C Y B E R  F O R T R E S S  E N T E R P R I S E
Agenda

I. 13:30 – 13:45  Game History
II. 13:45 – 14:10 Introduction (concept, navigation, rules)
III. 14:10 – 14:50 1st Game Session
IV. 14:50 – 15:00 Summary of the 1st Game Session
V. 15:00 – 15:30 Coffee Break
VI. 15:30 – 15:45 Introduction (2nd Game Session)
VII. 15:45 – 16:35 2nd Game Session
VIII. 16:35 – 16:45 Summary of the 2nd Game Session
IX. 16:45 – 16:50 The Cyber Fortress Enterprise
X. 16:50 – 17:00 Results & Rewards
04.2019
Project kick-off

05.2019
Premiere

03.2020
Online version

09.2020
Cyber Fortress League 1

01.2022
Cyber Fortress League 2

12.2022
Cyber Fortress League 3

20.23
Cyber Fortress World Cup
Premiere 2019 – Polish Naval Academy, Summer Cybersecurity School
History

Hybrid version 2021
History

https://youtu.be/aPEZUnKsEi
Cyber Fortress

Cyber Fortress is a strategic simulation game which main idea and the task is to build the best cybersecurity system to prevent players’ organizations against the most likely threats and to effectively react during the incident mitigation phase.

Safeguards represent cybersecurity measures that come from four main areas:

- **organizational** (CERT, SOC team, ...)
- **technical** (SIEM, anti-DDoS, ...)
- **procedural** (incident response procedure, ...)
- **data sources**
Cyber Fortress

Cyber Fortress is based on:

• VERIS Framework (http://veriscommunity.net/)
• MITRE ATT&CK Framework (https://attack.mitre.org/)
• Bow-Tie Risk Assessment model
• Defense-in-Depth model
Cyber Fortress - VERIS Framework

**VERIS Framework** - a dictionary for recording events and sharing event information, a set of metrics designed to provide a common language for describing security events in a structured and repeatable way.

Kick-off: **2010 r.**

Project sites:
- https://github.com/vz-risk/veris
- http://veriscommunity.net/
Cyber Fortress – MITRE ATT&CK Framework

MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) Framework (https://attack.mitre.org/) - a structured, globally accessible knowledge base of tactics, techniques and procedures that are used by attackers, continuously updated and developed by a community of cyber security professionals.

The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
Cyber Fortress – MITRE ATT&CK Framework

Tactics, Techniques, Procedures (TTPs) define the specific behaviors and tools used by cybercriminals or cybercrime groups to achieve their goals at each stage of an attack. Knowing the modus operandi of attackers who are potentially motivated to attack us, we can better prepare to defend ourselves and detect the attack.

tactics = goal

technique = way of achieving the goal

procedure = way to implement the technique
Cyber Fortress - Defense-in-Depth

**Defense-in-Depth** - multi-level defense strategy - a way of designing the security of information systems, involving the introduction of multiple independent levels of security.
Practical information

- PC or phone, Chrome/Firefox/Safari browser (private mode)
- Internet access
- **If during the game, something goes wrong - RELOAD webpage**
- You will play 2 Games (3 Scenarios)
- Logging into the game is done with a PIN code
- **ONLY the team Captain logs into the game**
- The game consists of Events (Injects)
- Events could be Informational, Positive and Negative in nature
- In the Briefing section you will find the most important information about the Scenario
- Safeguards are divided into 8 categories (Organization, Physical infrastructure, Entire network, Network edge, Internal network, Host, Applications and Data)
- **There is a ninth category of Safeguard - Data Sources - which must be unlocked by purchasing the correct safeguard from the other eight categories**
- Some safeguards will not work unless they had been bought before the first Inject occurred
- Some safeguards will not work unless they had been bought before the first Inject occurred
- You can find the list of Safeguards with description at: https://cyberfortress.comcert.pl/safeguards
Interface of the Game

