Cyberwarfare Defense Plan: Protect the Western Interconnection Power Grid

Truc L. Huynh, Computer Science

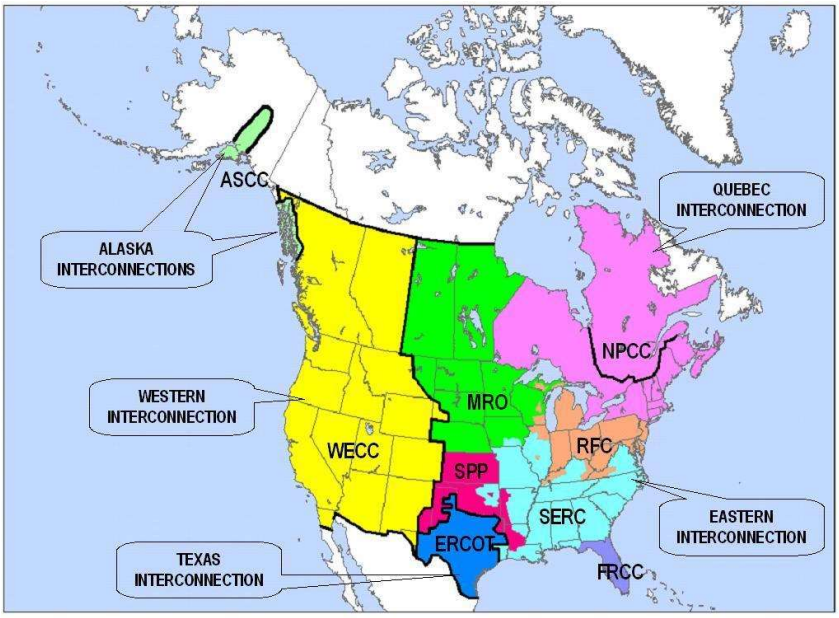
Matt Kolter, Computer Science

Purdue University Fort Wayne

Cyberwarfare Defense Plan:

PART I: Identifying Cyber Threats and Applying the Cyber Kill Chain to Protect the Western Interconnection

The interconnection power grid of the U.S Western (also called Western Interconnection) is a wide-area synchronous grid and one of the two major alternating currents (AC) power grids in the North American power transmission grid (mark yellow on the map). If this system is hit



Images retrieved from (2)

with a large-scale attack this will bring significant damage to North America (including the United States and Canada). According to our intelligence, the threat is from Russia, which is well-funded, well-equipped, and capable of a large-scale attack. They plan to install malicious software within the grid's computer network to, at some point, disrupt power to 11 states. Therefore, we analyze this threat and create a cyber-defense plan to ensure the security and safety of the Western Interconnection power grid computer network.

I- Supply Chain Security Management Issues

We introduce three supply chain security management issues: the use of the internet of things (IoT) and smart grid technologies; the lack of training for phishing attacks; and the vulnerabilities that exist in legacy systems (a combination attack).

One concern is the use of the internet of things (IoT) and smart grid technologies to connect to power meters and appliances, which could allow "an attacker to take over thousands (if not millions) of unprotected devices, preventing power from being delivered to end users". According to (3), a hypothetical attack targeted power generators of Eastern Interconnection developed by Lloyd's of London. In this scenario, the disruption of just nine transformers (10 percent of targeted generators) could cause widespread outages. The result was a blackout covering fifteen states and the District of Columbia, leaving ninety-three million people without power. Estimates economic costs are $243 billion US dollars and a small rise in death rates as health and safety systems fail.

According to (4), another threat is the use of malware dropped on electric companies' networks using spear phishing attacks that tricked employees into downloading from mock emails. These methods have successfully attacked Ukraine's power grid: In 2015 Black Energy malware and KillDisk malware destroyed part of Ukraine's power grid.

The most dangerous cyberattack as we can imagine up to now is a combination attack. In 2017, A combination attack (known as "NotPetya") using a power grid attack, a malware attack (known as "Petya"), and a security vulnerability (EternalBlue exploit) cost an estimated $10 billion. "NotPetya" access and crippled the computers of utility companies, banks, airports, government agencies in Ukraine, and some multinational corporations (FedEx, Merck, Maersk, and other corporations). According to Kenneth Geer, a veteran cybersecurity expert and senior fellow at the Atlantic Council who advises NATO's Tallinn cyber center, the "NotPetya" attack

was the most damaging attack in history and close to cyber war, and the cost far exceeded a missile fired from the Donbas into Kyiv.

