BLACK CELL
Protecting critical infrastructures

Heatmaps of the Adversarial Tactics, Techniques, and Procedures in the Field of Operational Technology for Electric Sector

Whitepaper

TABLE OF CONTENTS

1. INTRODUCTION

More than 60% of ICS (Industrial Control Systems) vulnerabilities disclosed can be exploited remotely, highlighting the importance of protecting internet-facing ICS devices and remote access connections. These statistics mostly happen because in terms of industry 4.0 projects, information security is still deemed as an unnecessary cost.

The goal of this paper is to aggregate, evaluate and visualize the most leveraged attack techniques against the electric sector. **The generated heatmaps, that discussed in this paper is unique, because there is no attack heatmap exist that targets the electric sector.**

The main security issue with ICS/OT (Operational Technology) devices is that they had been planned for fully segregated, insular infrastructures, with no Internet access and updates populated via removable medias in an air-gapped workflow. Therefore, when these devices and environments had been designed, security was not considered as a priority. As for the CIA (Confidentiality, Integrity, and Availability) triad, opposite priorities apply for IT (Information Technology) and OT systems. OT focuses on availability and safety, whereas for IT systems integrity and confidentiality are the top priorities.

Based on this insight on security aspects of IT and OT convergence one cannot expect that it would be a simplistic "merge" between the two. This paper summarizes the most emerging cybersecurity issues to be considered for the ICS/OT infrastructures.

1.1. THREATS

Threat means, something or someone that can obtain, damage, or destroy an asset, any possible danger. A new incident that potentially harm a system. Anything or anyone that or who can exploit a vulnerability and it doesn't matter if it is intentional or unintentional. Usually, it is estimated by the likelihood of a cybersecurity attack.

Threats can generally be categorized in one of the following: natural, unintentional, or intentional threats. Threat priorities can be different from exfiltration of secrets / ransom to large scale and persistent of compromise. Latter is typically a goal of APTs (Advanced Persistent Threats).

2. THE SCOPE OF THE RESEARCH

Intelligence is not quite useful if it cannot be processed by the entity. Therefore, when the scope had been defined, several aspects was considered to make the research as usable as possible in real life. The scope briefly provides an actionable threat intelligence report, which describes a sector-specific prioritised action plan to mitigate the white spots in the entities' detection ecosystems.

The other important aspect is to encompass todays' hybrid warfare spectrum, including critical infrastructure systems, of which the OT systems are the most vulnerable. In this paper one of the most affected sectors, the electric sector will be discussed.

The applied or created intelligence must be honed by the wide professional community and/or the government. Civilian entities and industries can hardly afford intelligence specialists, but they can collect and use information later turned into intelligence. It could be high-level IoCs (Indicator of Compromise) such as a domain or an IP address of a C2 (Command&Control) server, malware signatures, vulnerability disclosures,

dumps, leaks and so on. This paper focuses specifically on the TTPs (Tactics, Techniques, and Procedures).

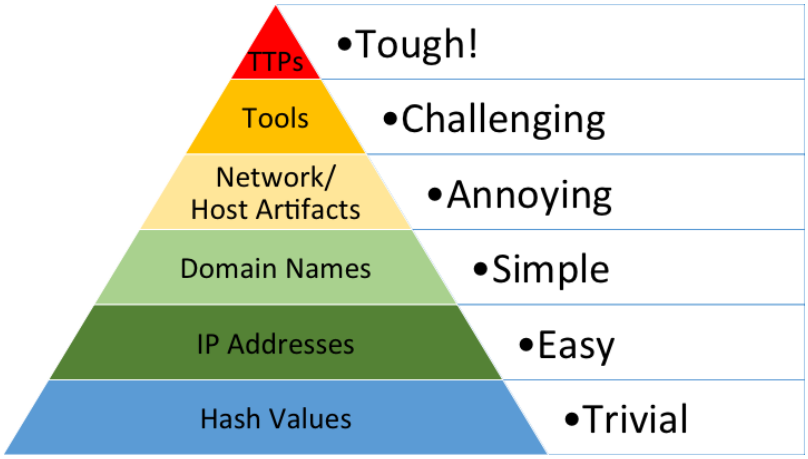


Figure 1. David Bianco – The Pyramid of Pain

Source: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

To illustrate this concept, David Bianco has created the Pyramid of Pain (Figure 1.). This is a simple diagram showing the relationship between the types of indicators that can be used to detect the adversary's activities and how much effort ("pain") it causes them when those indicators can be denied. When detecting and responding at the TTPs level, one is operating directly on the adversary's behaviours, not against their tools. In terms of pure efficiency this level is ideal. If adversary TTPs can be detected and responded quickly enough, they can be forced to do the most time-consuming thing possible: learn new behaviours [1].

3. METHODOLOGY

Numerous assessment frameworks exist that address cybersecurity, but some of them are more about the compliance or not as objective as the subject requests it or just simply unmature. MITRE ATT&CK Framework [2] is a widely accepted knowledge base

of adversary tactics, techniques, and sub-techniques. The term of TTPs describe the behaviours, processes, actions, and flows used by the adversaries to gain access to the victims' infrastructures or its elements. In this paper two specific domains of MITRE ATT&CK v12 will be discussed: "Enterprise" and "ICS". The former domain consists of 14 tactics, 193 techniques, and 401 sub-techniques and the ICS domain consists of 12 tactics, 79 techniques. It is said to be the most pragmatic way to address attacks on critical infrastructure today.

