platforms

- Desktop

- Laptop

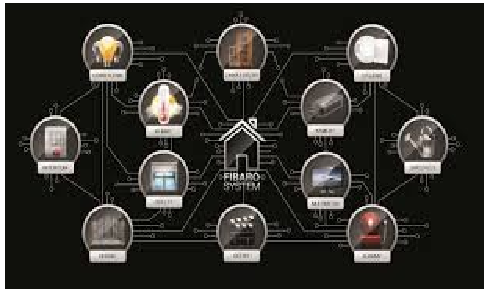
- Mobile

- Tablet

- Gaming Console

- Smart Health

- Smart Home



- Smart TV

- CCTV

- ICS / SCADA

- Drone

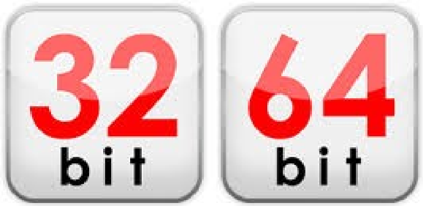
Replicate Traffic of Large Diversity of OS

- Windows

- Unix / Linux

- Mac

- 32 Bit and 64 Bit



- Android

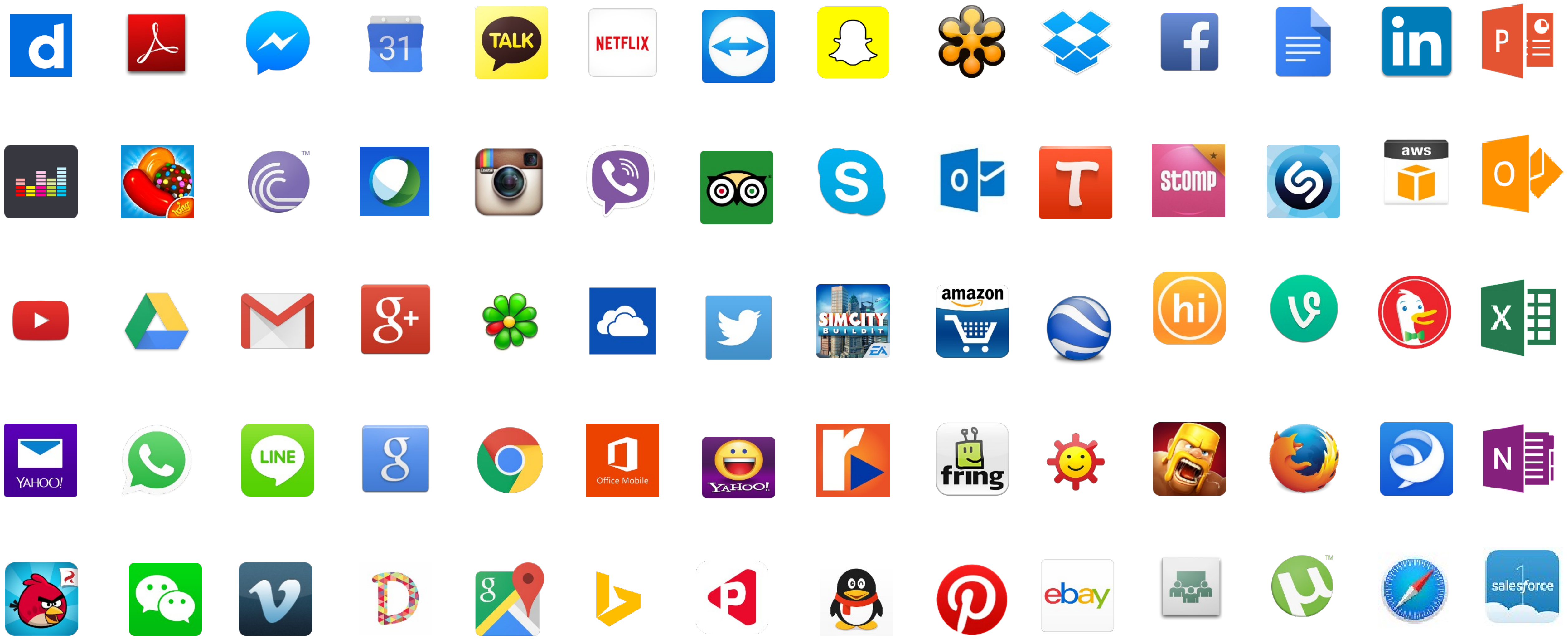
- iOS

- Windows Phone

- BlackBerry OS

Replicate Traffic of Large Diversity of Legitimate Applications

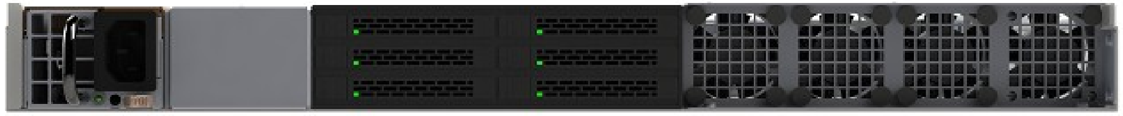
- Generation of client/server, peer-to-peer, web base, mobile and proprietary applications



Replicate Large Diversity of Malicious Traffic

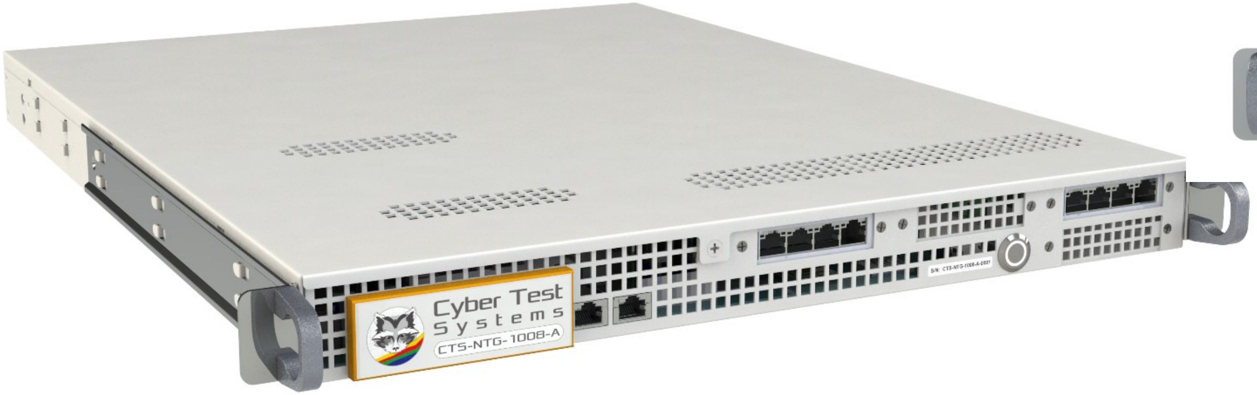
- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Reflective Denial of Service (RDoS)
- Distributed Reflective Denial of Service (DRDoS)
- Network Reconnaissance
- Application Reconnaissance
- Brute-Force
- Data Leakage
- Server Side Vulnerabilities and Exploits
- Client Side Vulnerabilities and Exploits
- Web Exploit Kits
- Malicious Domains
- Malicious Websites
- Malicious Phishing Websites
- Newly Emerging APT and Known Malwares for Windows, OS X, Linux, Android, iOS
- Botnet Communications between Command and Control (C&C) and Bots

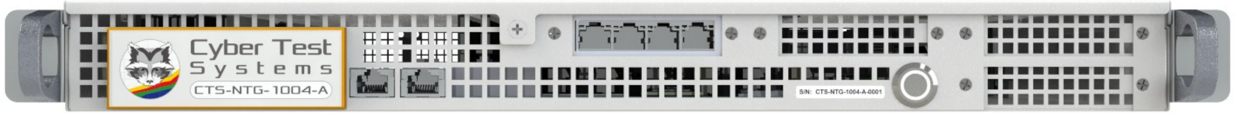
Network Traffic Generator CTS-NTG 1004-A

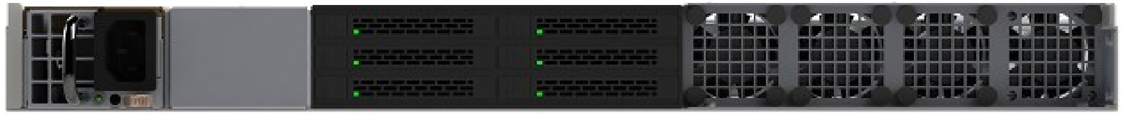


- 1U Portable Appliance
- 1x Port 10/100/1000 Copper for Management and 1x Port for Recovery
- 4x Ports 10/100/1000 Copper for Network Traffic Generation Max 4 Gbps
- 1x SSD for OS and removable for military sector
- 1x 1 TB for Storage in Raid 1 and removable for military sector

Network Traffic Generator CTS-NTG 1008-A



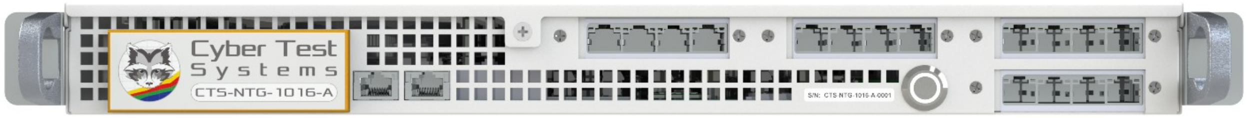


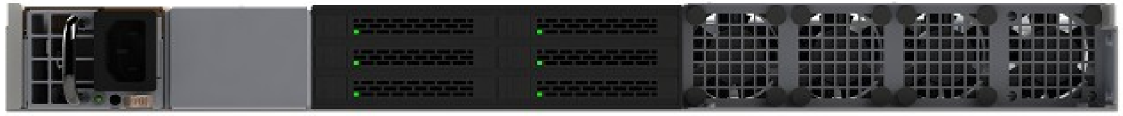


- 1U Portable Appliance
- 1x Port 10/100/1000 Copper for Management and 1x Port for Recovery
- 8x Ports 10/100/1000 Copper for Network Traffic Generation Max 8 Gbps
- 1x SSD for OS and removable for military sector
- 1x 1 TB for Storage in Raid 1 and removable for military sector

Network Traffic Generator CTS-NTG 1016-A

Cyber Test
Systems
CTS-NTG-1016-A



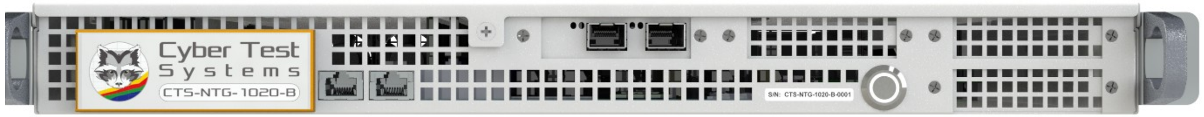


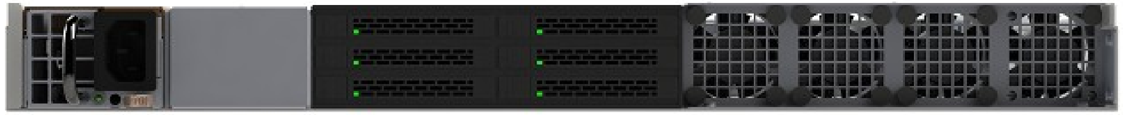
- 1U Portable Appliance
- 1x Port 10/100/1000 Copper for Management and 1x Port for Recovery
- 16x Ports 10/100/1000 Copper for Network Traffic Generation Max 16 Gbps
- 1x SSD for OS and removable for military sector
- 1x 1 TB for Storage in Raid 1 and removable for military sector

Network Traffic Generator CTS-NTG 1020-B

Cyber Test Systems

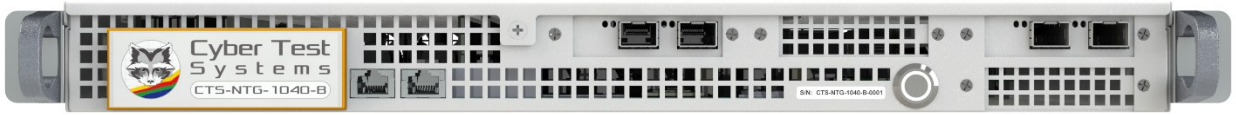
Cyber Test
Systems
CTS-NTG-1020-B

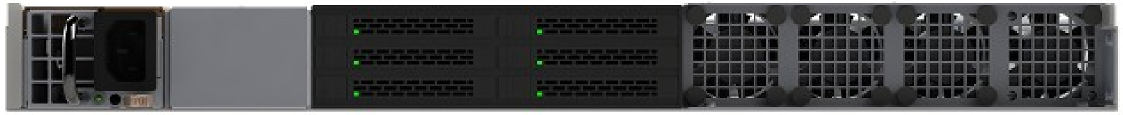




- 1U Portable Appliance
- 1x Port 10/100/1000 Copper for Management and 1x Port for Recovery
- 2x Ports 1/10 SFP/SFP+ for Network Traffic Generation Max 20 Gbps
- 1x SSD for OS and removable for military sector
- 1x 1 TB for Storage in Raid 1 and removable for military sector

Network Traffic Generator CTS-NTG 1040-B





- 1U Portable Appliance
- 1x Port 10/100/1000 Copper for Management and 1x Port for Recovery
- 4x Ports 1/10 SFP/SFP+ for Network Traffic Generation Max 40 Gbps
- 1x SSD for OS and removable for military sector
- 1x 1 TB for Storage in Raid 1 and removable for military sector

Network Traffic Generator CTS-NTG 1080-B

Cyber Test Systems

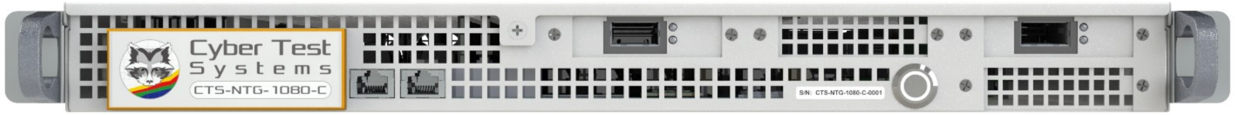
Cyber Test
Systems
CTS-NTG-1080-B

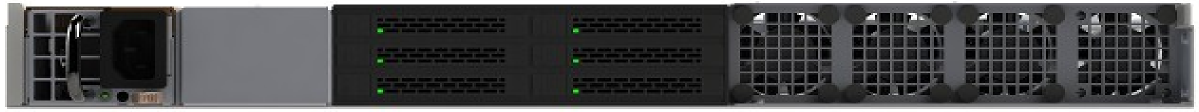
Cyber Test
Systems
CTS-NTG-1080-B

- 1U Portable Appliance
- 1x Port 10/100/1000 Copper for Management and 1x Port for Recovery
- 8x Ports 1/10 SFP/SFP+ for Network Traffic Generation Max 80 Gbps
- 1x SSD for OS and removable for military sector
- 1x 1 TB for Storage in Raid 1 and removable for military sector

Network Traffic Generator CTS-NTG 1080-C

Cyber Test
Systems
CTS-NTG-1080-C





- 1U Portable Appliance
- 1x Port 10/100/1000 Copper for Management and 1x Port for Recovery
- 2x Ports 40 GigE QSFP for Network Traffic Generation Max 80 Gbps
- 1x SSD for OS and removable for military sector
- 1x 1 TB for Storage in Raid 1 and removable for military sector

Network Traffic Generator CTS-NTG 1200-D

Cyber Test Systems

- 1U Portable Appliance
- 1x Port 10/100/1000 Copper for Management and 1x Port for Recovery
- 2x Ports 100 GigE QSFP28 for Network Traffic Generation Max 200 Gbps
- 1x SSD for OS and removable for military sector
- 1x 1 TB for Storage in Raid 1 and removable for military sector

Network Traffic Generator CTS-NTG 1400-D

Cyber Test Systems

- 1U Portable Appliance
- 1x Port 10/100/1000 Copper for Management and 1x Port for Recovery
- 4x Ports 100 GigE QSFP28 for Network Traffic Generation Max 400 Gbps
- 1x SSD for OS and removable for military sector
- 1x 1 TB for Storage in Raid 1 and removable for military sector

What is a Cyber Range ?