II- Network Defense Strategies

There are many network defense and emergency-response vendors available but a few stand out as the leaders (5) (6) (7). Crowdstrike (https://www.crowdstrike.com) offers a complete line of products that offer protection for an entire enterprise. Cisco Secure IPS (https://www.cisco.com/c/en/us/products/security/ngips/index.html) offers both hardware and software to protect and analyze threats. Cisco also obtained Snort, an open-source intrusion prevention system, in 2013. Another hardware and software vendor is Palo Alto (https://www.paloaltonetworks.com/network-security/advanced-threat-prevention) with their Network Threat Protection product. Juniper (https://www.juniper.net/us/en/products/security/srx-series.html) offers its SRX line of firewall equipment with cloud and local-based threat detection and analytics. AlienVault USM (https://cybersecurity.att.com/products/usm-anywhere/how-it-works) owned by AT&T provides options for many environments including virtual environments. Cynet XDR and 360 (https://www.cynet.com/platform/) offer detection, correlation, and investigation software solutions. Last, but not least, Proofpoint Advanced Threat Protection (ATP) (https://www.proofpoint.com/us/products/advanced-threat-protection) is another option to assist in protecting against cyber threats.

PART II: Malware Threats

I- Identifies and Describes Malware Threats

Possible malware that could affect the Western Interconnection power grid computer network: NotPetya (malware), Stuxnet (worm), and Flame (malware). This malware can be installed on the system by:

- Social Engineering: for example, a USB attack is a method that tricks company staff by plugging an anonymous USB into the computer system. Or Human Interface Device spoofing (HID) is the method that tricks company staff to plug malware-infected hardware into their system. E.g., a designed keyboard that can grant remote access to hackers was designed to trick an employee's computer into thinking it's a regular keyboard.
- Phishing: Spear phishing is the method that tricks company staff into running a malware-infected attachment. (1)
- Other methods can also be used, but they may require time and money in developing sophisticated tools: zero-day attacks, advanced malware, and strategic web compromises

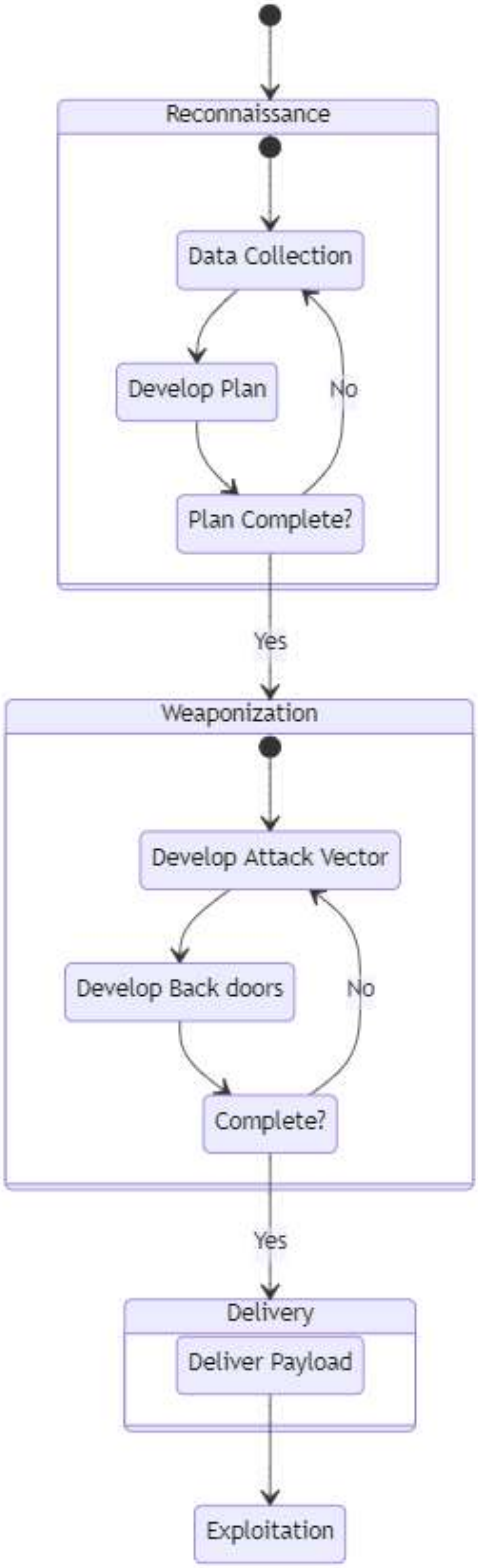
Hackers can encrypt data in computers and databases. Viruses can also spread to other computers within the network or send collected information to hackers. Hackers then can leverage this initial access to gain access to sensitive company information stored on its internal system. Further cyber-attacks can occur when enough sensitive information is collected (1).