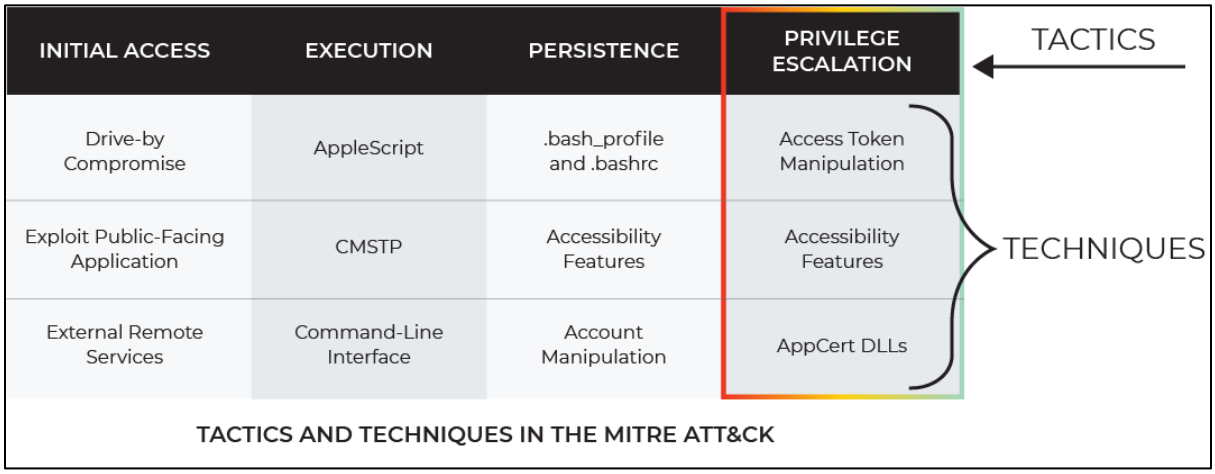


Figure 2. Tactics and Techniques in the MITRE ATT&CK

Source: https://blog.cyberproof.com/blog/creating-a-smarter-soc-with-the-mitre-attck-framework

The goal of the paper is to provide the electric – regardless of whether it is smart or not – grids, TSOs (Transmission System Operators), DSOs (Distribution System Operators), nationally distributed systems, microgrids a way to develop, organize, and adopt a threat-informed defensive strategy in a standardized and prioritised way, based on their sector [3]. The results clearly highlight those techniques that are essential to monitor them, to define alerts on them and to properly react on them. This capability requires visibility with drilldown opportunities in the corresponding datasets. For measurement purposes a logging gap analysis should be conducted. The entities must collect the proper events for their detection use cases, i.e., events and series of

events where alert setting is based on the risk tolerance by correlation rules or queries. Without the proper data, there cannot be a proper detection.

As there are numerous historical data and analyses on cyber-attacks, this research intends to focus on aggregating the most actionable methods for detecting adversary TTPs. In addition to the analyses, nearly all available and relevant information was gathered about each incident for which the following sources have been used:

- **Clear web:** On the clear web (everything that is indexed by the most popular search engines, or in other words, where robots.txt exists) a special workaround called Google Dork has been used that strongly supports targeted OSINT (Open-Source Intelligence) activities. Dorking or GHDB (Google Hacking Databa) is a resource for security researchers, where Google's proprietary built-in query language can be used. These fit for the purpose regarding this research.
- **Deep web:** For the further analysis to drill-down or enrich the data, the deep web had been used, where robots.txt does not exist or is not allowed.
- **Meta Search Engine:** For meta search engine, SearX had been used.
- **Dark web:** The dark web has also been taken advantage of by a commercial tool – made by Cyber Intel Matrix – that allows to be crawling not just TOR, but I2P and Zeronet/Freenet as well. This tool also provides a Telegram, Twitter, and Discord crawler, that proved to be useful.

The first step of outlining the research methodology was to pinpoint the most relevant incidents, where the search process was structured by first setting up the scope of the search, then breaking it down. Therefore, "skeleton queries" had been defined for Dorking, that have met certain criteria. This revealed the most interesting incidents that had been flagged for drill down.

As the incidents that have the impact or potential had been selected, the drilldown phase was followed. That process was about to collect all kind of information that is relevant or linked to the specific incidents. Reducing the noise and filtering out the inappropriate materials were the biggest part of the research.

After the proper materials had been prepared, all the data had to be reviewed, and specific malwares and tools had to be identified that had been retrieved from the techniques and procedures used in each cyber incident. In this phase the nature of the attack, the campaign had to be analysed. In most cases the enrichment of the data was needed when the used tools, an attack surface, an APT, a criminal gang, or new IoC revealed. To determine the concrete statement or finding the used techniques, MITRE ATT&CK's website had been used to query with the extracted command, tool, or procedure. With the retrieved information from MITRE, the technique could be precisely determined, and the tactic could be pinpointed from the technique.

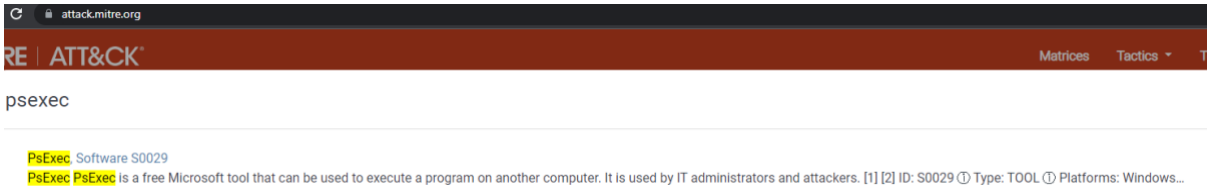


Figure 3. Techniques Used by Turla

Source: https://attack.mitre.org

APT groups and other criminal gangs – that widely used as a synonym although it is worth treating them separately – usually specialized for certain sectors. In this paper the used name convention is threat actors or adversaries. Each actor's profile, based on MITRE, so they can be used to map observed behaviours to possible adversaries [4]. The threat profile for threat actors may contain a list of the exploitation tools, malwares, typical techniques used at various stages of the attacks they had been responsible for in the past. Some of them have coverage in both domains of MITRE ATT&CK (ICS and Enterprise) some of them just have in one of them.

What makes this phase easier is that there is a kind of "recycling". For example, reusing of old-fashioned tools like Mimikatz (widely used open-source credential dumping

tool) is still very common. To evade the defence, these usually still use obfuscation, code hiding, but adversaries cannot do much against TTP based detections.

In the next step, the threat actors had been filtered based on the sectors where they operate and an offender heatmap was created using a Github project called MITRE ATT&CK Navigator [Appendix I] .