What is a Cyber Range ?

A Cyber Range is an infrastructure where you replicate a real environment like a pre-production in order to train and evaluate IT, Network Operations Center (NOC), Security Operations Center (SOC) and Cyber Incident Response (CIRT) teams working on their ability to execute their Cyber Incident Response Plans (CIRP) against single-vector and multi-vector cyber attack scenarios.

Board and C-Suite level participants could be trained in the areas of cyber threat awareness, risk management, business continuity planning, and crisis communications preparation.

A Cyber Range is composed, of 5 teams :

Red Team

Green Team

Yellow Team

Blue Team

White Team

What are the Team Roles in Cyber Range ?

Red Team

The Red Team simulates malicious users sending cyber attacks using Single Vector, Multi-Vectors and Campaigns.

Green Team

The Green Team simulates legitimate users over wire or wireless connections operating their desktops, laptops, tablets, smartphones accessing to the application infrastructure hosted on the network infrastructure managed by blue Team.

Yellow Team

The Yellow Team simulates innocent users member of the Green Team but time to time are clicking on phishing link or install malicious app without knowing.

Blue Team

The Blue Team simulates the IT, NoC, SoC, CIRT users managing the availability, the scalability, the security and the stability of network infrastructure and application infrastructure.

White Team

The White Team creates the cyber attacks scenarios and then monitor success or failure of blue team to defend properly against cyber attacks launched by red team, keeping availability, scalability, security and performance of network infrastructure and application infrastructure for green team.

Who use Cyber Range ?

- Militaries
- Governments
- Defense Integrators
- Network Equipment Manufacturers
- Service Providers
- Enterprises
- Universities and Polytechnics
- Science and Technology Research Institution

Cyber Attacks Scenarios - Single Vector and Multi-Vectors

- Single Vector type of Cyber Attacks Scenarios :
  - Type 1 - Denial of Service (DoS)
  - Type 2 - Distributed Denial of Service (DDoS)
  - Type 3 - Reflective Denial of Service (RDoS)
  - Type 4 - Distributed Reflective Denial of Service (DRDoS)
  - Type 5 - Network Reconnaissance
  - Type 6 - Application Reconnaissance
  - Type 7 - Brute-Force
  - Type 8 - Data Leakage
  - Type 9 - Server Side Vulnerabilities and Exploits
  - Type 10 - Client Side Vulnerabilities and Exploits
  - Type 11 - Web Exploit Kits
  - Type 12 - Malicious Domains
  - Type 13 - Malicious Websites
  - Type 14 - Malicious Phishing Websites
  - Type 15 - Newly Emerging and Known Malwares for Windows, OS X, Linux, Android, iOS
  - Type 16 - Botnet Communications between Command and Control (C&C) and Bots

- Multi-Vectors type Cyber Attacks Scenarios :
  - Combination of multiple single vectors cyber attacks scenarios combined together to be able to generate advanced type of cyber attack scenarios

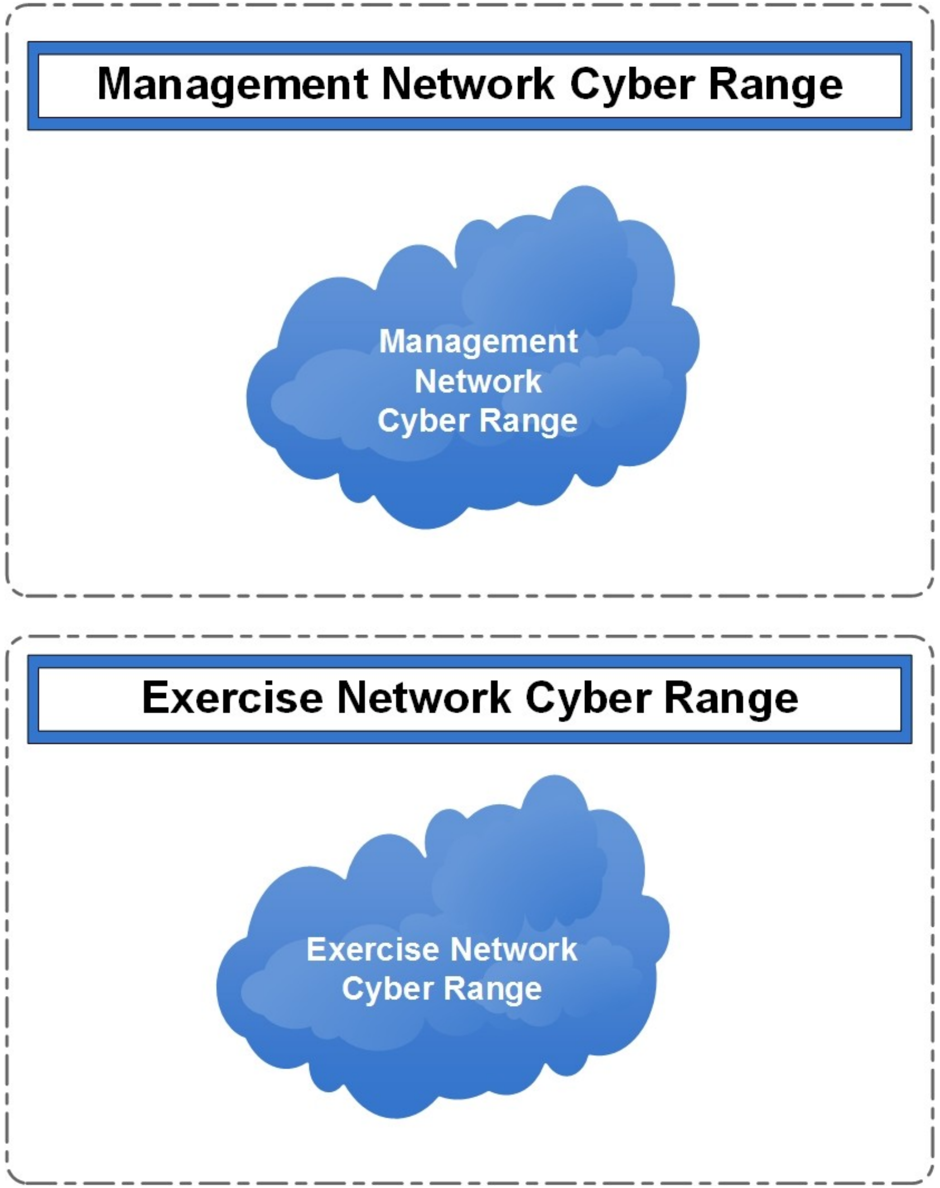
Components Deployed in Cyber Range

Cyber Test Systems

- Network Traffic Generator
- Application Traffic Generator
- TAP and Aggregator
- Network Packet Broker
- Switch
- Router
- Firewall
- Next Generation Firewall
- IPSec VPN Gateway
- SSL VPN Gateway
- Web Application Firewall (WAF)
- IDS/IPS
- Cache
- Transparent and Explicit Proxy
- Anti-Adwares
- Anti-Virus
- Anti-Malwares
- Anti-Spywares
- URL Filter
- Content Filter
- SMTP Relay
- Anti-Spam
- WAN Accelerator
- Anti-Advanced Persistent Threat (APT)
- Network Data Loss Prevention
- QoS DPI
- Application DPI
- Load Balancer
- Anti-DDOS System
- Anti-Botnet System
- Lawful Intercept System
- Data Retention System / Full Packet Capture System
- Network Monitoring Platform
- SIEM
- Desktop End Point Security
- Mobile End Point Security
- ICS/SCADA Security Solution
- Desktop and Laptop
- Servers
- Mobile and Tablets
- IoT Devices
- ICS / SCADA Devices

What is a Cyber Range Infrastructure ?

Cyber Test Systems

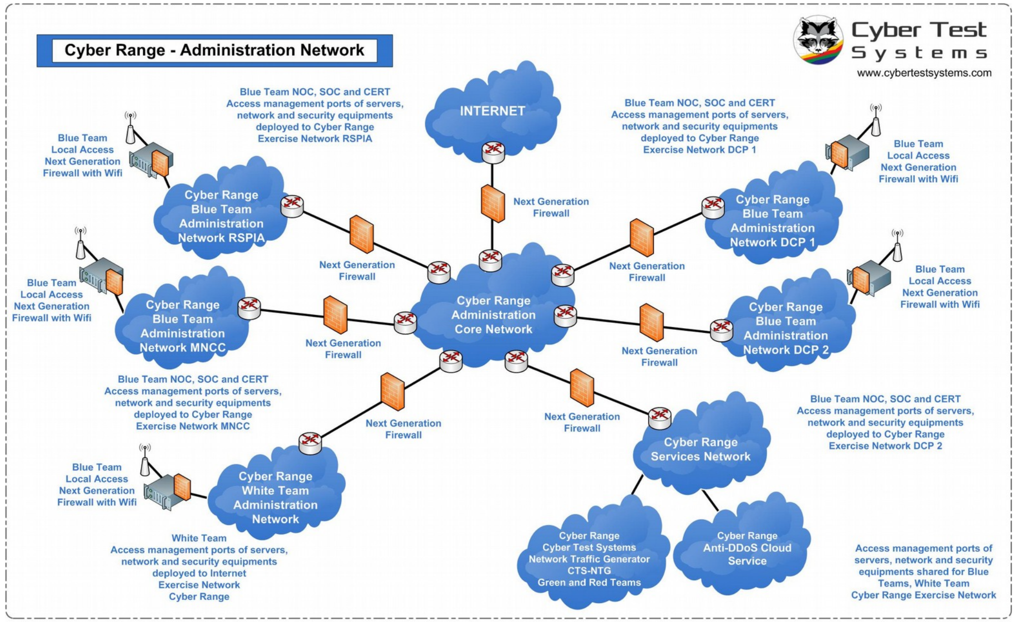

Management Network Cyber Range

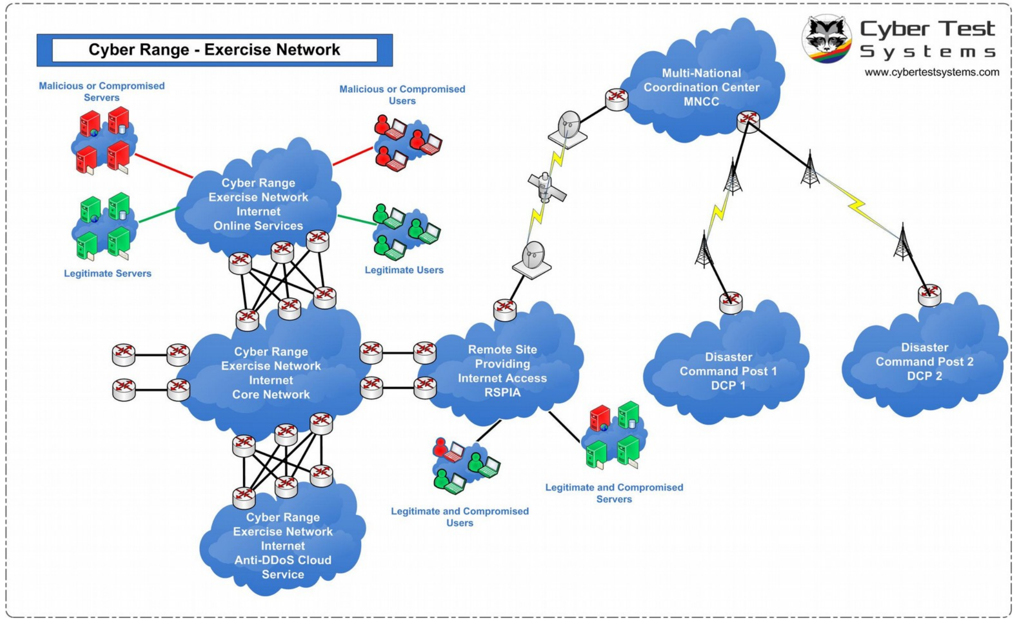
Management Network Cyber Range

Exercise Network Cyber Range

Exercise Network Cyber Range

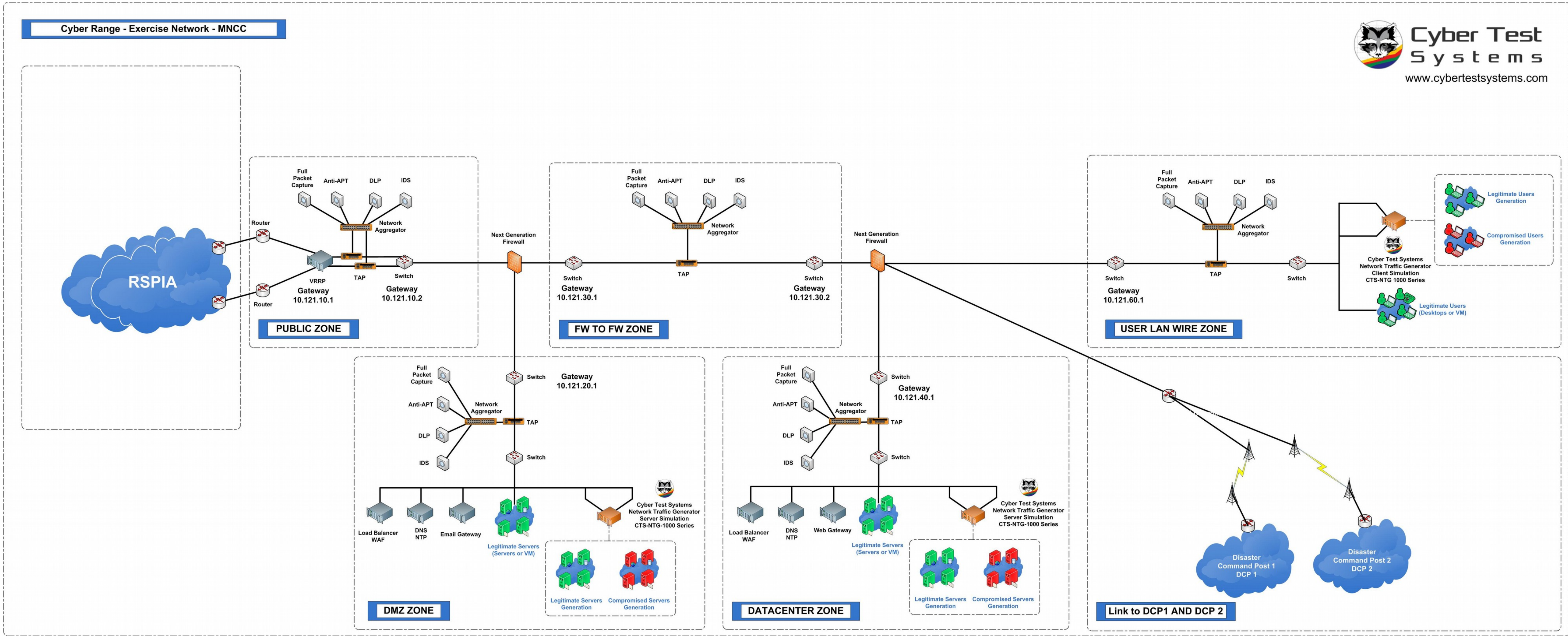
What is a Cyber Range Infrastructure ?