Cyber Fortress

Join the game

Lobby

Games list

Attack

Cyber Fortress

Enter PIN and join the game

Next

Next

Game Master will start the game 😊
Interface of the Game

To purchase a Safeguard, select it (it is possible to select many) and then click Buy button (the Reset button resets the selection).
The Game requires a PIN number to log you into the Lobby

Cyber Fortress - Introduction

Link to the Cyber Fortress Game:
https://cyberfortress.comcert.pl/
1ST GAME SESSION:
The Energy System Attack
The Energy System Attack Scenario

On 23 December 2015, hackers using the BlackEnergy 3 malware remotely compromised information systems of three energy distribution companies in Ukraine and temporarily disrupted the electricity supply to consumers. Most affected were consumers of Prykarpattyatoblenenergo (Ukrainian: Прикарпаттяобленерго; servicing Ivano-Frankivsk Oblast): 30 substations (7 110kv substations and 23 35kv substations) were switched off, and about 230,000 people were without electricity for a period from 1 to 6 hours.

At the same time, consumers of two other energy distribution companies, Chernivtsioblenergo (Ukrainian: Чернівціобленерго; servicing Chernivtsi Oblast) and Kyivoblenergo (Ukrainian: Київобленерго; servicing Kyiv Oblast) were also affected by a cyberattack, but at a smaller scale. According to representatives of one of the companies, attacks were conducted from computers with IP addresses allocated to the Russian Federation.

The Scenario has been based upon Events described above.
1. Reconnaissance – 2014 or earlier
2. Resource Development – Develop Capabilities: Malware (BE3) – 2014 or earlier

**CORPORATE NETWORK**
3. Initial access - Phishing: Spearphishing Attachment – May 2014 - June 2015
8. Discovery – Account discovery, Remote system discovery - June 2015- December 2015
   Lateral Movement – Remote services - June 2015- December 2015

**ICS NETWORK**
9. Initial Access – External remote services
   Lateral movement – Valid accounts, External remote services

Source: When the lights when out – ukrainian attack report
CORPORATE NETWORK
12. Execution – Scheduled Task - December 2015
ICS NETWORK
CORPORATE NETWORK
15. Impact – Network Denial of Service: Direct Network Flood - 23 December 2015
Lateral Movement – Remote services - June 2015- December 2015
ICS NETWORK
17. Impact – Data destruction

Source: When the lights when out – ukrainian attack report
The Energy System Attack Scenario

Link to the Cyber Fortress Game:
https://cyberfortress.comcert.pl
(the Team Captain ONLY)

list of Safeguards with description:
https://cyberfortress.comcert.pl/safeguards

The Game Session will last for: 40 min
Budget: $ 2 500 000
1ST GAME SESSION:
The Energy System Attack
EFFICIENT SAFEGUARDS
The Energy System Attack Scenario 1

1. Threat actors initiate phishing campaign against electricity distributors.
2. Threat actors successfully install BlackEnergy after employees open the email attachments.
4. Deliver Malware Plugins to enable credential harvesting and internal network reconnaissance.
5. BE3 malware plugins conduct credential harvesting and network discovery functions.
The Energy System Attack Scenario 2

Threat actors conduct internal reconnaissance on corporate network to discover potential targets and expand access.

Threat actors use stolen credentials to gain access and conduct reconnaissance on deployed systems.

Attackers deliver KillDisk malware to network share and set policy on DC to retrieve malware and execute upon system reboot.

Threat actors schedule unauthorized outage of UPS for telephone communication server and data center servers.
The Energy System Attack Scenario 2

Threat actors use native remote access services and valid credentials to open breakers and disrupt power distribution to over 225,000 customers.

Threat actors deliver malicious firmware updates to communications devices that cause converters to malfunction and break connections.

Threat actors initiate DoS attack on telephone call center at one of the targeted distributors.

Previously scheduled UPS outage cuts power to targeted telephone communications server and data center servers.

Scheduled execution of KillDisk malware erases the master boot records and deletes system log data.