The whole process in simple terms:

1. **Step 1** – Find the most relevant incidents
2. **Step 2** – Gather all available information about the incidents
3. **Step 3** – Pinpoint the used tools or malware
   3.1. Determine the used attack techniques
   3.2. Try to determine the attack procedures
4. **Step 4** – Identify the threat actors (APT, criminal groups)
   4.1. Gather the typical attack techniques
   4.2. Try to determine the attack procedures
5. **Step 5** – Determine the involvement of the human factor from the victim's side
   5.1. Determine the used attack techniques
   5.2. Try to determine the attack procedures

Regarding the heatmap, first, the layers had to be defined. Layers provides a matrix view of tactics and techniques for a specific technology domain (Enterprise and ICS). ATT&CK Navigator can manipulate both technology domains' knowledge bases. Within a technology domain, the Navigator allows to filter the view of the matrix in a variety of ways, displaying the tactics and techniques that are important for the scope. The definition of any technique can be viewed in the visible matrix by right-clicking on the technique and selecting "view technique" in the pop-up menu. A new browser tab will be opened displaying the definition of the technique. In this way the Navigator allows to explore a given ATT&CK matrix and access the definitions of the techniques. Beyond the filters, layers also provide options for customization of the view of the matrix. The features of colouring, hiding, commenting, and assigning numeric scores,

links, and metadata to techniques are available in order to help with the analysis of threats and the identification of defences against those threats. As stated earlier, the Navigator is designed to be simple, allowing to assign any meaning to the color-coding, scores, and comments. This way the Navigator can support the purposes of any research without requiring changes to the Navigator code itself [5].

Each created layer is independent. These layers are the following:

- **'Analysed incident and the identified tools or malwares' layer,**
- **'Threat actor groups' layer,**
- **'Entry points' layer:** that had been built from determining the involvement of the human factor.

A value had been allocated to the techniques in each layer that reflects on various field where some vectors were considered.

1. **Impact Score**

   The first one was the impact score with a range of 1-5 where value 1 stands for techniques that have impact that the victim could solve in days, value of 5 stands for techniques where, human life was at risk or could have died.

2. **Evasion Score**

   A score for evasion had been also calculated with a score range 1-5 where the value 1 stands for techniques that could be triggered via exiting signature-based detections tools and the value 5 applies to the techniques that could be highly covered by the operation.

3. **Complexity Score**

   A complexity vector had been also created with score range 1-5 where the required competence, experience and knowledge from the adversarial side was considered (able to use tools=1 – making tailored malware =5).

4. **Historical Successfulness Score**

The next important vector is the historical successfulness (proven) where score 1 stands for partially or no success and score 5 stands for perfect execution and full success.

5. **Data Accuracy Score**

Because of the volume of the data, a multiplier had been used in all techniques and on all layers – for example threat actors from MITRE – that reflects on the data accuracy with range of 0,5-1,5.

To mark this in the Enterprise layer for weighting RAG (Red, Amber, Green) indicators was defined, where:

- Red (X>100 points) is urgent and important,
- Amber (100>X>64) is important,
- Green (X<44) is lower priority.

The scoring gradient has been defined from green to red where the minimum value is 3,5 and the maximum value is 104.

The same methodology was used to mark the OT layer for weighting with RAG indicators, where:

- Red (X>79 points) is urgent and important,
- Amber (79>X>64) is important
- Green (X<64) is lower priority.

The scoring gradient has been defined from green to red where the minimum value is 5 and the maximum value is 79.

4. ANALYSED INCIDENTS, THREAT ACTORS AND IDENTIFIED TOOLS OR MALWARES

Evolution of tradecraft represents an evolution of capabilities regarding the adversaries. To fully comprehend this evolution targeting the electric sector the mother of all such malware, Stuxnet must be understood.

4.1. STUXNET

Stuxnet was the first confirmed attack against OT where a tailored malware was leveraged. The Windows part of the code armed with four zero-day exploits. The most interesting component, however, was the malware payload that was OT specific. It had deep knowledge about the industrial processes. In IT it is important for adversaries to identify vulnerabilities and exploit them to load malware and gain privileges on systems. In OT the adversaries need to learn the physical process like engineering of the systems and their components in how they work together. Stuxnet's strength was leveraging functionality in Siemens devices to interact with uranium enrichment centrifuges through abuses of those normal functionality. The purpose of these equipment was to be able to control and change the speed of the centrifuges. Stuxnet had a pre-programmed knowledge on the speeds that would cause the centrifuges to burst from their casings. OT malware leveraging knowledge of industrial processes was now a thing. It was specific to Siemens equipment and unique for the facility in Iran [6]. For this reason, **Stuxnet is not included in the heatmap**. There were some kind "variants" like Flame, Duqu, but those were not necessarily used to target the electric sector.

4.2. DRAGONFLY

It was an espionage campaign with the targets being more than 2,000 sites of an electric power and petrochemical asset owners. The Dragonfly campaign leveraged the Havex malware. There was one commonality between implementation, integration, and the physical processes required at each site and that was the OPC protocol. It is a kind of universal translator for many industrial components and is readily accessible in an HMI or dedicated OPC server. Havex leveraged legitimate functionality in the OPC protocol to map out the industrial equipment on the OT network. There was no kind of physical disruption or destruction, but it was designed to attack in the future with another specific malware.

4.3. BLACKENERGY 2

This OT specific malware contained exploits for specific types of HMI applications like Siemens Simatic, GE CIMPLICITY, and Advantech WebAccess. Blackenergy 2 was a smart approach against Internet connected HMIs. Upon exploitation of the HMIs, the adversaries had access to a central location in the OT to start to learn the industrial process and gain the graphical representation of that OT through the HMI. Gaining a foothold in these networks that had access to lot of components of the OT while maintaining C&C to Internet locations are not enough to cause physical damage, but it is an ideal for espionage. Since it was not electric specific it does not have a layer, but the Sandworm team whose developed it has.

4.4. BLACKENERGY 3

This was a revolutionary cyber-attack against electric grid operators three power companies in Ukraine on 23rd December 2015. It was the first known event when a cyberattack had disrupted an electric grid. The suspected offender was the Sandworm team, and they used the Blackenergy 3 malware. Blackenergy 3 does not contain any

kind of OT components in the way that Blackenergy 2 does. Sandworm leveraged the malware to gain access to the IT networks of these power companies and then pivot into the OT networks. The adversaries performed their reconnaissance where they have learned the operations and used the legitimate functionality of distribution management systems to disconnect substations from the grid. With this move they left more than 225,000 customers without power for up to 6 hours. They wiped out Windows systems with KillDisk malware and used malicious firmware updates of serial-to-ethernet devices. These resulted in the Ukrainian operators in the grid lost their ability for automated control, for up to a year in some locations.