Cyber Range - Administration Network
Cyber Test Systems
www.cybertestsystems.com
INTERNET
Next Generation Firewall
Cyber Range Administration Core Network
Blue Team NOC, SOC and CERT Access management ports of servers, network and security equipments deployed to Cyber Range Exercise Network RSPIA
Blue Team Local Access Next Generation Firewall with Wifi
Cyber Range Blue Team Administration Network RSPIA
Next Generation Firewall
Blue Team Local Access Next Generation Firewall with Wifi
Cyber Range Blue Team Administration Network MNCC
Next Generation Firewall
Blue Team NOC, SOC and CERT Access management ports of servers, network and security equipments deployed to Cyber Range Exercise Network MNCC
Next Generation Firewall
Blue Team Local Access Next Generation Firewall with Wifi
Cyber Range White Team Administration Network
White Team Access management ports of servers, network and security equipments deployed to Internet Exercise Network Cyber Range
Blue Team NOC, SOC and CERT Access management ports of servers, network and security equipments deployed to Cyber Range Exercise Network DCP 1
Blue Team Local Access Next Generation Firewall with Wifi
Cyber Range Blue Team Administration Network DCP 1
Next Generation Firewall
Blue Team Local Access Next Generation Firewall with Wifi
Cyber Range Blue Team Administration Network DCP 2
Next Generation Firewall
Next Generation Firewall
Cyber Range Services Network
Blue Team NOC, SOC and CERT Access management ports of servers, network and security equipments deployed to Cyber Range Exercise Network DCP 2
Cyber Range Cyber Test Systems Network Traffic Generator CTS-NTG Green and Red Teams
Cyber Range Anti-DDoS Cloud Service
Access management ports of servers, network and security equipments shared for Blue Teams, White Team Cyber Range Exercise Network


Cyber Range - Exercise Network
Cyber Test Systems
www.cybertestsystems.com
Malicious or Compromised Servers
Malicious or Compromised Users
Cyber Range Exercise Network Internet Online Services
Legitimate Servers
Legitimate Users
Cyber Range Exercise Network Internet Core Network
Cyber Range Exercise Network Internet Anti-DDoS Cloud Service
Remote Site Providing Internet Access RSPIA
Legitimate and Compromised Users
Legitimate and Compromised Servers
Multi-National Coordination Center MNCC
Disaster Command Post 1 DCP 1
Disaster Command Post 2 DCP 2

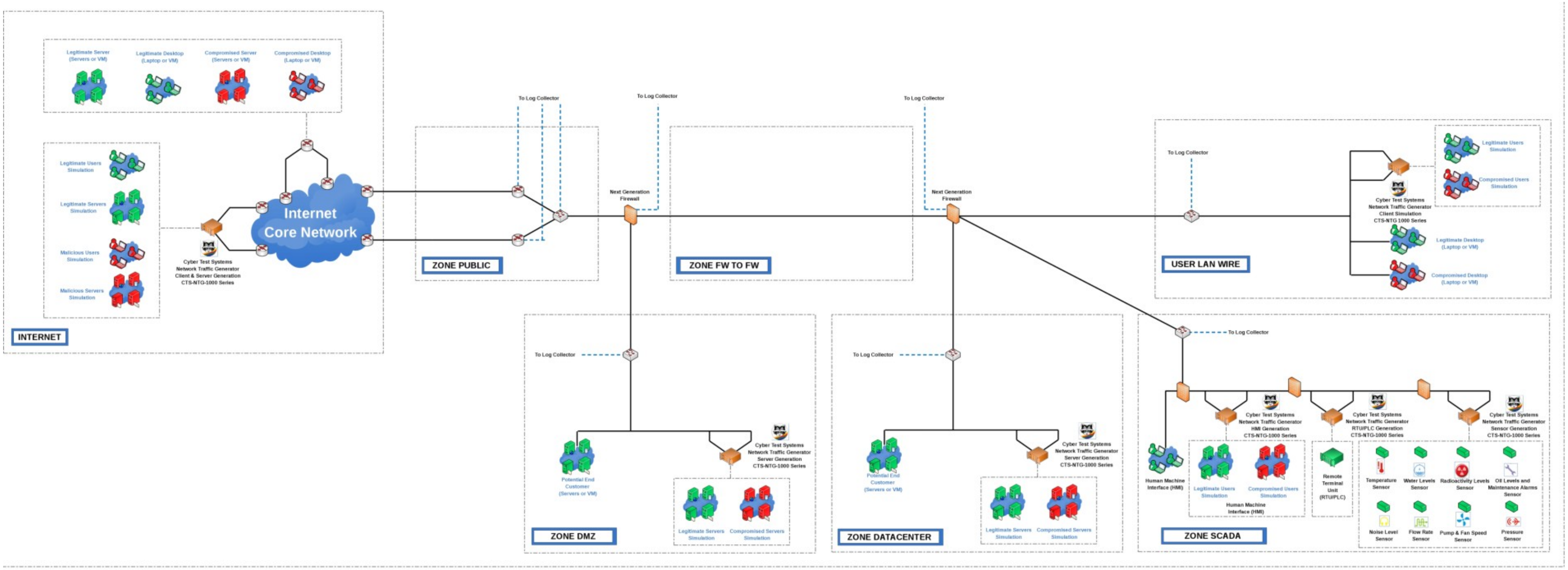
What is a Cyber Range Exercise Network ?

Cyber Test Systems



What is a Cyber Range Exercise Network with SCADA ?

Cyber Test Systems



Legitimate Server (Servers or VM)
Legitimate Desktop (Laptop or VM)
Compromised Server (Servers or VM)
Compromised Desktop (Laptop or VM)
Legitimate Users Simulation
Legitimate Servers Simulation
Malicious Users Simulation
Malicious Servers Simulation
Cyber Test Systems Network Traffic Generator Client & Server Generation CTS-NTG-1000 Series
Internet Core Network
INTERNET
To Log Collector
To Log Collector
To Log Collector
Next Generation Firewall
Next Generation Firewall
ZONE PUBLIC
ZONE FW TO FW
To Log Collector
Cyber Test Systems Network Traffic Generator Client Simulation CTS-NTG 1000 Series
Legitimate Users Simulation
Compromised Users Simulation
Legitimate Desktop (Laptop or VM)
Compromised Desktop (Laptop or VM)
USER LAN WIRE
To Log Collector
Potential End Customer (Servers or VM)
Cyber Test Systems Network Traffic Generator Server Generation CTS-NTG-1000 Series
Legitimate Servers Simulation
Compromised Servers Simulation
ZONE DMZ
To Log Collector
Potential End Customer (Servers or VM)
Cyber Test Systems Network Traffic Generator Server Generation CTS-NTG-1000 Series
Legitimate Servers Simulation
Compromised Servers Simulation
ZONE DATACENTER
To Log Collector
Cyber Test Systems Network Traffic Generator HMI Generation CTS-NTG-1000 Series
Cyber Test Systems Network Traffic Generator RTU/PLC Generation CTS-NTG-1000 Series
Cyber Test Systems Network Traffic Generator Sensor Generation CTS-NTG-1000 Series
Human Machine Interface (HMI)
Legitimate Users Simulation
Compromised Users Simulation
Human Machine Interface (HMI)
Remote Terminal Unit (RTU/PLC)
Temperature Sensor
Water Levels Sensor
Radioactivity Levels Sensor
Oil Levels and Maintenance Alarms Sensor
Noise Level Sensor
Flow Rate Sensor
Pump & Fan Speed Sensor
Pressure Sensor
ZONE SCADA

Cyber Test Systems

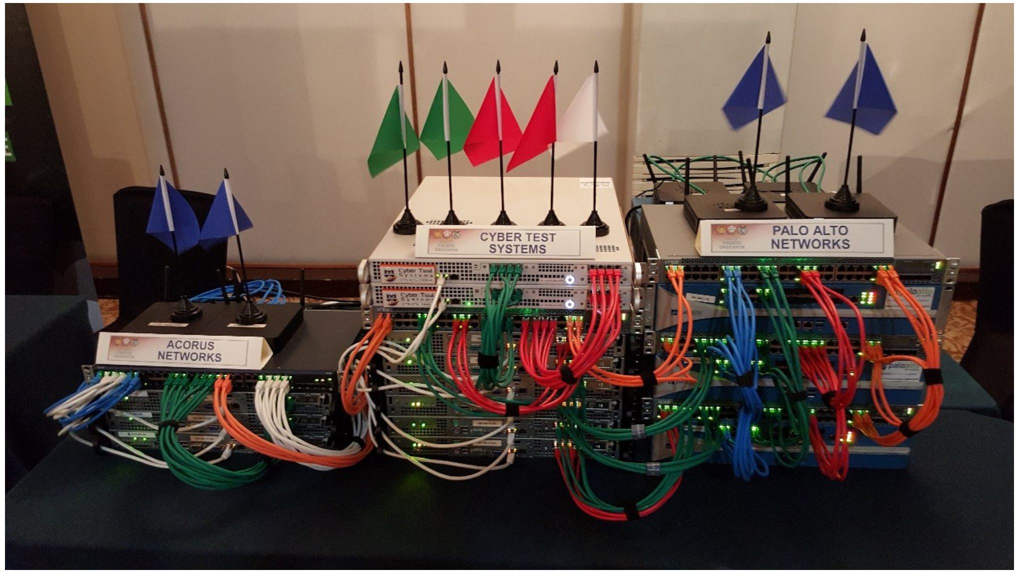
Cyber Range – Cyber Defense Training Center - References

Combined Endeavor 2014 Germany – Cyber Range - 42 nations

Cyber Test Systems provided the entire IA Network Infrastructure to monitor, identify and block attacks on Unclassified Network and Mission Network for 42 nations.

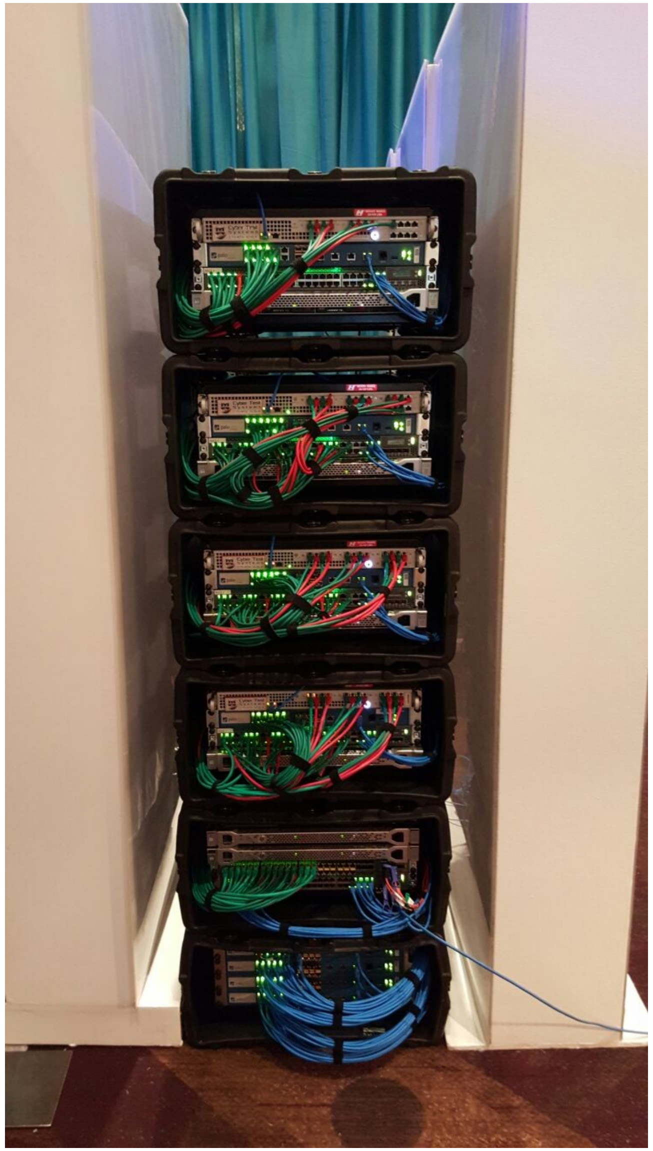
Pacific Endeavor 2015 Philippines – Cyber Range - 22 Nations

Cyber Test Systems



Palo Alto Networks Ignite 2016 US – Cyber Range

Cyber Test
Systems



SingTel Cyber Security Institute 2016 Singapore – Cyber Range

- SingTel Cyber Security Institure CSI is 10 000 square foot facility providing cyber skills development and education programmes tailored to the varying needs of company boards, C-suite management, technology and operational staff. Board and C-Suite level participants are trained in the areas of cyber threat awareness, risk management, business continuity planning, and crisis communications preparation.

- The cyber operations team are trained in incident response plan capabilities to sharpen their skills.

SingTel Cyber Security Institute 2016 Singapore – Cyber Range

Cyber Test Systems

NATO NIAS 2016 Belgium – Cyber Range

Cyber Test Systems
Test your Cyber Defense capabilities with Network Traffic Generator CTS-NT
Cyber Range
designed by Cyber Test Systems

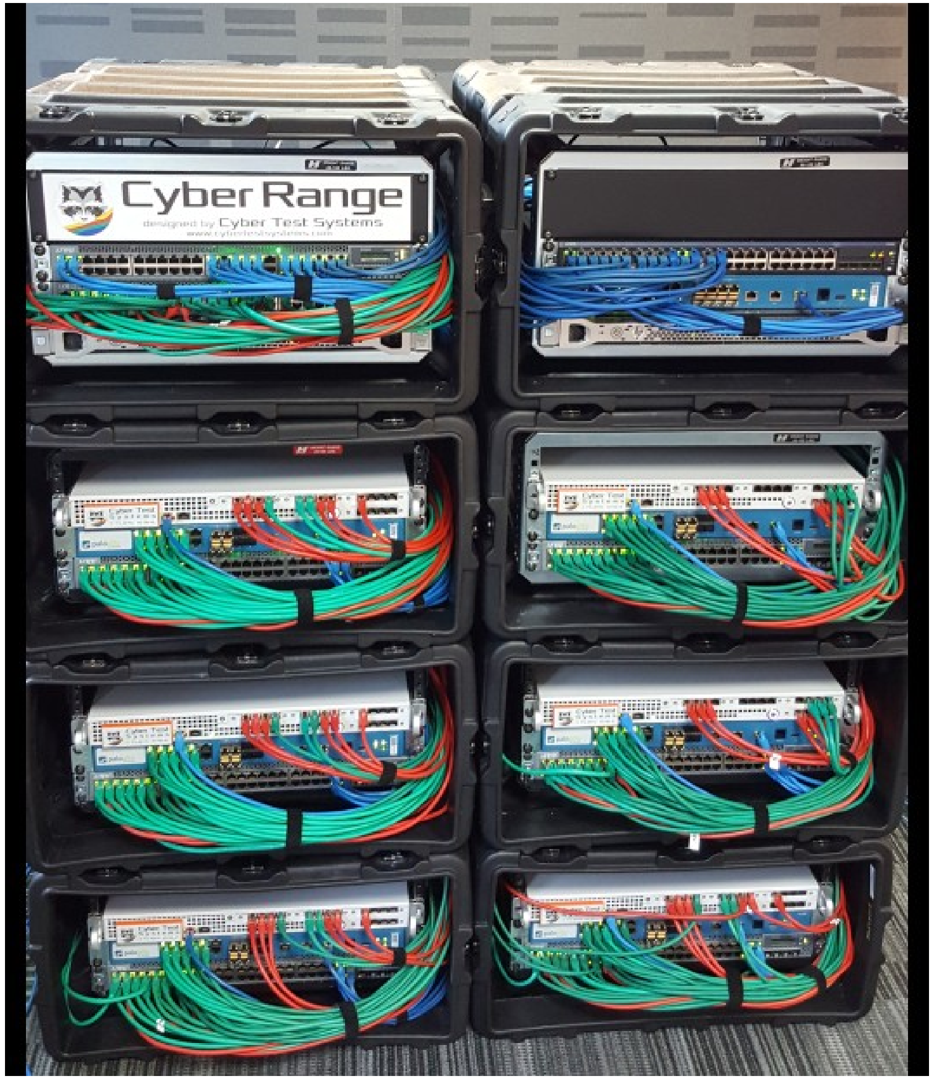
French Pavillon Cyber Range with French Cyber Security experts