No mitigations
2ND GAME SESSION: WEBSITE DEFACEMENT & RANSOMWARE SCENARIOS

INTRODUCTION
Vulnerabilities (security vulnerabilities are flaws in a computer system that weaken the overall security of the device/system.

0-day vulnerabilities are those that the manufacturer or user of the software or system does not know about.
Website Defacement Scenario - 0-day (vulnerabilities)

**Log4Shell Timeline**

- **Nov 11**: Issue first reported on Github
- **Dec 01**: First indication of exploit in the wild
- **Dec 09**: Twitter #log4j #log4Shell
  - Tweet: Log4Shell: Exploits (including exploit examples)
- **Dec 10**: CVE-2021-44228
  - Announced
  - CVSS 10
- **Dec 14**: CVE-2021-4104
  - Published: Untrusted deserialization flaw affecting Log4j 1.2
  - CVSS 8.1
- **Dec 17**: CVE-2021-45105
  - Denial of Service (DoS) vulnerability affecting Log4j versions from 2.0-beta2 to 2.16.0
  - CVSS 5.0
- **Dec 18**: CVE-2021-45046
  - Updated to a CVSS 3.0 limited RCE vulnerability
- **Dec 28**: CVE-2021-44832
  - Limited RCE (requires access to configuration):
    - Patched with Apache Log4j 2.17.1, 2.12.4, and 2.12.2
    - CVSS 6.6

- **Dec 06**: Log4j 2.15.0 released.
  - Patching CVE-2021-44228
  - (yet un-announced)
- **Dec 13**: Log4j 2.16.0, 2.12.2
  - Released. Disabling JNDI by default as CVE-2021-44228 was deemed still exploitable in certain non-default configurations
  - CVE-2021-45046
  - Published as a limited DoS vulnerability
  - CVSS 3.7
  - CVE-2021-44228
  - New local attack vector identified

---

Image credit: [rezilion][1]

[1]: https://www.rezilion.com/
Website Defacement Scenario - Replacing site content

Website Defacement is an attack on a website that changes its appearance or content.

Websites in the gov.ua domain were compromised (as of January 14, 2022):
• Government services portal "Diia" - diia.gov.ua
• Cabinet of Ministers - kmu.gov.ua
• Ministry of Foreign Affairs - mfa.gov.ua
• State Rescue Service - dsns.gov.ua
• Ministry of Education and Science - mon.gov.ua
• Ministry of Youth and Sport - sport.gov.ua
• Ministry of Energy - mpe.kmu.gov.ua
• Ministry of Agrarian Policy - minagro.gov.ua
• Ministry of Veterans Affairs - mva.gov.ua
• Ministry of Environment Protection and Natural Resources - mepr.gov.ua
• State Treasury Service - treasury.gov.ua

Website Defacement Scenario - Replacing site content

Defacement is an attack on a website that changes its appearance or content.

Wh0ops! - Stupid!

- Hellow Goverment Polandia! -

Did you know about the issue in Indonesia related to the hacking carried out by Bjorkanism?
To the Polandia Government please for the existence of Bjorka is he Polandia?
If Bjorka's presence is in Poland & what is the intent and purpose of hacking Indonesian state documentation and distributing it publicly in open forums?!

:t.me/stupidhack

#Indonesia#Hackers#Rules

Wh0ops! - Stupid - Mc'Si0vVv - ./FellGans - $akSec166 - Atengg377
Ransomware Scenario

Types of malware

1. Malvertising
2. Cryptojacking
3. Spyware
4. Adware
5. Ransomware
6. Trojan
7. Worms
8. Rootkits
9. Backdoors
Ransomware Scenario

How Ransomware Works

1. Bad guys create ransomware themselves or buy/lease it from other cybercriminals.
2. Cybercriminals use social engineering to gain access to your network or systems.
3. They use the malware to digitally encrypt all your IT systems and data possible.
4. Attackers use your encrypted sensitive data as leverage to force you to pay a ransom.