4.5. INDUSTROYER

The Industroyer malware impacted a single transmission level substation in Ukraine on 17th December 2016. Some elements of this attack appear to have been more of a proof of concept rather than a fully capable malware, but a kind of automation can be identified. To understand this evolution, it is the codification and the scalability in the malware towards what has been learned through previous attacks. Industroyer took an approach to understand and codify the knowledge of the OT process to disrupt operations as Stuxnet did. It leveraged the OPC to help to map the environment and select its targets like Havex did. It targeted the configuration files and the libraries of HMIs to understand the environment as Blackenergy 2 had done. And took the same approach to understand OT operations and leveraging the systems against themselves like in the attack against Ukraine in 2015. It had been used all together, giving the adversaries a platform to conduct attacks against OT in various environments [5]. Because of these serious capabilities and attributes, Industroyer have the highest values in the scoreboard. Another connection with the sector: in March 2020, The European Network of Transmission System Operators for Electricity (ENTSO-E) has admitted that they fell victim to a cyberattack with the same symptoms of and Swissgrid and Fingrid a Norwegian TSO. Based on the available information it seems that it was also the Industroyer [7].

4.6. SANDWORM

The connected threat actor called Sandworm Team. Sandworm Team is a threat group with deep knowledge that has been attributed to Russia's General Staff Main Intelligence Directorate and Main Centre for Special Technologies military unit 74455. This group has been active since 2009 at least. In October 2020, the US indicted six GRU Unit 74455 officers associated with Sandworm Team for the following cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, the 2017 worldwide NotPetya attack, targeting the 2017 French presidential campaign, the 2018 Olympic Destroyer attack against the Winter Olympic Games, the 2018 operation against the Organisation for the Prohibition of Chemical Weapons, and attacks against the country of Georgia in 2018 and 2019. Some of these were conducted with the assistance of GRU Unit 26165, which is also referred to as APT28 [8].

4.7. KOREAN ELECTRIC UTILITY

In 2014 the major Korean electric utility has been affected by destructive malware, which was designed to wipe the MBRs (Master Boot Records) of affected systems. It is believed that this MBR wiper arrived to the target systems in part via a vulnerability of the HWP (Hangul Word Processor), a commonly used application in South Korea. The malware was the TROJ_WHAIM.A, which is a MBR wiper. In addition to the MBR, it overwrote the files that are of specific types on the affected system and installed itself as a service on affected machines ensuring the persistence. It used file names, service names, and descriptions of actual and legitimate Windows services that ensured a cursory examination of a system's services may not find anything malicious, helping this threat evade detection. There are no existing ATT&CK mapping structures, so I performed that manually based on Trend Micro analysis [9].

- T1566 Spear phishing: The infection was via targeted email

- T1562 Impair Defenses: Indicator Blocking because it could set the registry, HKEY_LOCAL_MACHINE\SOFTWARE\PcaSvcc\finish to 1.
- T1574 Services File Permissions Weakness: It installed itself as a service on affected machines
- T1485 Data destruction: It was able to recursively wipe folders and files
- T1561 Disk Wipe: Disk Content Wipe. It could corrupt disk partitions and obtain raw disk access to destroy data.
- T1561.002 Disk Wipe: Disk Structure Wipe. It could corrupt disk partitions, damage the Master Boot Record (MBR), and overwrite the Master File Table (MFT) of all available physical drives.

This incident may connect to the breaches of South Korean banks and media companies in March 2013 that conducted by Lazarus group and used wiper as well, but since this is highly hypothetical it cannot be layered.

4.8. INDIAN STATE LOAD DISPATCH CENTRES

In April 2022 Cybersecurity researchers observed adversaries penetrating the networks of at least seven Indian SLDCs (State Load Dispatch Centres) which oversee operations for electrical grid control. The SLDCs manage OT systems and researchers suggested that PLA-linked adversary may be involved. This targeting has been geographically concentrated, with the identified SLDCs located in North India, in proximity to the disputed India-China border. The interesting part that previously one of these SLDCs was also targeted by RedEcho activity. To achieve this, the group likely compromised and co-opted internet-facing DVR/IP camera devices for C2 of Shadowpad malware infections, as well as use of the open-source tool FastReverseProxy (FRP) [10]. RedEcho activity identified in February 2021, and one of the SLDCs targeted in these recent attacks was also targeted in previous RedEcho activity. There are also some notable distinctions that have led the researchers to the conclusion that the activity is not the part of the RedEcho campaign. In the attacks, the threat actors compromised and co-

opted internet-facing, third-party DVR/IP camera devices as C2s for Shadowpad malware infections. However, threat actors failed in compromising the OT network, but the goal behind the intrusions was likely to enable information gathering surrounding critical infrastructure systems or pre-positioning network access for future activity [11,12,13]. This layer consists of the used tools and their technic profile.

4.9. OTHER RELEVANT THREAT ACTOR GROUPS

Allanite needs to be considered since they have a serious track record that includes electric utilities as well [14]. This squad presumably belongs to a Russian cyber espionage group, that has primarily targeted the electric utility sector within the United States and United Kingdom. The group's techniques are like Dragonfly, although ALLANITE's technical capabilities did not show any disruptive or destructive signs.

APT35 or Charming Kitten, Phosphorus, Ajax Security NewsBeef (by Kaspersky) or Magic Hound is an Iranian-sponsored threat group operating primarily in the Middle East that dates back as early as 2014. The group behind the campaign has primarily targeted organizations in the energy, government, and technology sectors. There is some infrastructure overlap, but their techniques must be considered. [15].

Last, but not least XENOTIME is one of the most if not the most dangerous threat actor based on the publicly available information. These adversaries intentionally compromising and disrupting industrial safety instrumented systems [16].

5. ENTRY POINTS

This weighted layer contains the Initial Access Tactic where the adversaries are trying to get into the network. It consists of techniques that use various vectors to gain a foothold, including targeted spear phishing and exploiting weaknesses on public-

facing web servers. Footholds gained through initial access may allow for continued access [17].

As there is no statistics for the leveraged techniques under this tactic, a weighted layer had to be generated for multi-purpose. MITRE ATT&CK framework can be used as a dependency graph, where one of the most curious points is to get in the network (this is the reason that it has been highlighted). Regarding entry points 'ATT&CK for ICS' will be discussed because it contains three more techniques and it fit for the purpose for secops (security operations) aspect as well. The scoring starts from 5 to 15, to properly balance the rest of the heatmap.