Pacific Endeavor 2016 Australia – Cyber Range - 22 Nations

Cyber Test Systems

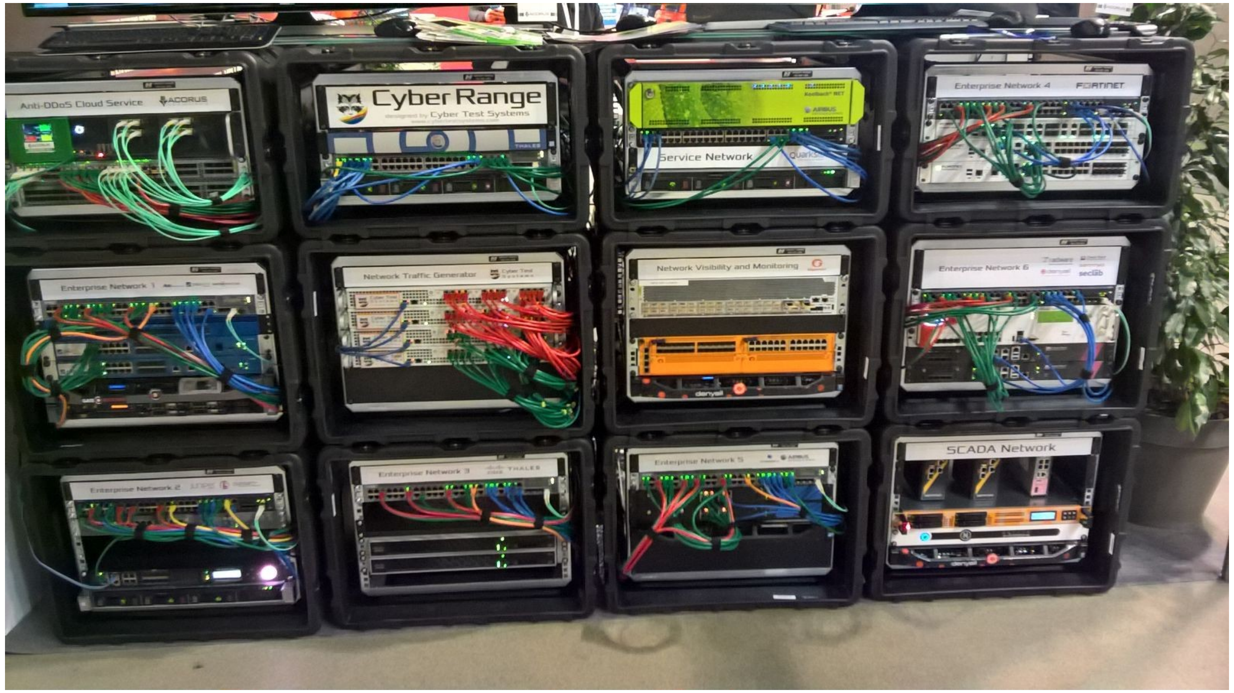
CDANS 2017 UK – Cyber Range - 16 Nations

Cyber Test
Systems



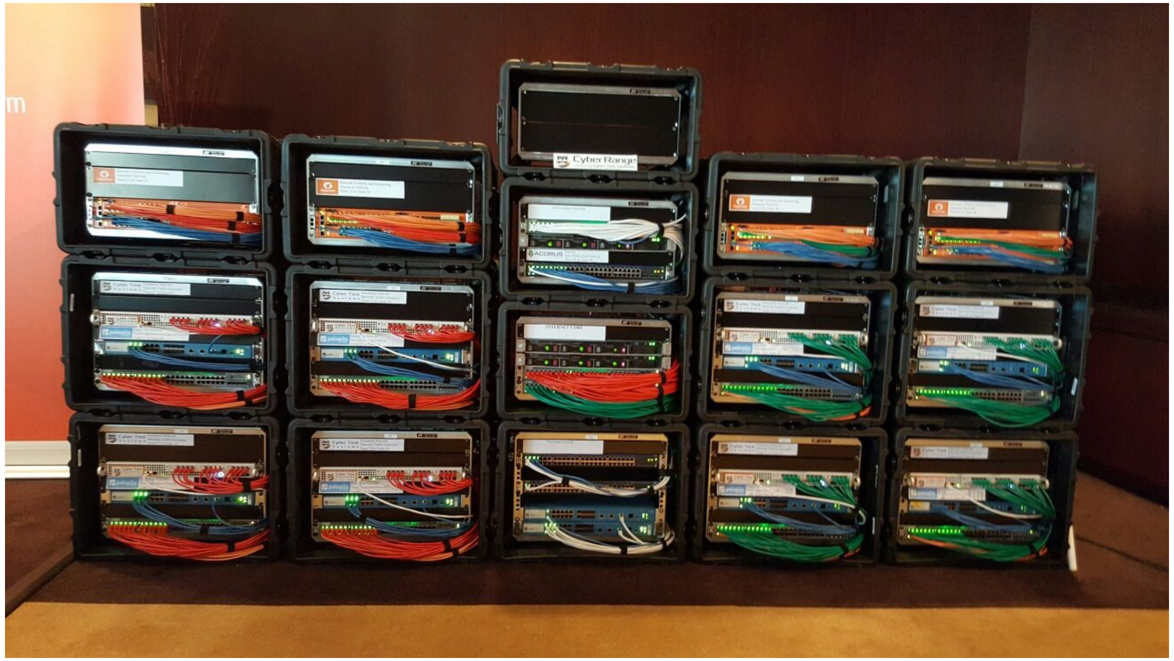
FIC 2017 France – Massive Cyber Range Multi-Vendors

Cyber Test Systems



Cyber Range with the largest diversity of solutions with the integration of 22 solutions including : Cyber Test Systems, Fortinet, Cisco, Gigamon, Juniper, Check Point, Palo Alto Networks, SecLab, Sentryo, GateWatcher, Diateam, CapStar Forensics, Acorus Networks, A10 Networks, F5 Networks, HP, DenyAll, StormShield, Airbus Defense and Space, Thales, QuarksLab and Radware

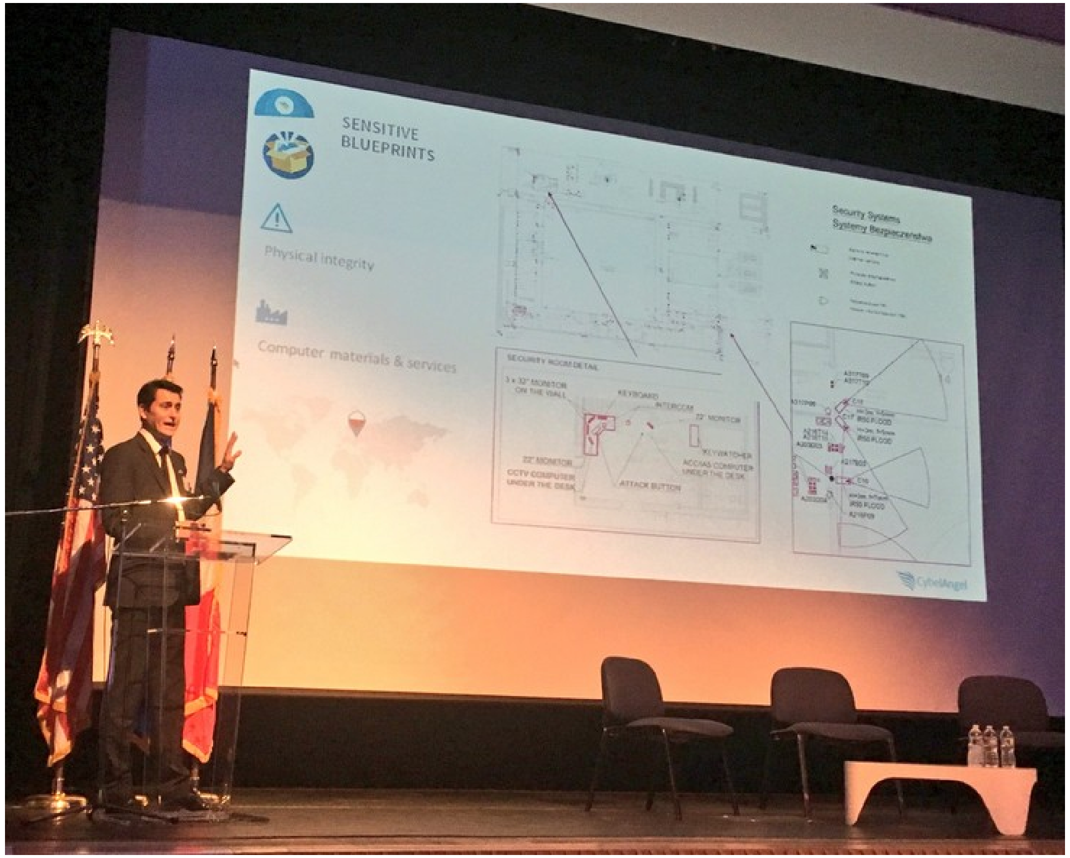
2017 Korea – Cyber Range - 48x Teams

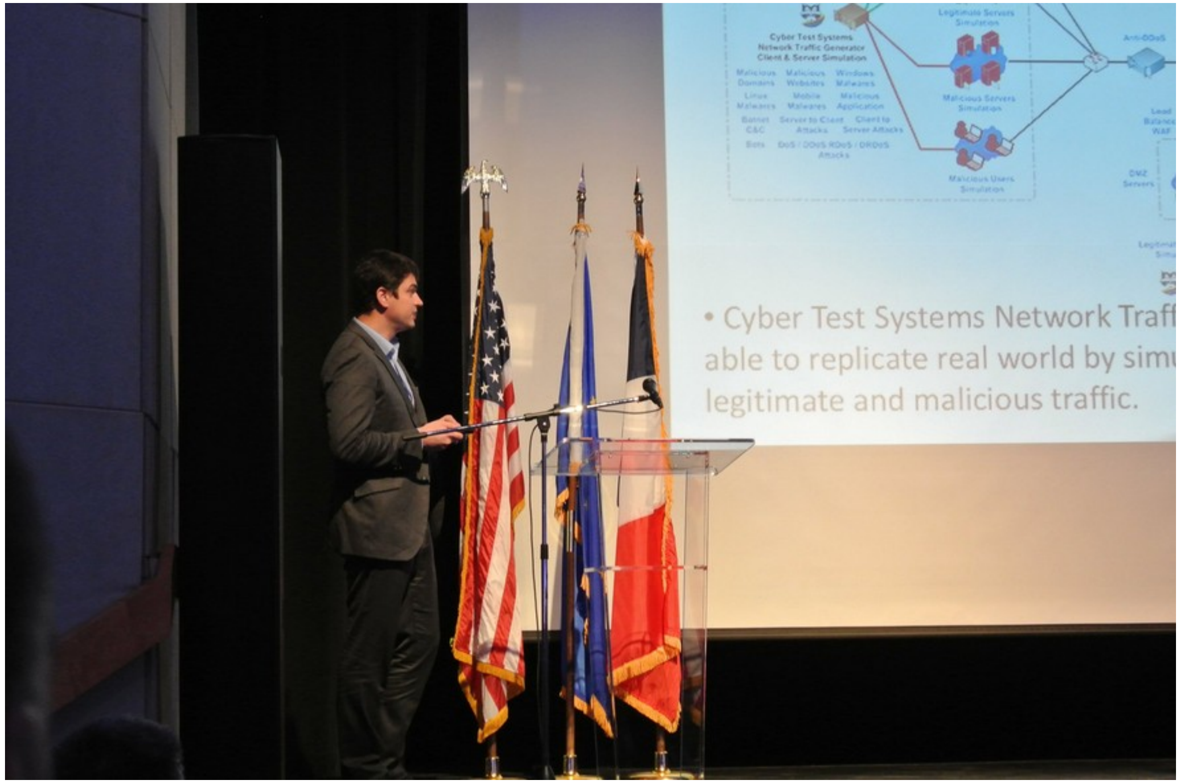


SoC Cyber Range with the largest teams 48x teams 72 participants.

DEFNET 2017 France – Cyber Range
Largest French Cyber Military Exercise

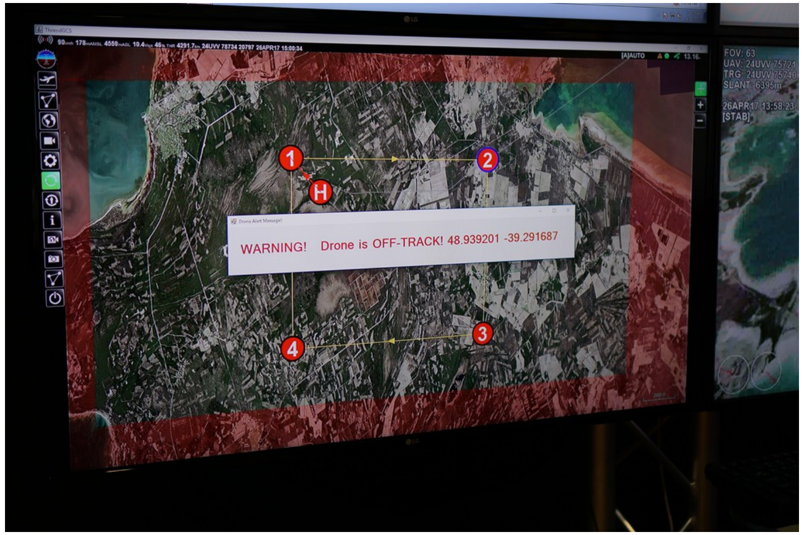
GBEF 2017 US – Cyber Range Civilian and Military Government Business Executive Forum




Cyber Test Systems
Network Traffic Generator
Client & Server Simulation
Legitimate Servers Simulation
Malicious Servers Simulation
Malicious Users Simulation
Anti-DDoS
Load Balancer WAF
DMZ Servers
• Cyber Test Systems Network Traff
able to replicate real world by simu
legitimate and malicious traffic.

Cyber Test Systems

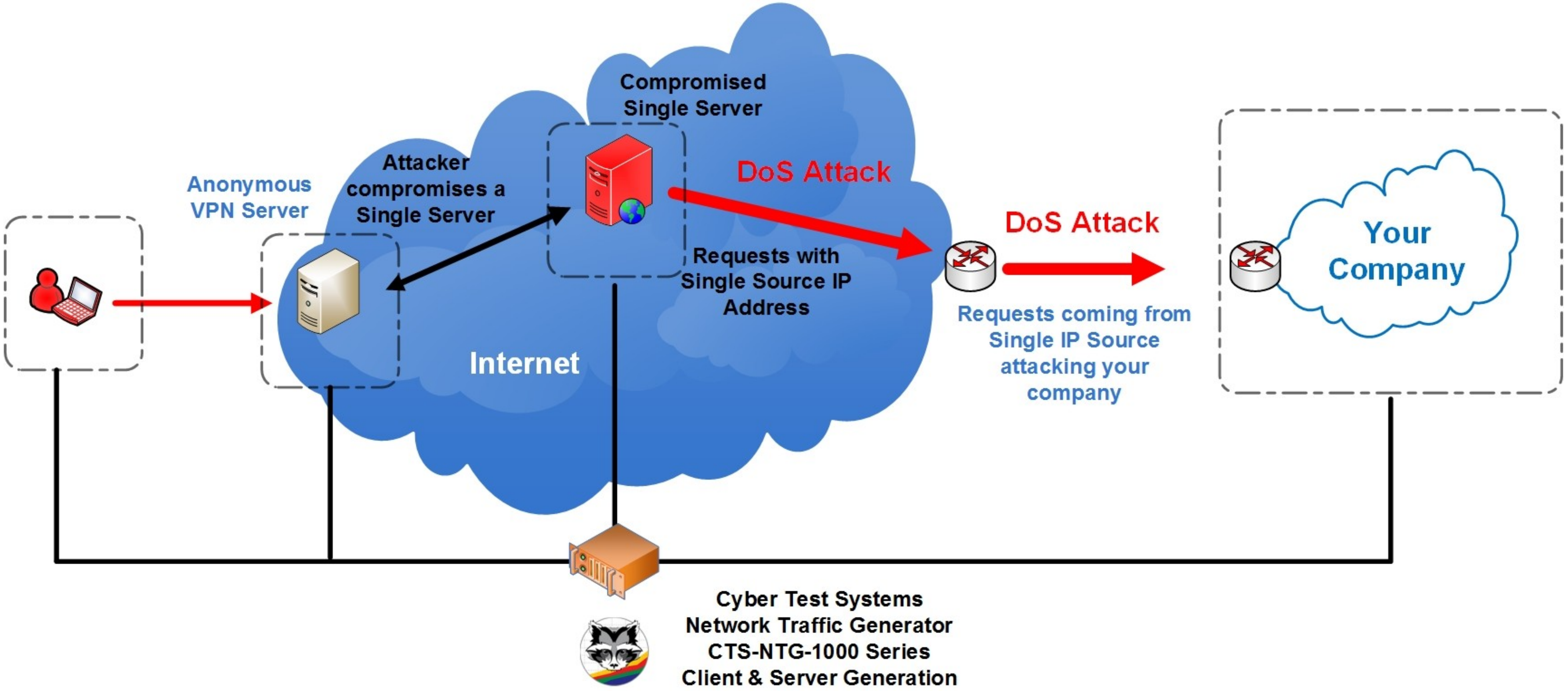
NATO CCDCOE 2017 Estonia - Locked Shield 2017
Largest NATO Cyber Exercise