In some cases, attackers will exfiltrate your data prior to encrypting your systems.
Ransomware Scenario

1. Attacker profiles the targeted institution through social engineering
2. Attacker sends well-crafted spear phishing emails
3. Target opens the malicious content in the phishing mail
4. Target system compromised
5. Target internal network system compromised
6. Data extraction to the APT Group

https://resources.infosecinstitute.com/topic/phishing-apt-advanced-persistent-threats/
2ND GAME SESSION: WEBSITE DEFACEMENT & RANSOMWARE SCENARIOS
Website Defacement Scenario

You are a government organization responsible for ensuring national security and you run several websites that are a trusted source of information for citizens and news agencies.

In November 2021, security researchers discovered a vulnerability that allows an attacker to take over a web server called Log4shell. Security updates resolving the issue were released on December 3, 2021. Your Organization uses the software in which the Log4shell vulnerability was discovered on all Web portals that are published on the Internet.
Ransomware Scenario

You are a government organization responsible for ensuring national security and you run several websites that are a trusted source of information for citizens and news agencies.

On December 20, 2022, all employees of your organization received an email with the title „The Obligatory Cyber Awareness Training - announcement." In the body of the message, the Organization's Board of Directors informed employees that due to the growing number of cyberattacks, all employees are required to undergo a cyber-awareness training. Attached to the message was a pdf file with the Board's resolution and an Excel spreadsheet containing a list of available training dates. Many employees of the Organization opened both files without any verification.
Website Defacement & Ransomware Scenarios

Link to the Cyber Fortress Game:
https://cyberfortress.comcert.pl
(the Team Captain ONLY)

list of Safeguards with description:
https://cyberfortress.comcert.pl/safeguards

The Game Session will last for: 50 min
Budget: $ 1 700 000
2nd Game Session: Website Defacement & Ransomware Scenarios

Efficient Safeguards
Ransomware Scenario

The mandatory cyber-awareness training email contains an attachment with malicious content

An employee launched a malicious attachment

Malware executed commands on the command line to establish a connection to the Command&Control server

Malware has established a connection to the C&C server using non-standard ports

Malware has downloaded a file containing a malicious script
## Ransomware Scenario

1. **Malware adds a malicious script to the user account properties. The script will be executed every time the user logs in.**
2. **Malware tries to get the administrator credentials of the infected device.**
3. **Malware acquires administrative credentials of the infected device.**
4. **Malware disables antivirus protection and event logging.**
5. **Malware seeks other users’ credentials.**

### Organizational Impact
- **Integration and Access Management System (IAM):** $178,000
- **Privileged Access Management (PAM) System:** $280,000
- **Workstation protection system (End Point Security):** $88,800
- **Configuration Management Database System (CMDB):** $48,000

### Physical Infrastructure Impact
- **Application sandbox:** $45,000
- **Software whitelisting:** $88,800

### Entire Network Impact
- **Password policy:** $25,000
- **Identity and Access Management System (IAM):** $178,000

### Network Edge Impact
- **Hardening and updating of Network Servers and Devices:** $88,000
- **Configuration management:** $72,000
- **Database System (CMDB):** $48,000

### Data Impact
- **Data Sources:**
- **Data:** $88,800

### Application Impact
- **Workstation protection system (End Point Security):** $88,800
- **Configuration Management Database System (CMDB):** $48,000

### Network Impact
- **Internal Network:**
- **Host:**
- **Applications:**
- **Data:**
- **Data Sources:**
Ransomware Scenario

- Malware obtains other users' credentials
- Malware scans the infected system for version information, distribution, vulnerability, installed software, etc.
- Malware scans compromised users' files for important and sensitive data
- Malware scans the environment for network shares accessible to compromised user accounts
- Malware infects files shared via administrative network shares - in order to spread the infection