5.1. DRIVE-BY COMPROMISE

This happens when the adversaries can gain access to a system when a user visits a website as part of a normal browsing session. It is a kind of watering hole attack. The adversary may target a specific entity, for example trusted third-party suppliers or other industry specific vendors, who often visit the target website. This technic had already been used in the electric sector. It is required more stages that need to hit by the adversary [17].

10 points

5.2. EXPLOIT PUBLIC-FACING APPLICATION

Adversaries could leverage vulnerability to exploit internet-facing software to get into an industrial network. This can be user applications, or an underlying networking implementation as well. Targets of this technique can be intentionally exposed for the purpose of remote management and visibility. This is a wildly used, popular technic [17].

15 points

5.3. EXPLOITATION OF REMOTE SERVICES

This technic can be uses for lateral movement and initial access well, where the adversaries can exploit a software vulnerability. This is common way for ransomware infection. There are a lot of unpublic incidents where this played a role in [17].

10 points

5.4. EXTERNAL REMOTE SERVICES

When attackers try to leverage external remote services that allow users to connect to internal network resources from external locations like VPNs (Virtual Private Network) [17].

10 points

5.5. INTERNET ACCESSIBLE DEVICE

In some aspect, industry 4.0 introduced these kinds of techniques since the data driven OT need to be connected. Access to the device was protected by password authentication, although the application was vulnerable to brute forcing. This one will be the most leveraged entry point in my opinion because these IoT (Internet of Things) devices are made on an assembly line in rush where in the most cases no chance to test, but easier to test by the adversaries [17].

15 points

5.6. REMOTE SERVICES

Remote Services receive the same score as the external one [17].

10 points

5.7. REPLICATION THROUGH REMOVABLE MEDIA

This was the Stuxnet's entry point. This enables initial access to target devices that never connect to untrusted networks but are physically accessible. It also gets 15

points because of its popularity and historical successfulness [17].

15 points

5.8. ROGUE MASTER

It happens when the attacker setup a rogue master to leverage control server functions to communicate with outstations. It is also a good technic that can be covered by impersonating a master. It also has track record. [17].

10 points

5.9. SPEAR PHISHING ATTACHMENT

It is a variant of spear phishing, and a form of a social engineering attack against specific targets. This is widely used, and regarding my experience the most leveraged entry point [17].

15 points

5.10. SUPPLY CHAIN COMPROMISE

Adversaries perform this technic to gain control systems environment access through infected products, software, workflows, or manipulation of products, such as devices or software. It can occur at all stages of the supply chain, and it can also involve the compromise and replacement of legitimate software and patches. Since HAVEX is used this technic, it received 10 points [17].

10 points

5.11. TRANSIENT CYBER ASSET

These technic targets devices that are transient across ICS networks and external networks. Normally, transient assets are brought into an environment by authorized personnel and do not remain in that environment on a permanent basis. These assets are usually needed to support management functions and may be more common in systems where a remotely managed asset is not feasible. The point is 5 because this

requires cross-domain intelligence [17].

5 points

5.12. WIRELESS COMPROMISE

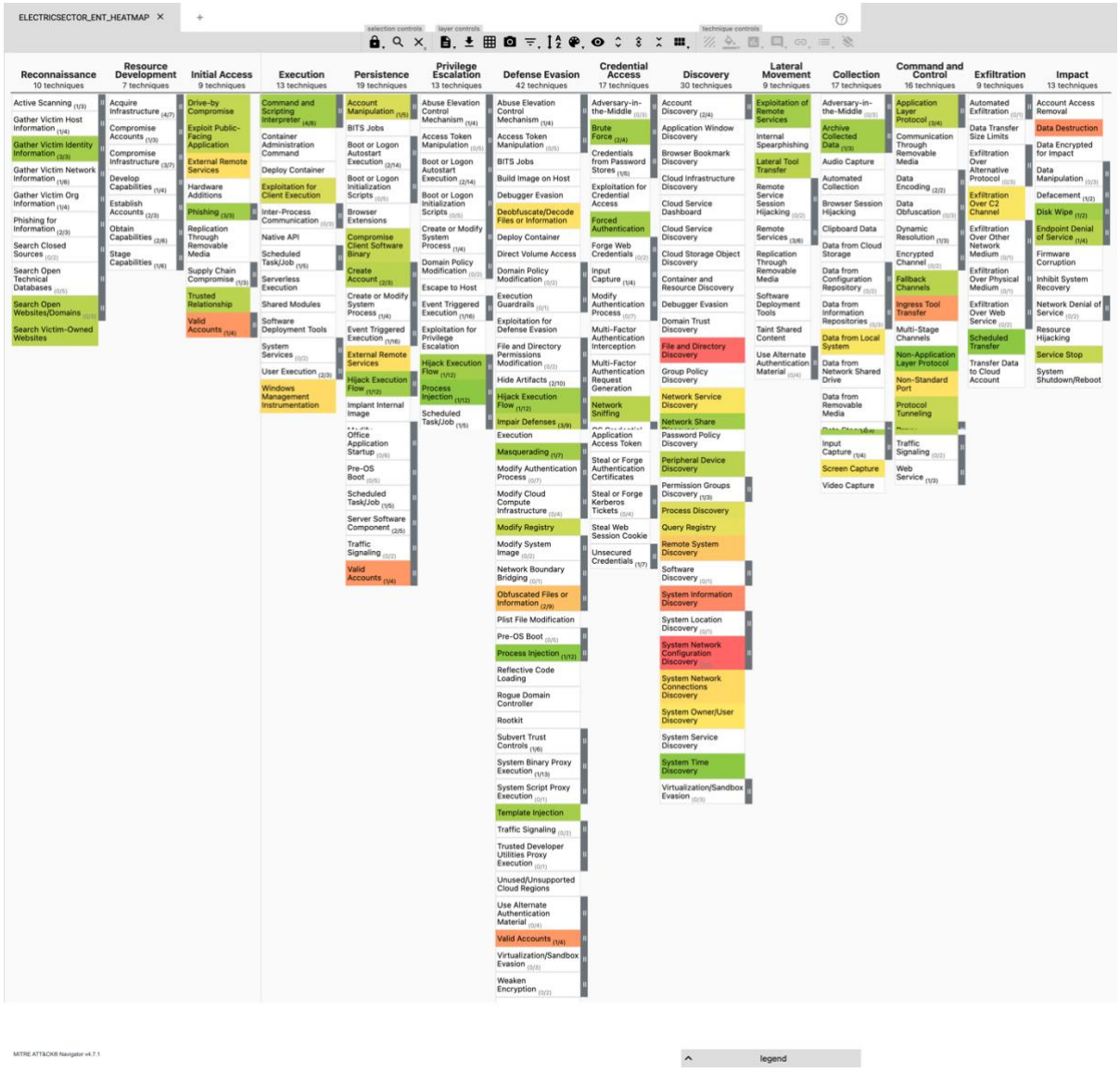
Threat actors can perform wireless compromise as a method of gaining communications and unauthorized access to a wireless network. They can utilize radios and other wireless communication devices on the same frequency as the wireless network. Wireless compromise can be done as an initial access vector from a remote distance. The electric sector is mostly "safe" against" these vectors so it received 5 points [17].