WARNING! Drone is OFF-TRACK! 48.939201 -39.291687

Cyber Range - Cyber Attack Scenarios
using
Cyber Test Systems Network Traffic Generator CTS-NTG

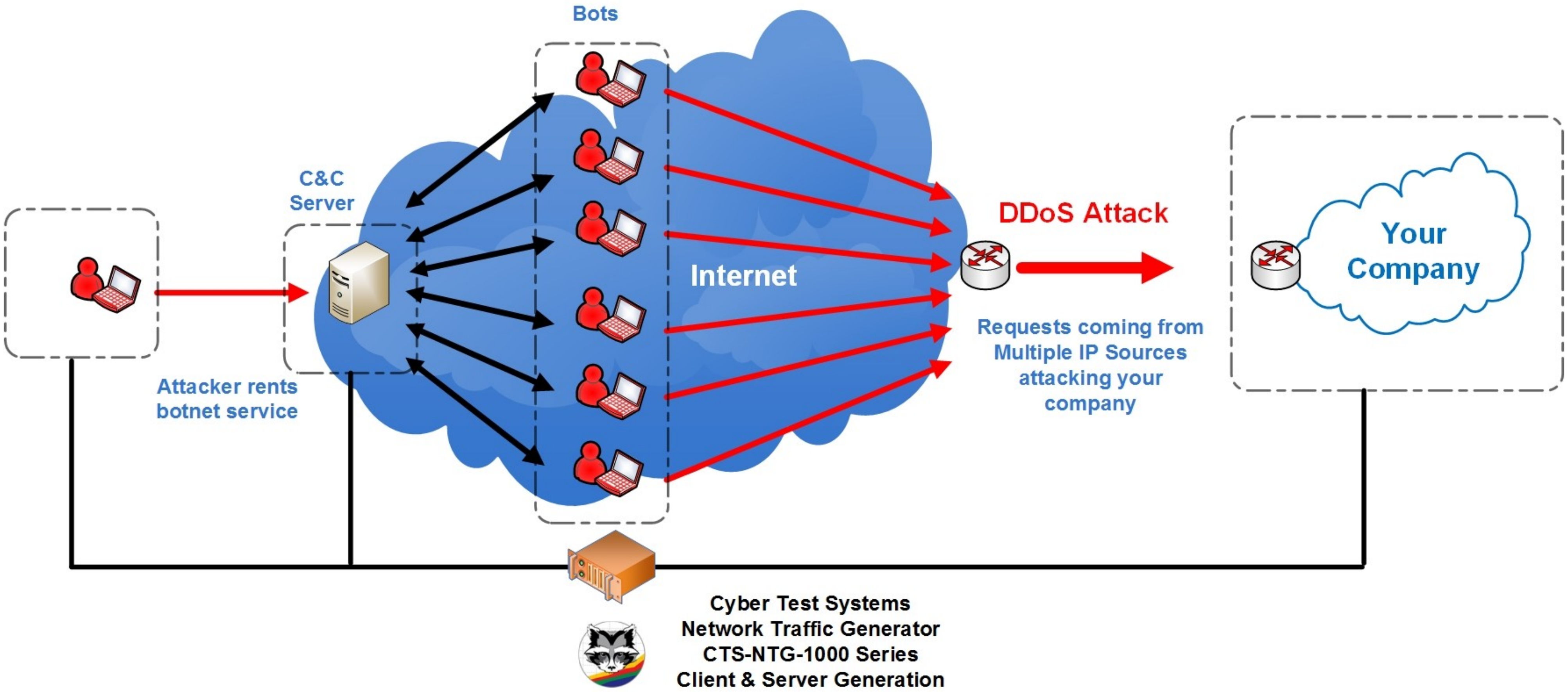
Denial of Service (DoS)

- A Denial-of-Service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinite interrupt or suspend services of a host connected to the Internet.



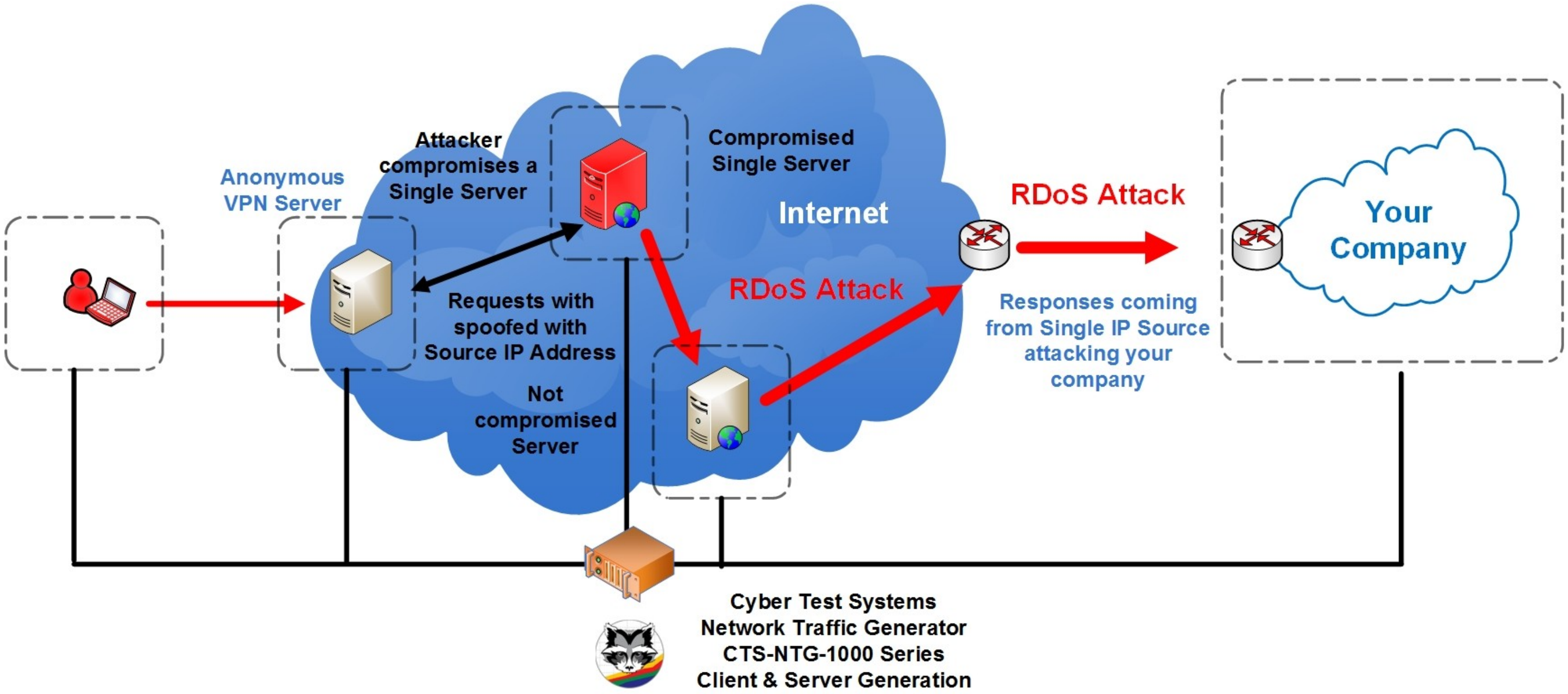
Distributed Denial of Service (DDoS)

- A Distributed Denial-of-Service (DDoS) is where the attack source is more than one, often thousands of, unique IP addresses. It is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.



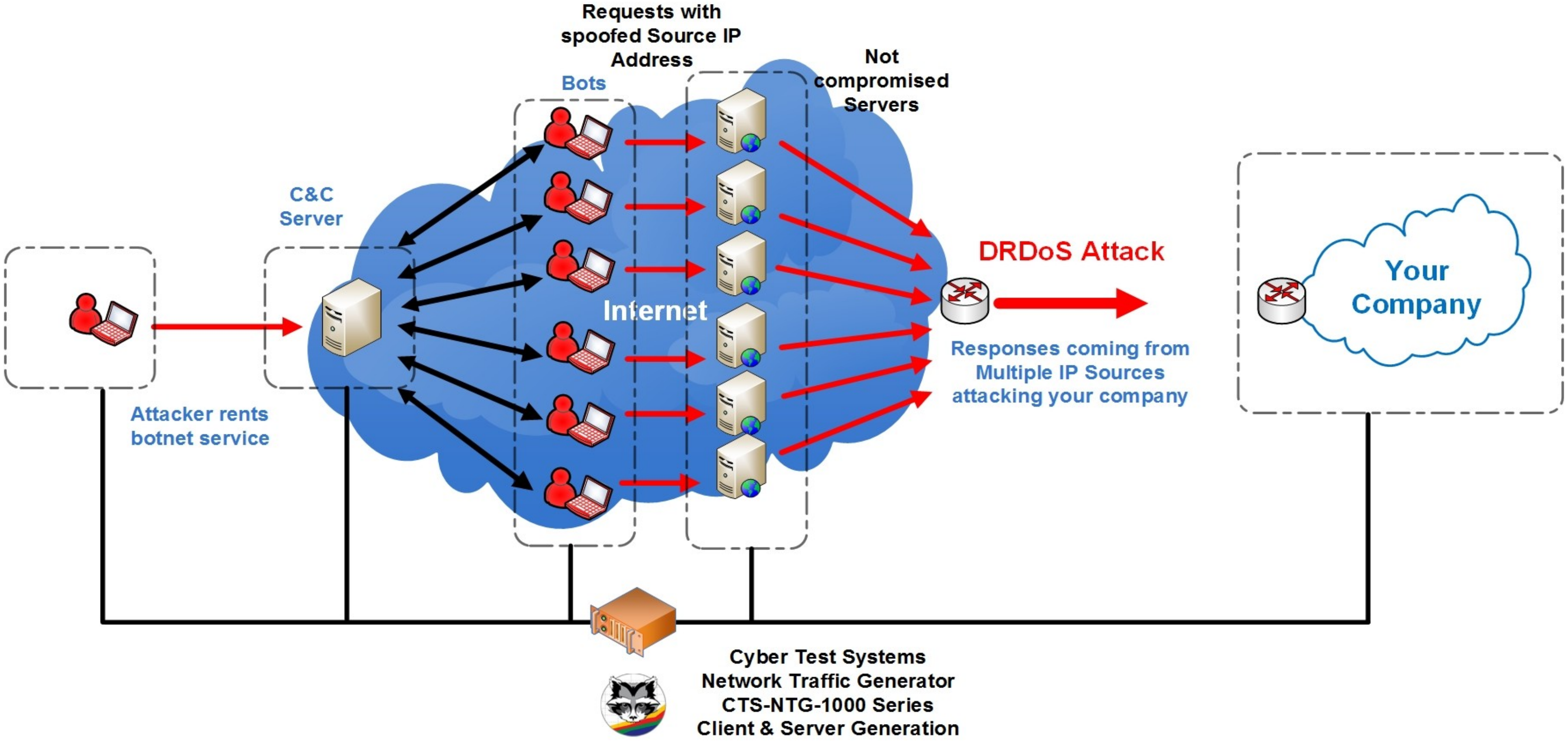
Reflective Denial of Service (RDoS)

- A Reflective Denial of Service (RDoS) is where it involves sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet Protocol address spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target.


Anonymous VPN Server
Attacker compromises a Single Server
Compromised Single Server
Internet
Requests with spoofed with Source IP Address
Not compromised Server
RDoS Attack
RDoS Attack
Your Company
Responses coming from Single IP Source attacking your company
Cyber Test Systems Network Traffic Generator CTS-NTG-1000 Series Client & Server Generation

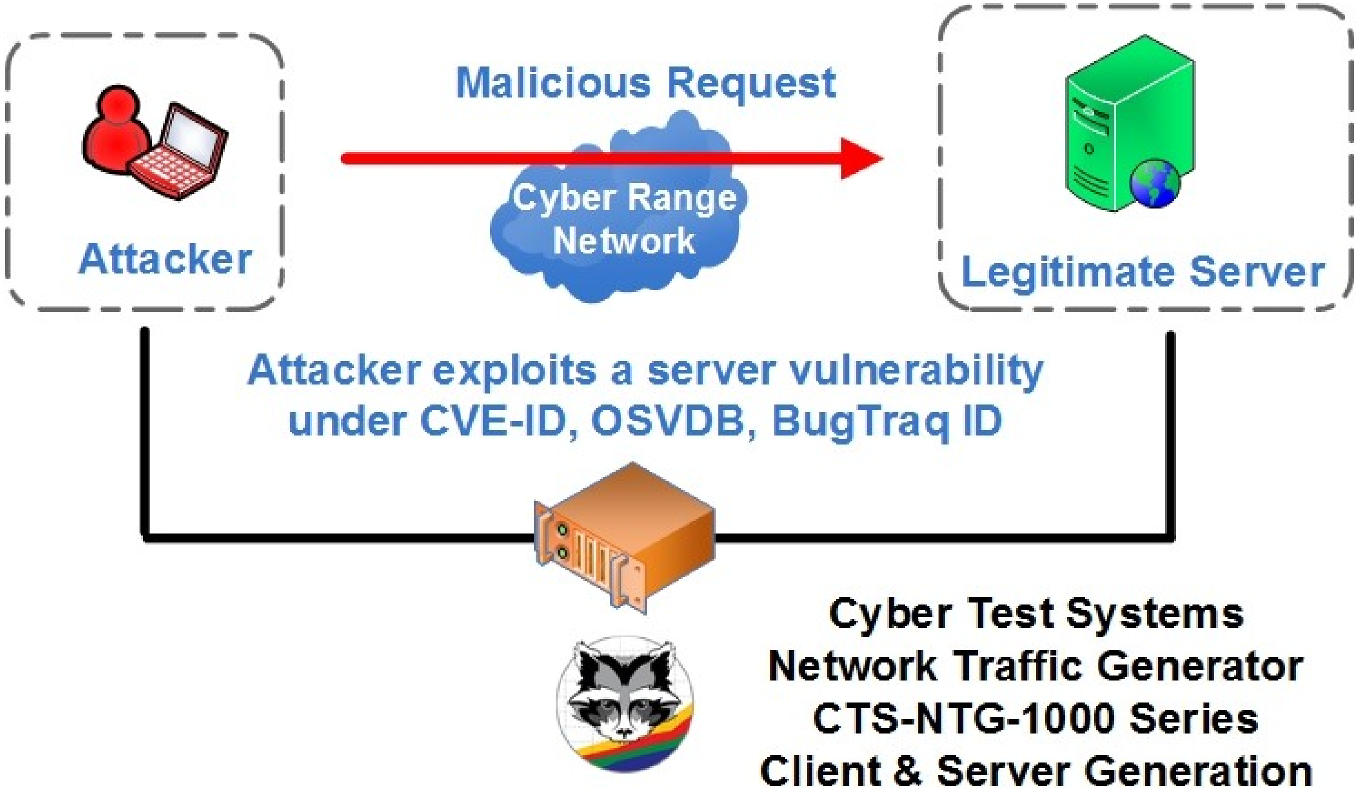
Distributed Reflective Denial of Service (DRDoS)

- A Distributed Reflective denial-of-service (DRDoS) usually involves multiple victim machines that unwittingly participate in a DDoS attack on the attacker’s target. Requests to the victim host machines are redirected, or reflected, from the victim hosts to the target. Usually they also elicit an amplified amount of attack traffic.