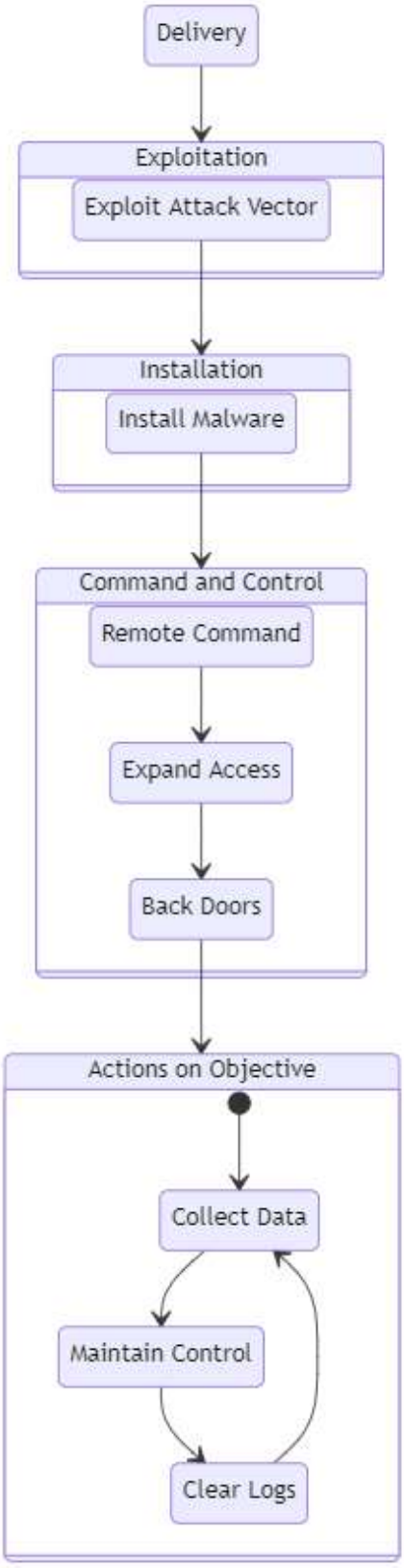
II- Cyber Kill Changes in the Western Interconnection

- Reconnaissance: Russia acknowledges the USA and its allies as a threat to them. In the situation that war (physical or cyber) happens, they can turn off the power supply of 11 states in the West.
- Weaponize: The weapon in this scenario is malicious software that will be installed (or may already happen) within the grid's computer network

- Delivery: The method most likely is social engineering (spear phishing, USB attack, or HID). The attack may happen with the help of insiders.
- Exploit: There are a couple of initial steps that hackers can use: Malware-infected USB may drop into the computer network area and accidentally plug into the Western Interconnection computer system. Another method is spear-phishing to trick company executives into running a malware-infected attachment. Hackers then can leverage this initial access to gain access to sensitive information that is stored in the internal system.
- Install: Most likely hackers will compromise computers on the Western Interconnection network, infecting them with malware. Remote access to internal systems should be established. That is the fastest way they get access to mass data, collect, and transfer the data to the server. The sensitive information will then be used against the Western Interconnection computer system.
- Command and Control: Control should be maintained until hackers get what they want.
- Act on Objective: The Objective would be to gain access to, disrupt, or control the Western Interconnection computer system. E.g., hackers can turn off the power of 11 states.