---

Blackboard Collaboration space

- ORGANIZATION
- PHYSICAL INFRASTRUCTURE
- ENTIRE NETWORK
- NETWORK EDGE

INTERNAL NETWORK

- HOST
- APPLICATIONS
- DATA
- DATA SOURCES
Ransomware Scenario

1. Malware prepares a list of files to be stolen and encrypted
2. Malware uploads files to the cybercriminals' web server
3. Malware disables the backup service
4. Malware encrypts data on infected devices

**Malware**
- Prepares a list of files to be stolen and encrypted
- Uploads files to the cybercriminals' web server
- Disables the backup service
- Encrypts data on infected devices

**Network Edge**
- Command Execution
- File Access
- Network Connection Creation

**Data Leakage Prevention (DLP) System**
- $203,000

**Web filtering**
- $150,000

**Backups**
- $178,000

**Configuration Management Database System (CMDB)**
- $48,000

**Workstation protection system (End Point Security)**
- $88,800

**Command Execution**
- $5,000

**File Access**
- $5,000

**Network Connection Creation**
- $5,000

**Taxonomy**
- **Organization**
- **Physical Infrastructure**
- **Entire Network**
- **Network Edge**
- **Internal Network**
- **Host**
- **Applications**
- **Data**
- **Data Sources**
Website Defacement Scenario

Attacker exploits the Log4Shell vulnerability in your organization's Internet-accessible systems

Attacker establishes connection to Command & Control (C2) server via proxy service

Attacker downloads tools (PsExec, Ngrok) and malware (Mimikatz) to compromised device

Attacker changes access passwords for local administrator accounts on compromised devices

Attacker creates additional local accounts with administrative privileges
Website Defacement Scenario

1. Attacker uses the Mimikatz malware to create a domain account with domain administrator rights
   - Multi-Factor Authentication (MFA)
     - $85,000

2. Attacker installs service that runs malware daily with SYSTEM privileges
   - Multi-Factor Authentication (MFA)
     - $85,000

3. Attacker uses Windows built-in accounts to run tools and commands
   - Configuration management
     - $72,000

4. Attacker adds exception to Microsoft Defender rules and lists Active Directory devices with use of PowerShell commands and scripts
   - Privileged Access Management (PAM) System.
     - $280,000

5. Attackers add exception to Microsoft Defender rules to bypass virus scanning and disable Defender’s GUI (graphical interface)
   - Identity and Access Management System (IAM).
     - $178,000

---

**ORGANIZATION**

**PHYSICAL INFRASTRUCTURE**

**ENTIRE NETWORK**

**NETWORK EDGE**

**INTERNAL NETWORK**

**HOST**

**APPLICATIONS**

**DATA**

**DATA SOURCES**
### Website Defacement Scenario

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Attacker gains credentials of other users previously logged on to compromised devices</td>
</tr>
<tr>
<td>2.</td>
<td>Attacker obtains the credentials of other users from other systems of the organization using the Mimikatz malware</td>
</tr>
<tr>
<td>3.</td>
<td>Attacker executes a Powershell script to get a list of all devices in the Organization’s Active Directory environment</td>
</tr>
<tr>
<td>4.</td>
<td>Attacker verifies access to the Internet by pinging 8.8.8.8</td>
</tr>
<tr>
<td>5.</td>
<td>Attacker uses RDP connections to infect devices in the Organization’s Active Directory environment</td>
</tr>
</tbody>
</table>

*Note: The diagram includes cost estimates for various cybersecurity measures.*
Website Defacement Scenario

Attacker removes previously used Powershell scripts

Attacker changes passwords on accounts with administrative privileges in the Active Directory environment and local accounts

Attacker makes changes to the websites published on the organization’s WWW servers, thus launching a disinformation campaign
### Summary (MITRE - Mitigations)