Requests with spoofed Source IP Address
Bots
Not compromised Servers
C&C Server
Internet
DRDoS Attack
Your Company
Responses coming from Multiple IP Sources attacking your company
Attacker rents botnet service
Cyber Test Systems Network Traffic Generator CTS-NTG-1000 Series Client & Server Generation

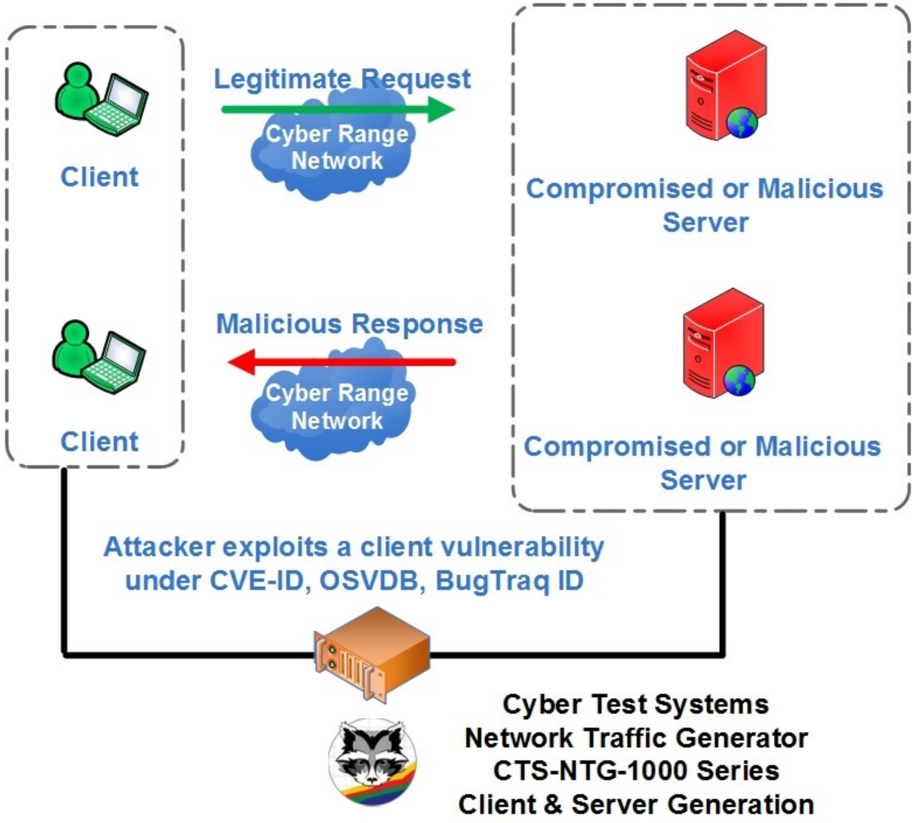
Server Side Vulnerabilities and Exploits

- A vulnerable service can be exploited by a person with malicious intent to gain access to information and/or environment. The vulnerability can potentially cause informational and operational loss if exploited. Attack is coming from client side to server side.


Malicious Request
Attacker
Cyber Range Network
Legitimate Server
Attacker exploits a server vulnerability under CVE-ID, OSVDB, BugTraq ID
Cyber Test Systems Network Traffic Generator CTS-NTG-1000 Series Client & Server Generation

Client Side Vulnerabilities and Exploits

- A vulnerable service can be exploited by person with malicious intent to gain access to information and/or environment. The vulnerability can potentially cause informational and operational loss if exploited. In this case, if the server is able to exploit vulnerability on the client side, the "infected" server can potentially exploit / uses the client to spread its payload.


Client
Legitimate Request
Cyber Range Network
Compromised or Malicious Server
Client
Malicious Response
Cyber Range Network
Compromised or Malicious Server
Attacker exploits a client vulnerability under CVE-ID, OSVDB, BugTraq ID
Cyber Test Systems Network Traffic Generator CTS-NTG-1000 Series Client & Server Generation

Web Exploit Kits

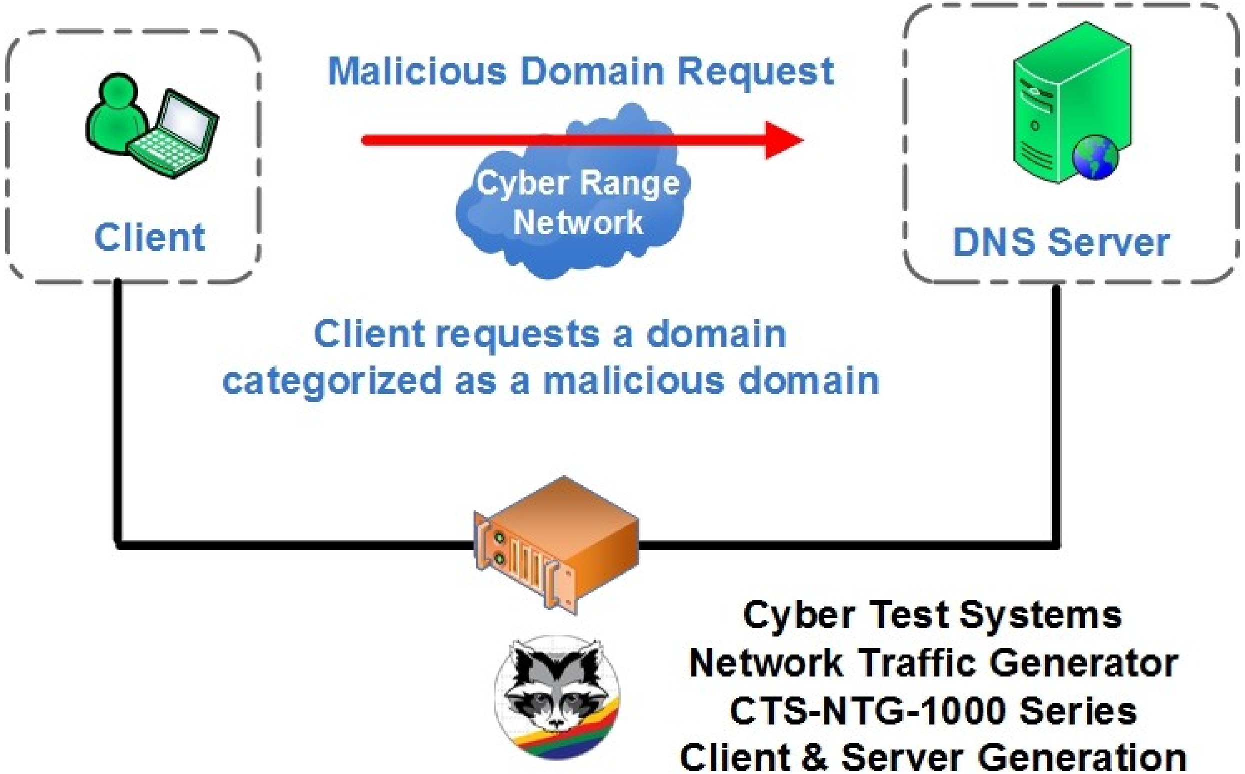
- Web Exploit Kit is a toolkit that automates the exploitation of client-side vulnerabilities, usually targeting browsers and programs that a website can invoke through the browser. exploit vulnerability on the client side, the “infected” server can potentially exploit / uses the client to spread its payload.

- The following Web Exploit Kit could be generated :

  - RIG EK
  - Angler EK
  - Nuclear EK
  - Neutrino EK
  - Magnitude EK
  - Sundown EK
  - Sweet Orange EK
  - KaiXin EK
  - Fiesta EK
  - Hunter EK
  - Styx EK
  - Goon EK
  - Whitehole EK
  - Cool EK
  - Blackhole EK
  - DotkaChef EK
  - Sibhost EK
  - FlashPack EK

Malicious Domains

- Malicious Domain is a Domain that is known to contain malicious content. A Domain categorized to provide malicious content often link to Malware that disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

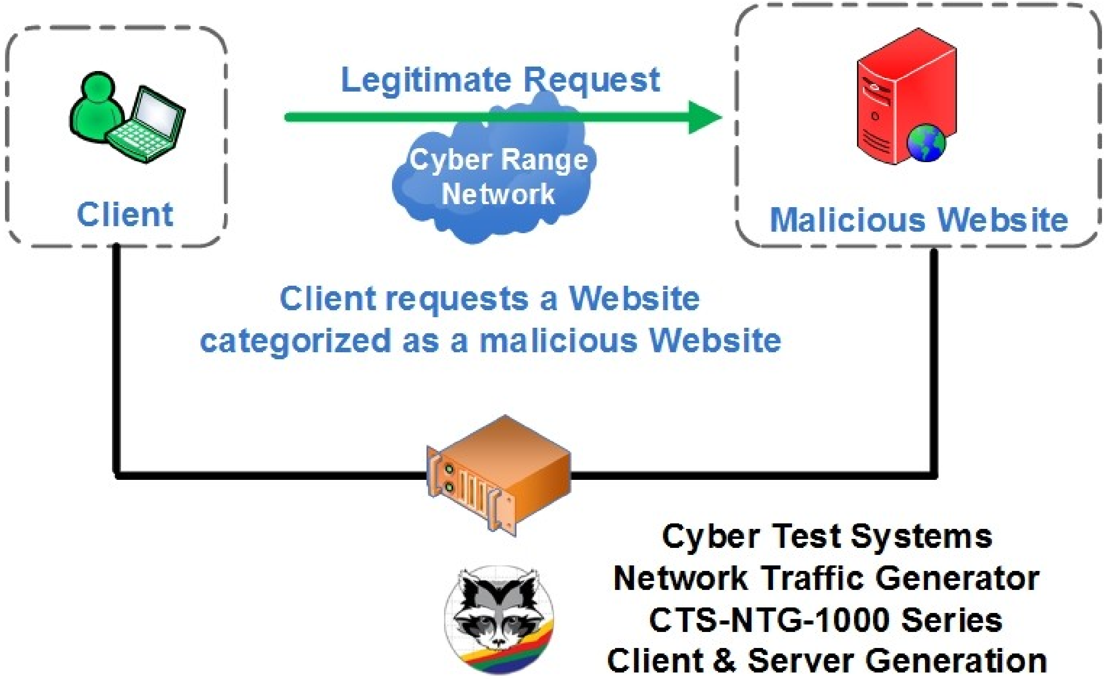


Client requests a domain categorized as a malicious domain

Cyber Test Systems
Network Traffic Generator
CTS-NTG-1000 Series
Client & Server Generation

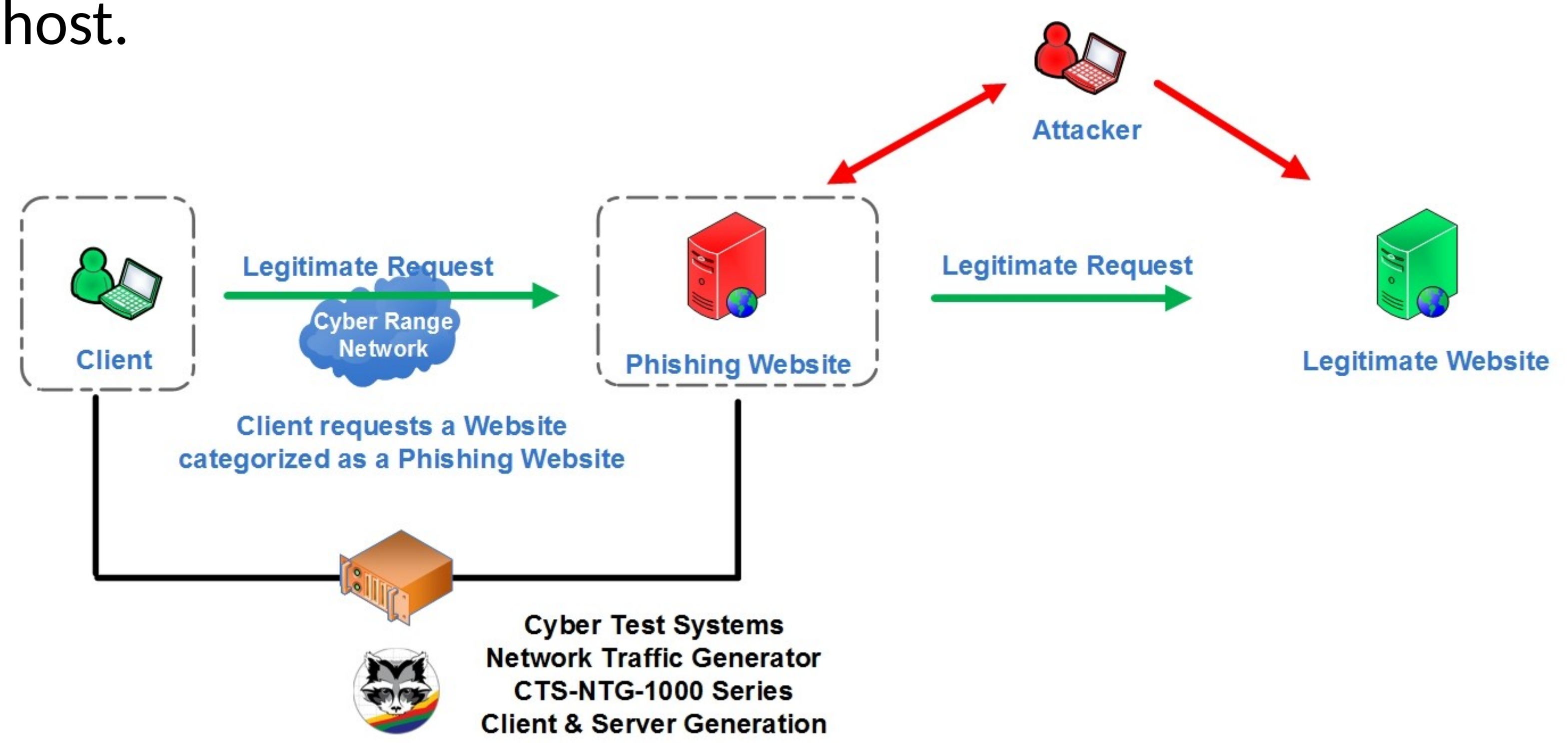
Malicious Websites

- Malicious Website is a Website that contains malicious content. A Website categorized to provide malicious content often link to Malware that disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.


Legitimate Request
Client
Cyber Range Network
Malicious Website
Client requests a Website categorized as a malicious Website
Cyber Test Systems
Network Traffic Generator
CTS-NTG-1000 Series
Client & Server Generation

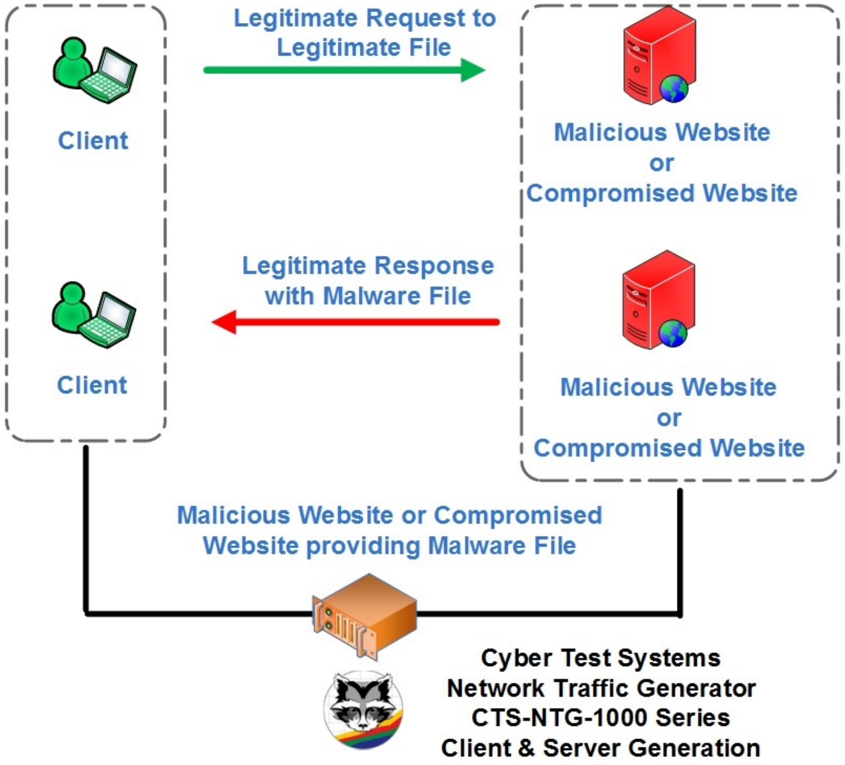
Malicious Phishing Websites

- Phishing Website is a Website attempting to acquire sensitive information such as usernames, passwords, credit card details, … for malicious reasons. Phishing occurs when the attacker pretends to be a trustworthy entity, either via email or web page. Victims are directed to fake web pages, which are dressed to look legitimate, via spoof emails, instant messenger/social media or other avenues. Often tactics such as email spoofing are used to make emails appear to be from legitimate senders, or long complex sub domains hide the real website host.