5 points

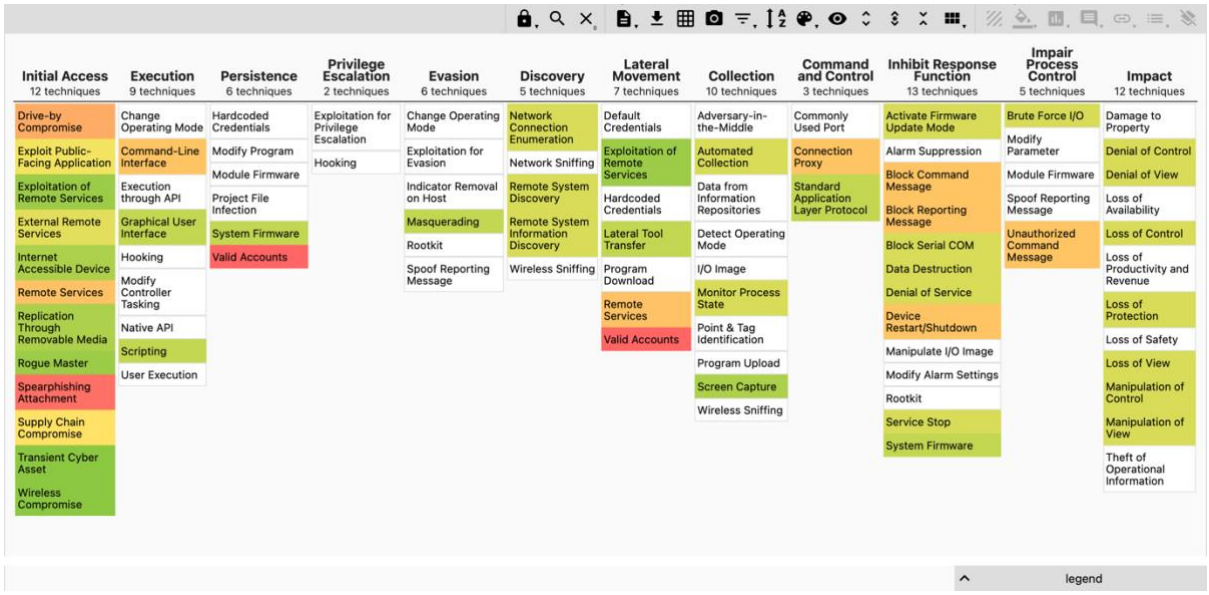
6. SCOREBOARD

Layers/score	Impact	Evasion	Complexity	Successfulness	Accuracy	**Sum**
Dragonfly	3	4	3	4	1	**14**
BlackEnergy3	4	3	3	5	1,5	**22,5**
Industroyer	5	4	5	5	1,5	**28,5**
Sandworm	4	4	3	4	1	**22,5**
Korean electric utility	3	3	3	4	1	**13**
Indian State Load Dispatch Centres	2	2	2	1	0,5	**3,5**
ALLANITE	4	4	4	3	1	**15**
APT35	3	3	3	4	1	**13**
XENOTIME	5	5	4	5	1	**19**

7. HEATMAP FOR ENTERPRISE DOMAIN



8. HEATMAP FOR ICS/OT DOMAIN



9. SUGGESTIONS

This heatmap aims to clearly pinpoint the most leveraged adversarial techniques, therefore the most important consummation of this paper is to fill the gaps in a prioritised order. DeTT&CT is a framework that could be a good support. This framework provides assistance for blue teams [Appendix I] in using ATT&CK to help them with scoring and comparing data log source, detection coverage. All the features can help in different ways, to get the electric sector more resilient against cyberattacks [18]. D3fend [19] also should be mentioned here, but it is still unmature. An excellent source could be the CAR (MITRE's Cyber Analytics Repository) that is a knowledge base of analytics developed by MITRE based on the MITRE ATT&CK adversary model. CAR defines a data model that is leveraged in its pseudocode representations, but also includes implementations directly targeted at specific tools. CAR is focused on providing a set of validated analytics [20].

To properly trigger the most urgent techniques the entities need to conduct ATT&CK based detection gap analysis. The objective is to analyse the organisation's detection coverage of generic threats. Detection coverage is to have sufficient capability to detect malicious utilization of specified tactics, techniques, and procedures (TTPs) [21]. As the comparison done the techniques that have the most score and in correspondence with the entity's infrastructure elements need to degrade to procedures.

Detecting the procedure aspect can be challenging during building detective capabilities in OT networks because even the engineers do not have a comprehensive inventory of what devices, assets, nodes are in the infrastructure. Based on best practices for OT security considerations here are some recommendations that will help organizations to protect the most essential assets and processes in today's interconnected world:

- **Continuous asset discovery** – To properly create rules and policies a dynamic inventory should be configured for the OT and IoT assets. To identify network devices the solutions should be passive (network TAP; SPAN port; packet broker) and should get the information below:
  - Device name, type, serial number, firmware version and components
  - Assets' metadata
  - Assets and subpart properties like site, name, IP address, MAC address and state
  - Embedded devices such as PLCs (Programmable Logic Controller) and their inner components
  - Logical node subsystems such as circuit breakers and switches
    - Measurement points
    - PC operating system and installed software apps with version numbers
- **Identify and prioritize vulnerabilities in OT assets** – Industrial networks contain thousands of OT and IoT devices from a variety of vendors. Unfortunately, most of those devices are not designed for the level of security required in an IIoT (Industrial Internet of Things) world and the active scanning is NOT recommended in the OT networks, not to mention penetration testing. So, nothing left just, to compare the list of the assets with vulnerability catalogue (NVD – National Vulnerability Database; CVE – Common Vulnerability & Exposures). From these data a robust vulnerability management program can be created.
- **Conduct a MITRE ATT&CK based gap analysis** – It is worth having a plan, a strategy that includes the most important key performance indicators. MITRE ATT&CK framework is one of the most comprehensive catalogues regarding the potential attacking scenarios, what must be addressed. But it is highly recommended to hire a professional company who do the assessment, based on the relevant procedures, NOT just the techniques. If the audit has been conducted based on the techniques only, that can result a false sense of security.