<table>
<thead>
<tr>
<th>Mitigation</th>
<th>Mitigated techniques use count by Threat Actors</th>
<th>Mitigated techniques use count by Malware</th>
<th>Techniques mitigated count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged Account Management</td>
<td>102</td>
<td>103</td>
<td>103</td>
</tr>
<tr>
<td>User Account Management</td>
<td>83</td>
<td>94</td>
<td>82</td>
</tr>
<tr>
<td>Pre-compromise</td>
<td>74</td>
<td>74</td>
<td>75</td>
</tr>
<tr>
<td>Audit</td>
<td>66</td>
<td>66</td>
<td>67</td>
</tr>
<tr>
<td>Execution Prevention</td>
<td>62</td>
<td>62</td>
<td>63</td>
</tr>
<tr>
<td>Network Intrusion Prevention</td>
<td>58</td>
<td>57</td>
<td>58</td>
</tr>
<tr>
<td>Restrict File and Directory Permissions</td>
<td>55</td>
<td>55</td>
<td>56</td>
</tr>
<tr>
<td>Disable or Remove Feature or Program</td>
<td>55</td>
<td>54</td>
<td>55</td>
</tr>
<tr>
<td>Password Policies</td>
<td>42</td>
<td>43</td>
<td>43</td>
</tr>
<tr>
<td>User Training</td>
<td>40</td>
<td>39</td>
<td>40</td>
</tr>
<tr>
<td>Network Segmentation</td>
<td>43</td>
<td>41</td>
<td>39</td>
</tr>
<tr>
<td>Filter Network Traffic</td>
<td>39</td>
<td>38</td>
<td>39</td>
</tr>
<tr>
<td>Behavior Prevention on Endpoint</td>
<td>37</td>
<td>36</td>
<td>37</td>
</tr>
<tr>
<td>Operating System Configuration</td>
<td>35</td>
<td>35</td>
<td>36</td>
</tr>
<tr>
<td>Multi-factor Authentication</td>
<td>40</td>
<td>38</td>
<td>36</td>
</tr>
<tr>
<td>Update Software</td>
<td>31</td>
<td>33</td>
<td>31</td>
</tr>
</tbody>
</table>

[https://jkb-s.github.io/snake-attack/](https://jkb-s.github.io/snake-attack/)
## Summary (MITRE – Data Sources)

<table>
<thead>
<tr>
<th>Data source</th>
<th>Data component</th>
<th>Sum of techniques' use count by Threat Actors</th>
<th>Sum of techniques' use count by Malware</th>
<th>Techniques count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td></td>
<td>2051</td>
<td>6431</td>
<td>326</td>
</tr>
<tr>
<td>Network Traffic</td>
<td></td>
<td>1620</td>
<td>3367</td>
<td>236</td>
</tr>
<tr>
<td>Command</td>
<td></td>
<td>1530</td>
<td>4364</td>
<td>256</td>
</tr>
<tr>
<td>File</td>
<td></td>
<td>1390</td>
<td>3304</td>
<td>280</td>
</tr>
<tr>
<td>Windows Registry</td>
<td></td>
<td>374</td>
<td>1314</td>
<td>86</td>
</tr>
<tr>
<td>Script</td>
<td></td>
<td>302</td>
<td>720</td>
<td>26</td>
</tr>
<tr>
<td>Application Log</td>
<td></td>
<td>292</td>
<td>127</td>
<td>55</td>
</tr>
<tr>
<td>Module</td>
<td></td>
<td>256</td>
<td>532</td>
<td>50</td>
</tr>
<tr>
<td>Logon Session</td>
<td></td>
<td>240</td>
<td>117</td>
<td>41</td>
</tr>
<tr>
<td>Service</td>
<td></td>
<td>150</td>
<td>493</td>
<td>32</td>
</tr>
</tbody>
</table>

[https://jkb-s.github.io/snake-attack/]
## Summation (MITRE – Data Sources)