Malwares for Windows, OS X, Linux, Android, iOS

- Malware is malicious software specially design to gain access or damage a computer without the knowledge of the owner for malicious reasons. Malware is a software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user.

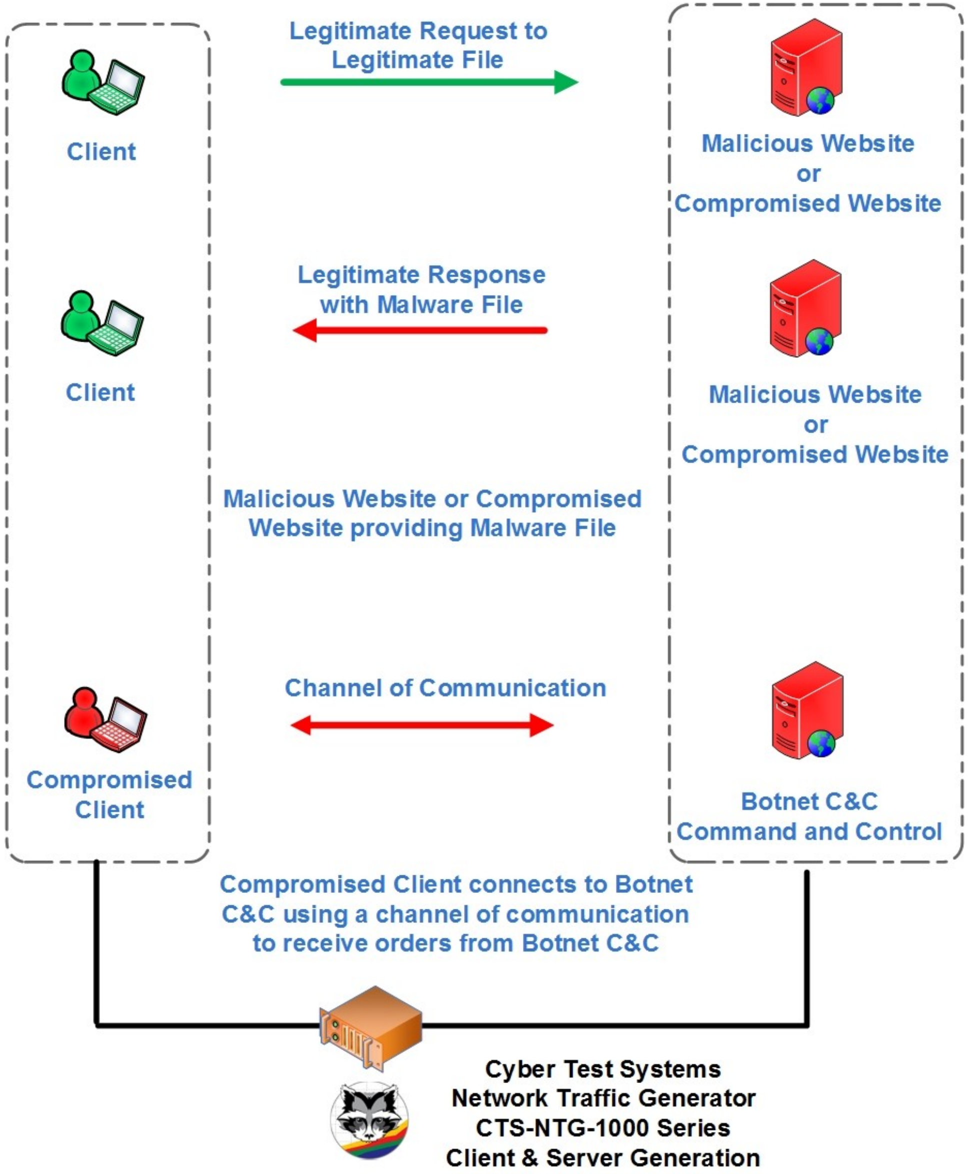

Legitimate Request to Legitimate File
Client
Malicious Website or Compromised Website
Legitimate Response with Malware File
Client
Malicious Website or Compromised Website
Malicious Website or Compromised Website providing Malware File
Cyber Test Systems Network Traffic Generator CTS-NTG-1000 Series Client & Server Generation

Botnets Communications between C&C and Bots

Cyber Test Systems

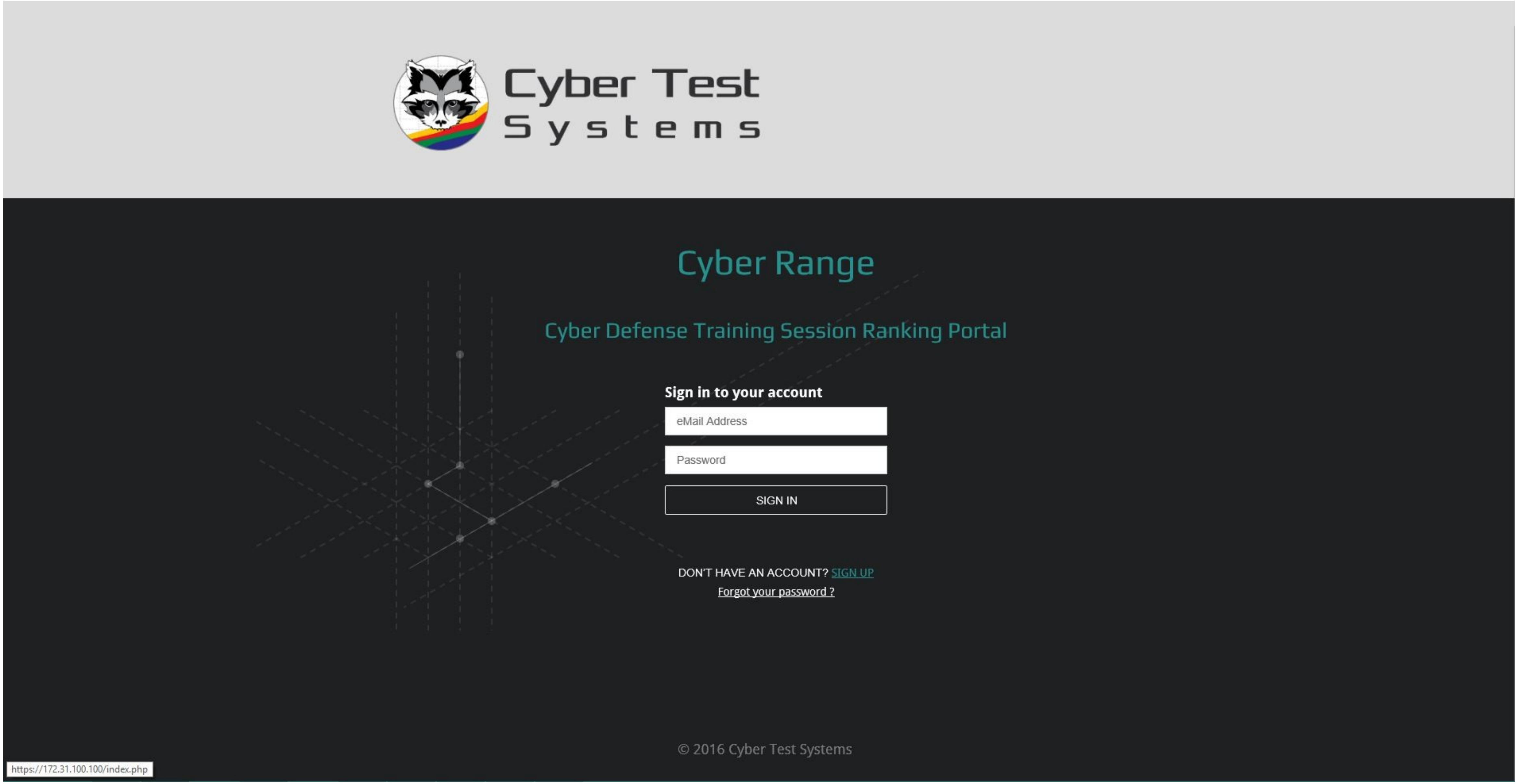
- Botnet communication is hidden channel of communication between compromised client acting as bot connecting to his C&C Command and Control to receive orders

- A clear distinction between a bot agent and a common piece of malware lies within a bot's ability to communicate with a command-and-control (C&C) infrastructure. C&C allows a bot agent to receive new instructions and malicious capabilities, as dictated by a remote criminal entity. This compromised host then can be used as an unwilling participant in Internet crime as soon as it is linked into a botnet via that same C&C.


Legitimate Request to Legitimate File
Client
Malicious Website or Compromised Website
Legitimate Response with Malware File
Client
Malicious Website or Compromised Website
Malicious Website or Compromised Website providing Malware File
Channel of Communication
Compromised Client
Botnet C&C Command and Control
Compromised Client connects to Botnet C&C using a channel of communication to receive orders from Botnet C&C
Cyber Test Systems Network Traffic Generator CTS-NTG-1000 Series Client & Server Generation

Cyber Range – Scoring
Using
Cyber Test Systems
Cyber Defense Training Session Ranking Portal

Cyber Range Cyber Defense Training Session Ranking Portal



Cyber Range

Cyber Defense Training Session Ranking Portal

Sign in to your account

eMail Address

Password

SIGN IN

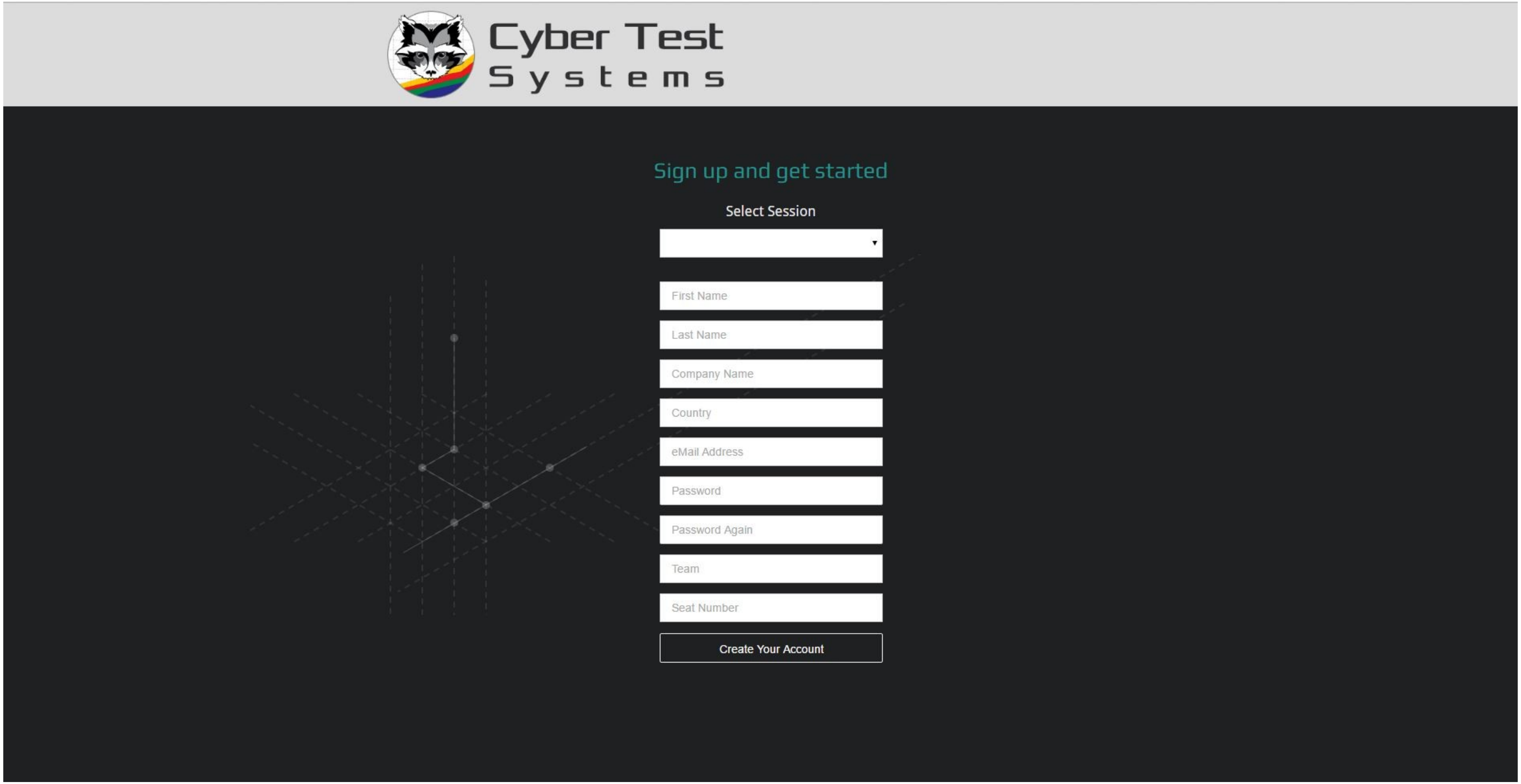
DON'T HAVE AN ACCOUNT? SIGN UP

Forgot your password ?