- **Double check the configuration of ICS devices** – It is a kind of hardening, but if the default password is changed is more than the average. With this step of user management (granting access to devices and denying access to those acting suspiciously or improperly) the attack surface can be reduced. The smaller the attack surface, the lower the risk.
- **IDPS (Intrusion Detection and Prevention Systems)** – Nearly every company has IDPS, but today sophisticated, matured workarounds should be used. Layered IDPS is where the internet facing device must perform an IPS (Intrusion Prevention System) function.
    - If a commercial firewall is in use, then it is very likely to perform this function. If there is no commercial firewall, a SNORT (open-source IDPS) with a Proofpoint ruleset must be installed.
    - All kind of VLAN (Virtual Local Area Network) have its own characteristics even if it is a homogeneous network, thus the recommendation is to implement a packet broker / TAP device or use a SPAN port to monitor the network segment with IDS (Intrusion Detection System). It can be a Suricata that have complementary rules with SNORT.
    - On the 3.5th level regarding the Purdue model [Appendix I], a firewall must be installed to separate the OT and IT. It is highly recommended to use Stateful and Deep Packet Inspection on OT specific ports (Modbus; Goose DNP3; IEC104; etc.) as well.
    - A SNORT in an IDS mode should be used in the OT environment as well where rules like stating that if the HMI (Human Machine Interface) communicates with any device other than the controller can be defined to send an alert. Another rule is 'IDS to Nothing' rule, that provides notification for the network administrator when another device attempts to communicate with it. This is a good indication that the attacker is likely to scan the network. It is a kind of deception.

- Deception is one of the best IDS tool and building deception-based IDS systems represents a high level of protection. As the cost of acquisition is relatively negligible and the expertise is more than dominant, it is therefore worth to invest in where the appropriate competence exists. There are a few solutions, like honeytokens. In this smart operation an admin username can be generated without privilege and a dummy password. If somebody tries it out, it generates an alert with a level of severity based on the source of the interaction/attack, like IP from outside the company < known malicious host (CTI – Cyber Threat Intelligence database) < internal IP address (lateral movement). But DNA honeypots; Honeyapps; ICS Honeypots; ICS honeynets (sandboxes); Fake personas; Purdue Decoy systems can also be used.
- And there is a nice to have category: building an own ML (Machine Learning) based anomaly detection, using Zeek [Appendix I] for example.

- **Calculate the business risk** – It has to be calculated for every asset across the enterprise is hard and time consuming, but it is worth doing it. The assets can be grouped.
  - The quantitative, calculated risks can be used to define the risk tolerance for each SIEM (Security Information and Event Management) use cases in the OT environment, in case if the IT and OT SIEM are separated. If there is only one SIEM instance that is responsible for IT and OT as well you OT specific rules can be also implemented, but the correlations should be taken care of.
- **Sector specific Cyber Threat Intelligence is elementary** – Choosing a solution that has the following specifications is essential:
  - ICS/OT IoCs,
  - Special detective rules against APTs (YARA, SNORT, SURICATA, SIGMA),
  - Deep, dark, and clear web monitoring capabilities, that can be used as an early warning system or to support the business risk intelligence.

- **The connected smart devices need special attention** – IIoT, IoT and IED (Intelligent Electronic Devices) such as a smart meter might create a gap in the security posture.

During the detection phase a large set of sector specific indicators can be gathered that need to be shared with the community. The most convenient way to harvest this low hanging fruit is the MISP (Malware Information Sharing Platform) which is an open-source solution for collecting, storing, distributing, and sharing cyber security indicators and threats about cyber incidents analysis and malware analysis [22]. This threat intelligence platform can be used not just for indicators, but for detections based on Sigma rules. Sigma becomes the de facto standard for expressing SIEM queries, that can be integrated into MISP events. This process is improving how Sigma rules can be shared and combining it with the MISP module makes it easier to export the rules in any format seamlessly [23].

The very last but one of the most important steps is to build a playbook for all detection with RACI (Responsible, Accountable, Consulted, Informed) and implement it into each entities' IRP (Incident Response Plan) then test it. Testing can be done by using Red or Purple Teaming [Appendix I] activity.

Updating ATT&CK Heatmap which has partially knowledge of each actor is challenging, but completely worth it. Only a piece of the puzzle can be seen because actors may change their behaviours and their TTPs evolve over time. The new incidents, and their analysed and parsed data must be introduced. Updating can be supplemented with in-house or commercial threat intelligence solutions by crawling the proper data, tagging, parsing, etc. [24].

The most matured version of this assessment and the corresponding detection capability development is a procedure based one where it will not be a matrix anymore, but a tensor.

It also needs to be mentioned that this paper is useful for the electric sector. Therefore, other sectors like finance, agriculture, health, transport, manufacturing, waterworks, aviation, telecommunication, pharma, oil, nuclear must also be addressed.

10. CONCLUSION

After a lot of security incidents that were or could have been catastrophic and warnings that the electric sector remains vulnerable, it does not take much imagination to envision what might happen if ICS facilities or systems fall into the wrong hands. As OT networks control critical infrastructures and processes, network failure inherently comes with a greater cost than in typical IT networks. The potential for substantial financial loss, environmental damage, and even loss of human life resulting from a security breach is a real possibility when considering ICS/OT risks.

Protecting connected devices requires a new approach, one that covers all assets, applies comprehensive and robust detection gap management, deploys ICS security in layers to prevent attacks from both external and internal sources, and mitigates cyber-attacks proactively. Every new ICS deployment should include the appropriate cybersecurity components to ward off attacks. And finally, business criticality should be top-of-mind when ICS security strategies are being developed and implemented [25].