<table>
<thead>
<tr>
<th>Data source</th>
<th>Data component</th>
<th>Sum of techniques’ use count by Threat Actors</th>
<th>Sum of techniques’ use count by Malware</th>
<th>Techniques count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>OS API Execution</td>
<td>474</td>
<td>2176</td>
<td>78</td>
</tr>
<tr>
<td></td>
<td>Process Access</td>
<td>102</td>
<td>236</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Process Creation</td>
<td>1361</td>
<td>3659</td>
<td>207</td>
</tr>
<tr>
<td></td>
<td>Process Metadata</td>
<td>68</td>
<td>160</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Process Modification</td>
<td>26</td>
<td>128</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Process Termination</td>
<td>20</td>
<td>72</td>
<td>3</td>
</tr>
<tr>
<td>Process Summary</td>
<td></td>
<td>2051</td>
<td>6431</td>
<td>326</td>
</tr>
<tr>
<td>Network Traffic</td>
<td>Network Connection Creation</td>
<td>436</td>
<td>855</td>
<td>58</td>
</tr>
<tr>
<td></td>
<td>Network Traffic Content</td>
<td>609</td>
<td>1358</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td>Network Traffic Flow</td>
<td>575</td>
<td>1154</td>
<td>82</td>
</tr>
<tr>
<td>Network Traffic Summary</td>
<td></td>
<td>1620</td>
<td>3367</td>
<td>236</td>
</tr>
<tr>
<td>Command</td>
<td>Command Execution</td>
<td>1530</td>
<td>4364</td>
<td>256</td>
</tr>
<tr>
<td>Command Summary</td>
<td></td>
<td>1530</td>
<td>4364</td>
<td>256</td>
</tr>
<tr>
<td>File</td>
<td>File Access</td>
<td>270</td>
<td>560</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>File Creation</td>
<td>534</td>
<td>1031</td>
<td>88</td>
</tr>
<tr>
<td></td>
<td>File Deletion</td>
<td>53</td>
<td>236</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>File Metadata</td>
<td>249</td>
<td>676</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>File Modification</td>
<td>284</td>
<td>801</td>
<td>99</td>
</tr>
<tr>
<td>File Summary</td>
<td></td>
<td>1390</td>
<td>3304</td>
<td>280</td>
</tr>
<tr>
<td>Windows Registry</td>
<td>Windows Registry Key Access</td>
<td>40</td>
<td>118</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Windows Registry Key Creation</td>
<td>99</td>
<td>342</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Windows Registry Key Deletion</td>
<td>38</td>
<td>162</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Windows Registry Key Modification</td>
<td>197</td>
<td>692</td>
<td>58</td>
</tr>
<tr>
<td>Windows Registry Summary</td>
<td></td>
<td>374</td>
<td>1314</td>
<td>86</td>
</tr>
</tbody>
</table>

[https://jkb-s.github.io/snake-attack/](https://jkb-s.github.io/snake-attack/)
The Vendor Event
Cyber Fortress Education

Military University of Technology

WSB Universities

POLISH-JAPANESE ACADEMY OF INFORMATION TECHNOLOGY

ISSA POLSKA

POLISH NAVAL ACADEMY of the Heroes of Westerplatte
Cyber Fortress LAB

- Using Real Life IT and OT Environments
- Emulation of TTP used in game scenarios
- Checking of efficiency chosen safeguards and data sources
- Verification of resiliense and visibility of real environments
And the Winner is...

<table>
<thead>
<tr>
<th>1st Game Session</th>
<th>2nd Game Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ardenia 55,14%</td>
<td>Verden 67,04%</td>
</tr>
<tr>
<td>Delmarva 52,06%</td>
<td>Calendria 65,78%</td>
</tr>
<tr>
<td>Calendria 47,08%</td>
<td>Rivia 64,39%</td>
</tr>
<tr>
<td>Talgar 41,13%</td>
<td>Eledor 61,59%</td>
</tr>
<tr>
<td>Rivia 40,57%</td>
<td>Ardenia 58,84%</td>
</tr>
<tr>
<td>Eledor 27,27%</td>
<td>Delmarva 54,00%</td>
</tr>
<tr>
<td>Verden 27,12%</td>
<td>Talgar 53,03%</td>
</tr>
</tbody>
</table>
And the Winner is...

1st place: Ardenia – 113,98
2nd place: Calendria – 112,86
3rd place: Delmarva – 106,06
Thank you!