© 2016 Cyber Test Systems

https://172.31.100.100/index.php

Cyber Range Cyber Defense Training Session Ranking Portal

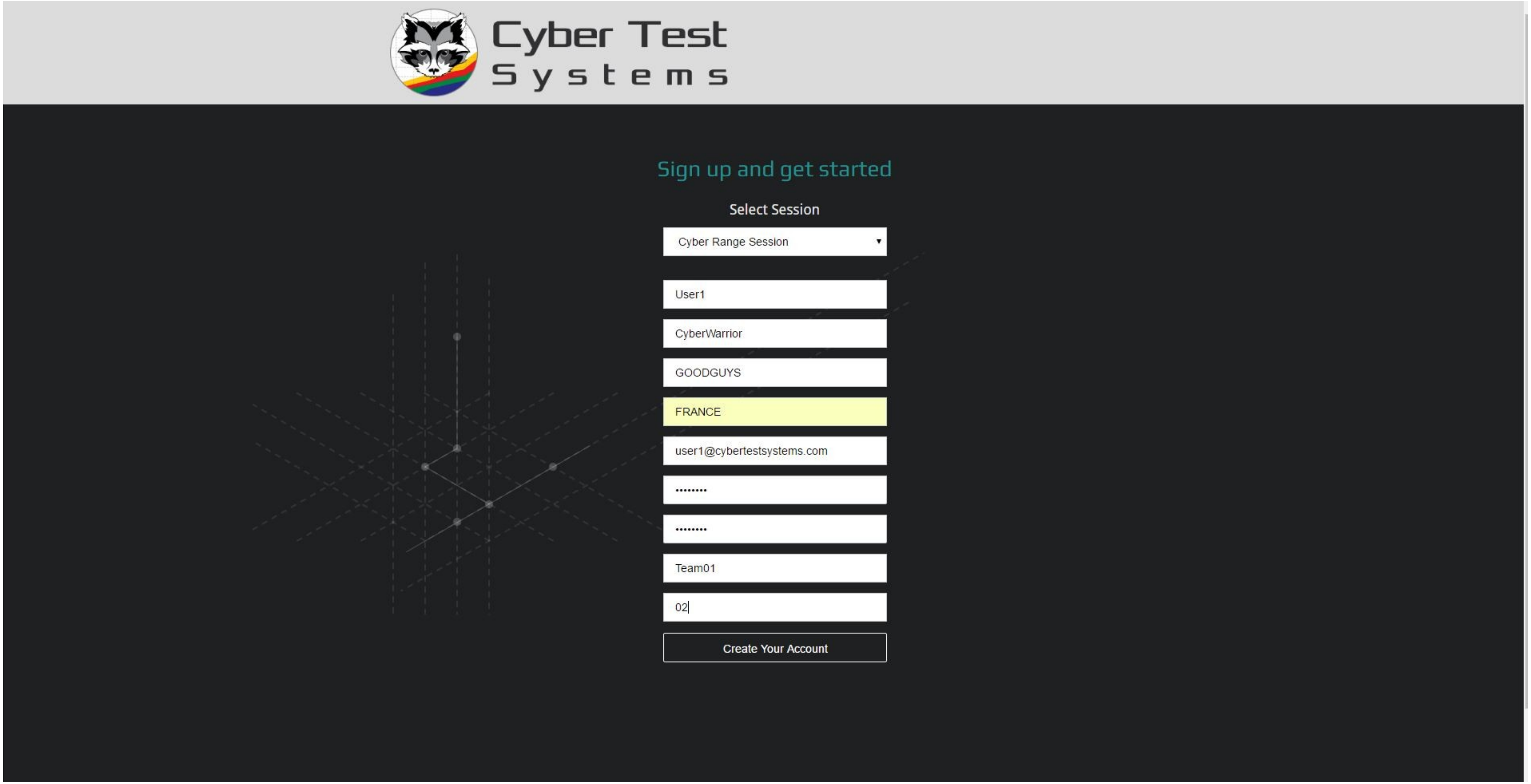


Cyber Test Systems

Sign up and get started

Select Session

Cyber Range Cyber Defense Training Session Ranking Portal



Sign up and get started

Select Session

Cyber Range Session ▾

User1

CyberWarrior

GOODGUYS

FRANCE

user1@cybertestsystems.com

••••••••

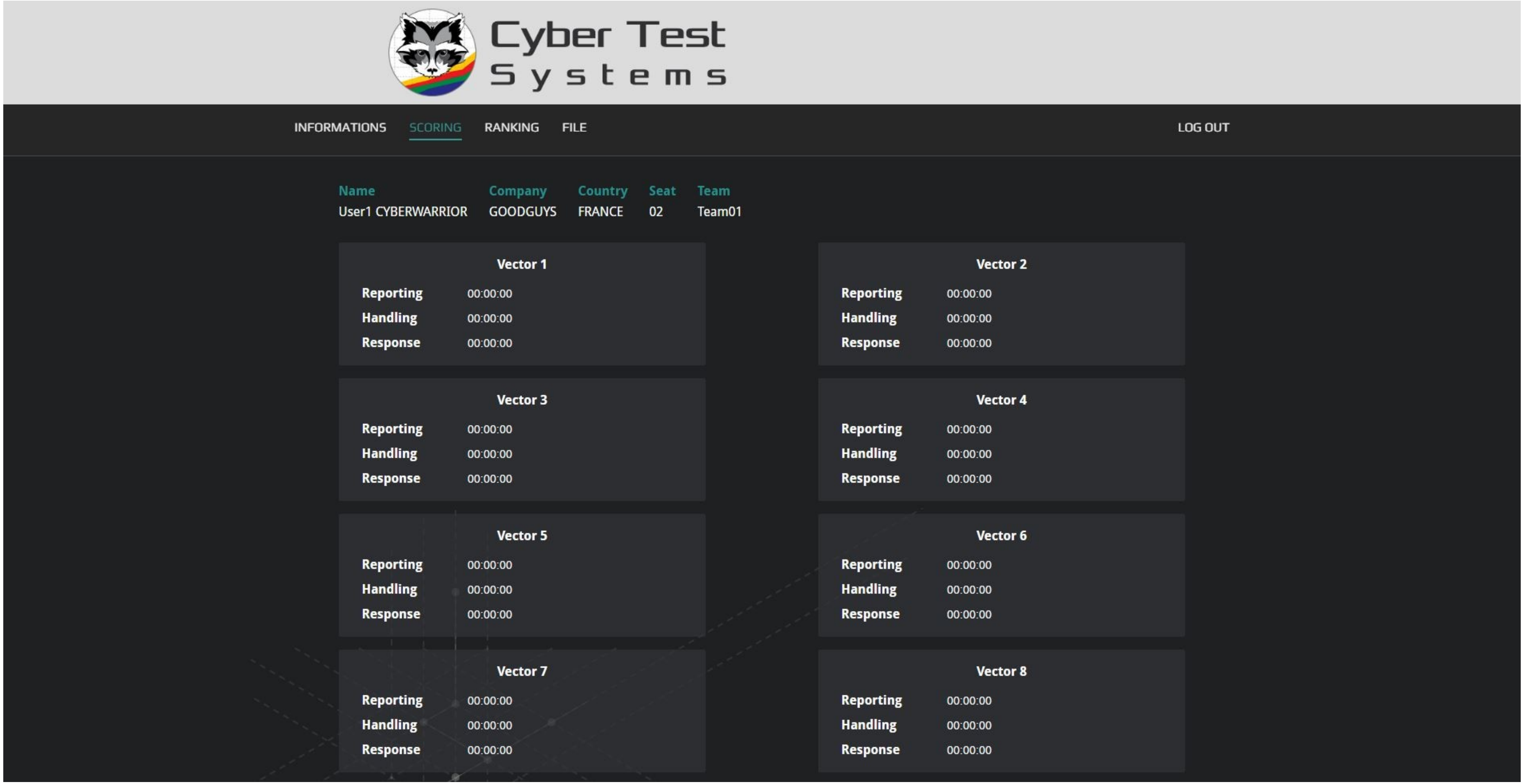
••••••••

Team01

02

Cyber Range Cyber Defense Training Session Ranking Portal

Cyber Test Systems



Name	Company	Country	Seat	Team
User1 CYBERWARRIOR	GOODGUYS	FRANCE	02	Team01

Vector 1	
Reporting	00:00:00
Handling	00:00:00
Response	00:00:00

Vector 2	
Reporting	00:00:00
Handling	00:00:00
Response	00:00:00

Vector 3	
Reporting	00:00:00
Handling	00:00:00
Response	00:00:00

Vector 4	
Reporting	00:00:00
Handling	00:00:00
Response	00:00:00

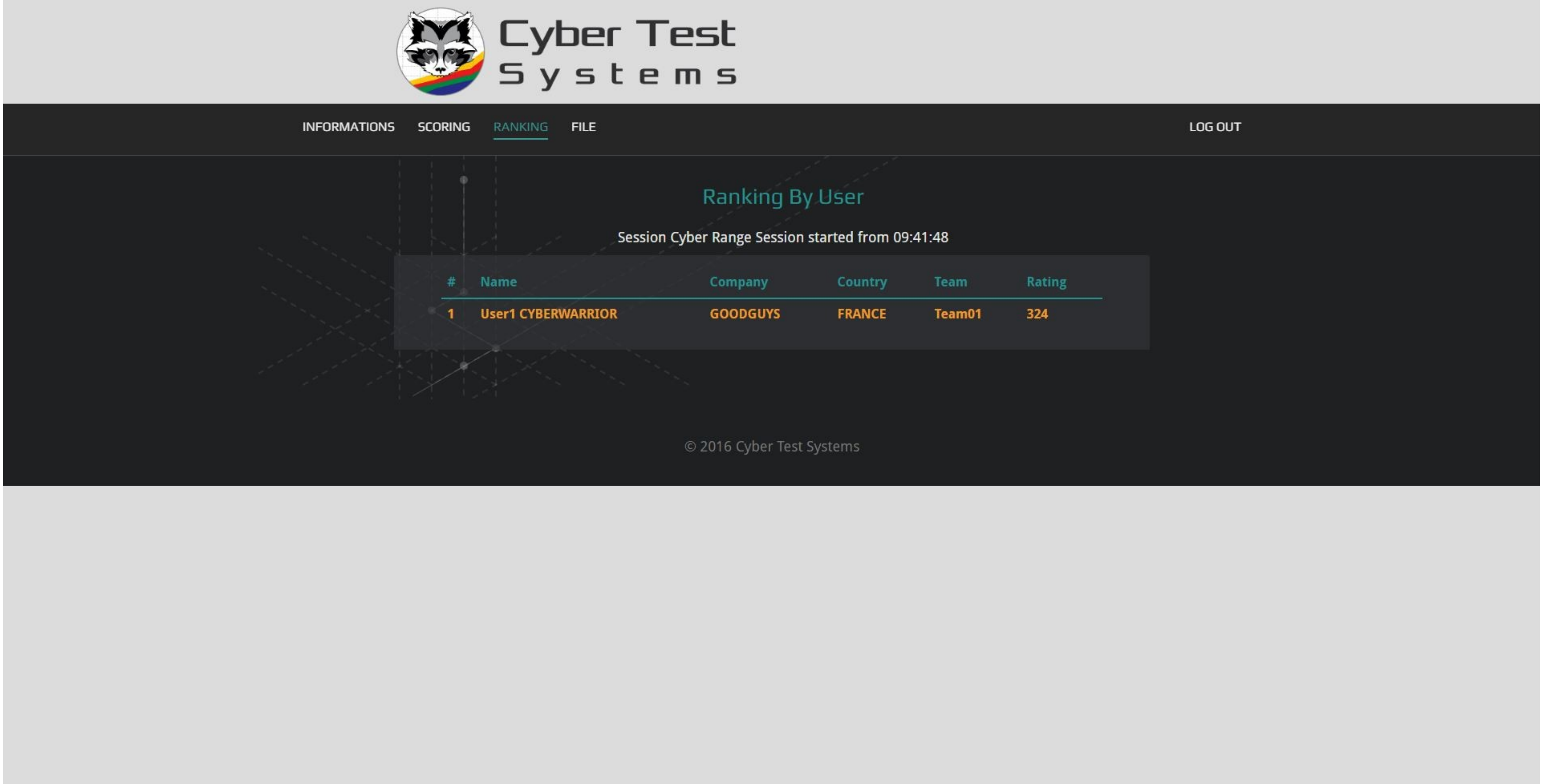
Vector 5	
Reporting	00:00:00
Handling	00:00:00
Response	00:00:00

Vector 6	
Reporting	00:00:00
Handling	00:00:00
Response	00:00:00

Vector 7	
Reporting	00:00:00
Handling	00:00:00
Response	00:00:00

Vector 8	
Reporting	00:00:00
Handling	00:00:00
Response	00:00:00

Cyber Range Cyber Defense Training Session Ranking Portal



Ranking By User

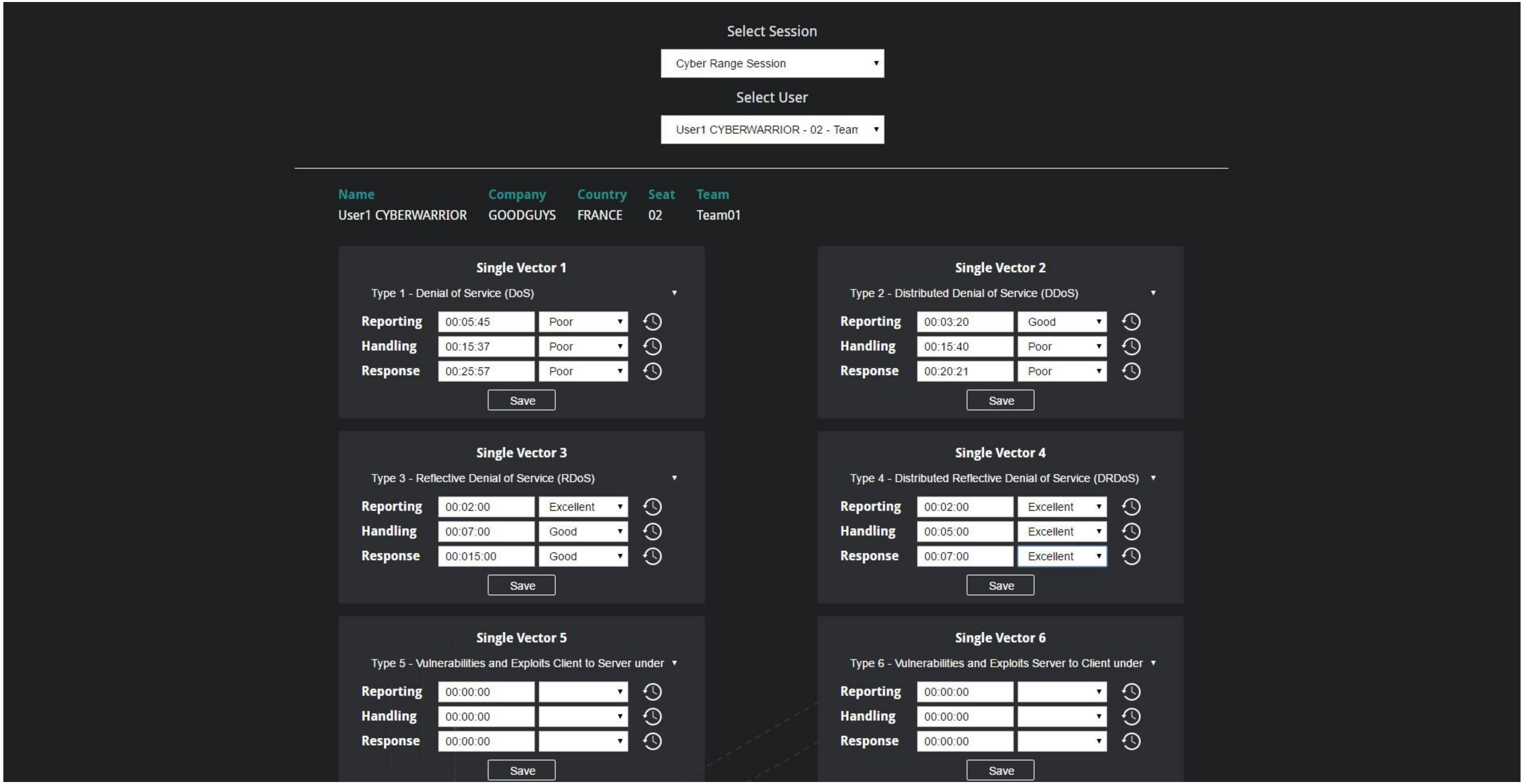
Session Cyber Range Session started from 09:41:48

#	Name	Company	Country	Team	Rating
1	User1 CYBERWARRIOR	GOODGUYS	FRANCE	Team01	324

© 2016 Cyber Test Systems

Cyber Range Cyber Defense Training Session Ranking Portal

Cyber Test Systems



Select Session

Cyber Range Session ▾

Select User

User1 CYBERWARRIOR - 02 - Tean ▾

Name	Company	Country	Seat	Team
User1 CYBERWARRIOR	GOODGUYS	FRANCE	02	Team01

Single Vector 1

Type 1 - Denial of Service (DoS) ▾

Reporting	00:05:45	Poor
Handling	00:15:37	Poor
Response	00:25:57	Poor

Single Vector 2

Type 2 - Distributed Denial of Service (DDoS) ▾

Reporting	00:03:20	Good
Handling	00:15:40	Poor
Response	00:20:21	Poor

Single Vector 3

Type 3 - Reflective Denial of Service (RDoS) ▾

Reporting	00:02:00	Excellent
Handling	00:07:00	Good
Response	00:015:00	Good

Single Vector 4

Type 4 - Distributed Reflective Denial of Service (DRDoS) ▾

Reporting	00:02:00	Excellent
Handling	00:05:00	Excellent
Response	00:07:00	Excellent

Single Vector 5

Type 5 - Vulnerabilities and Exploits Client to Server under ▾

Reporting	00:00:00	
Handling	00:00:00	
Response	00:00:00	

Single Vector 6

Type 6 - Vulnerabilities and Exploits Server to Client under ▾

Reporting	00:00:00	
Handling	00:00:00	
Response	00:00:00	

Cyber Test
Systems

Thank You

Gregory FRESNAIS
Co-founder
+ 33 6 72 51 09 22
gregory.fresnais@cybertestsystems.com