Security must consider the risk posed to human safety.

11. REFERENCES

[1] D. Bianco. (2013, March 1). The Pyramid of Pain. [Online]. Available: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

[2] The MITRE Corporation. (2022, September 19). ATT&CK Matrix for Enterprise. [Online]. Available: https://attack.mitre.org/

[3] E. Alsheh. (2022, June 14). Creating a Smarter SOC with the MITRE ATT&CK Framework. [Online]. Available: https://blog.cyberproof.com/blog/creating-a-smarter-soc-with-the-mitre-attck-framework

[4] Huntsman Security. (2020, September 16). Incident Response Using MITRE ATT&CK. [Online]. Available: https://www.huntsmansecurity.com/blog/incident-response-using-mitre-attack/

[5] J. Ondricek. (2022, September 21) MITRE ATT&CK Navigator. [Online]. Available: https://github.com/mitre-attack/attack-navigator/blob/master/USAGE.md

[6] R. M. Lee. (2017, June 13). Crashoverride – Analysis of the Threat to Electric Grid Operation. [Online]. Available: https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

[7] A. Owaida. (2020, March 12). European Power Grid Organization Hit by Cyberattack. [Online]. Available: https://www.welivesecurity.com/2020/03/12/european-power-grid-organization-entsoe-cyberattack/

[8] The MITRE Corporation. (2022, September 22). Sandworm Team. [Online]. Available: https://attack.mitre.org/groups/G0034/

[9] A. Camba, M. Hsieh. (2014, December 23). MBR Wiper Attacks Strike Korean Power Plant. [Online]. Available: https://www.trendmicro.com/en_us/research/14/l/mbr-wiper-attacks-strike-korean-power-plant.html?_ga=2.245602372.1952158992.1664823338-2027659359.1664823338

[10] Insikt Group. (2022, April 6). Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group. [Online]. Available: https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets

[11] M. Demboski, B. Eskridge. (2022, May 19). Cyber Attacks on Power Grids. [Online]. Available: https://www.ironnet.com/blog/cyber-attacks-on-the-power-grid

[12] Insikt Group. (2021, February 28). China-Linked Group RedEcho Target the Indian Power Sector Amid Heightened Border Tensions. [Online]. Available: https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf

[13] Insikt Group. (2022, September 23). Research Indicators and Detection Rules. [Online]. Available: https://github.com/Insikt-Group/Research

[14] E. Nakashima. (2017, July 8). U.S. Officials Say Russian Government Hackers Have Penetrated Energy and Nuclear Company Business Networks. [Online]. Available: https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html?noredirect=on&utm_term=.548d354bff69

[15] ETDA (Electronic Transactions Development Agency). (2022, September 13). APT Group: Magic Hound, APT 35, Cobalt Illusion, Charming Kitten. [Online]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Magic%20Hound%2C%20APT%2035%2C%20Cobalt%20Illusion%2C%20Charming%20Kitten&n=1

[16] Dragos Inc. (2022, September 28). XENOTIME. [Online]. Available: https://www.dragos.com/threat/xenotime/

[17] The MITRE Corporation. (2018, October 17). Initial Access. [Online]. Available: https://attack.mitre.org/tactics/TA0001/

[18] M. Bakker, R Bouman. (2022, October 2). DeTT&CK: Detect Tactics, Techniques & Combat Threats. [Online]. Available: https://github.com/rabobank-cdc/DeTTECT Downloaded: 2022.10.02

[19] The MITRE Corporation. (2022, October 2). Defend: A knowledge graph of cybersecurity countermeasures. [Online]. Available: https://d3fend.mitre.org/

[20] The MITRE Corporation. (2022, October 2). MITRE Cyber Analytics Repository. [Online]. Available: https://car.mitre.org/

[21] Black Cell Magyarország Ltd. (2022, Ocotber 2). Analyzing Gaps in Detection Coverage with MITRE ATT&CK. [Online]. Available: https://blackcell.io/mitre-attack-based-gap-assessment/

[22] MISP project. (2022, October 5). MISP Threat Sharing. [Online]. Available: https://www.misp-project.org/

[23] T. Pratzke. (2018, October 22). New tool in Sigma toolchain: Sigma2MISP. [Online]. Available: https://twitter.com/mispproject/status/1054651166301270016 Downloaded: 2022.10.05

[24] MISP Project. (2019, October 27). Visualizing common patterns using MISP and ATT&CK data. [Online]. Available: https://www.misp-project.org/2019/10/27/visualising_common_patterns_attack.html/

[25] Balbix Inc. (2022, October 6). OT and ICS Security: The Next Big Challenge. [Online]. Available: https://www.balbix.com/insights/ots-and-ics-security-the-next-big-challenge/

APPENDIX I

MITRE ATT&CK NAVIGATOR

The ATT&CK Navigator is web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more. Source: https://mitre-attack.github.io/attack-navigator/

BLUE TEAM

A blue team is a group of individuals who perform an analysis of information systems to ensure security, identify security flaws, verify the effectiveness of each security measure, and to make certain all security measures will continue to be effective after implementation. Source: https://en.wikipedia.org/wiki/Blue_team_(computer_security)

PURDUE MODEL

The Purdue Reference Model, as adopted by ISA-99, is a model for Industrial Control System network segmentation that defines six layers within these networks, the components found in the layers, and logical network boundary controls for securing these networks. Source: https://www.checkpoint.com/cyber-hub/network-security/what-is-industrial-control-systems-ics-security/purdue-model-for-ics-security/

ZEEK

Zeek is a passive, open-source network traffic analyzer. Many operators use Zeek as a network security monitor to support investigations of suspicious or malicious activity. Source: https://docs.zeek.org/en/master/about.html

RED TEAM

A red team is a group that plays role of an enemy or competitor to provide security feedback from that perspective. Red teams are used in many fields, especially in cybersecurity, airport security, law enforcement, the military and intelligence agencies. Source: https://en.wikipedia.org/wiki/Red_team

PURPLE TEAM

Purple Teaming is a mindset that incorporates the perspective of attackers and defenders. The red and blue teams should adopt this concept to improve the organization's defensive capabalities againt real-world cyber threats. Source: https://www.picussecurity.com/what-is-purple-teaming-and-why-do-you-need-it-in-your-security-operations.