Cyber Kill Chain Diagram




Delivery
Exploitation
Exploit Attack Vector
Installation
Install Malware
Command and Control
Remote Command
Expand Access
Back Doors
Actions on Objective
Collect Data
Maintain Control
Clear Logs

III- Adversary Modeling

There are many ways to model an adversary. Invincea models an adversary by assigning the following attributes:

1. Adversary Type (AT)
2. Campaign Objective (CO)
3. Campaign Vehicle (CV)
4. Campaign Weapon (CW)
5. Payload delivery (PD)
6. Payload Capabilities (PC)

The adversary type (AT) is defined as one of the following: Script kiddy, Hacktivist, hacking collective, Insider threat, Cyber terrorist, Commercial hacking (IP theft, customer data, etc.), Cyber-crime, National-state intelligence agency, or Nation-state cyber warfare.

The campaign objective (CO) is defined as one or more of the following: Account take-over, Botnet farming, Identity fraud, Data control for extortion, Wire fraud, DDOS, Click-fraud, Data record theft, Intellectual property theft, Intelligence collection, Data munging, Data destruction, System destruction, or corporate shaming/political agenda.

The campaign vehicle (CV) is defined as one of the following: Spear-phish with link/attachment, Compromised legitimate website, Malicious website, Malvertising, Social Engineering, Insider threat, Remote login, Physical media (USB/DVD), or Supply chain.....

The campaign weapon (CW) is defined as one or more of the following: IE, Firefox, Chrome exploit, Adobe Flash exploit, Oracle Java exploit, Microsoft Silverlight exploit, Microsoft Office exploits, Adobe Reader exploit, User-installed malware, or Socially engineered remote access.

The payload delivery (PD) is defined as one or more of the following: Executable file – pre-assembled, Executable file – just-in-time assembly on-host, Process hijacking/ROP, Scripting, or DLL injection/side-loading.

The payload capabilities (PC) are defined as one or more of the following: Backdoor for remote access, Privilege escalation, Keystroke logging, Screen capture, Browser data munging, Ransomware, Adware, click-jacking, Network mapping, Lateral movement, Command and control, DDOS, Data discovery, Data archiving, Data exfiltration, Data corruption, Data destruction, System wiping or patching known vulnerabilities.

PART III: Defense in Depth

I- Defense-in-Depth Layer Vulnerabilities

One vulnerability in the endpoint security layer is the failure to apply patches to security flaws on time. This could be due to insufficient personnel staffing, insufficient training, insufficient knowledge of the system, or negligence. Patch management is a common practice to manage third-party software vulnerabilities in operating systems, web servers, SQL servers, and many other services providing capability and products to the enterprise. According to Argonne National Laboratory (10), 59% of vulnerabilities are due to patch management. Many of the major data breaches are found to be due to patches not being applied promptly and known exploits being utilized to gain initial access that provides the attack vector.

A second vulnerability can be found in the physical security layer. There are several exploits from leaving a terminal open and available for another user to jump on utilizing the user's access to leaving network ports active allowing a non-authorized connection onto the computer network. Another possibility is also having an insecure server room. A server room would allow direct access to collect data, change network configuration, or cause massive disruption

and damage to the system. Although these attacks are low-tech, they are sufficient to collect data, destroy systems and data, and a pathway for injecting malware onto the systems or network.

II- Applied The NSA's Information Assurance–based Defense-in-depth Strategy to the Power Grid Computer Network

The Information Assurance–based defense-in-depth strategy use layers of defenses that a modern environment may need. The US-CERT's defense-in-depth strategy elements include risk management, cybersecurity architect, physical and host security, network architecture and perimeter security, monitoring, vendor management, and human elements (1). Therefore, successive defense-in-depth layers are a good combination of technology and human knowledge.

The NSA Information Assurance is a more advanced defense-in-depth model which combines people, operations, and technology. The NSA Information Assurance model consists of multiple supporting layers that cover both the individual who uses the technology; the technology itself; and how the daily operation that supports monitors, and maintenance of the work.

1. **People:**

   Applied the NSA Information Assurance Strategy. Our power grid company can start by hiring the right people. The next step would be training and rewarding staff to ensure that they know the right thing to do based on policy and procedures. They know how to do it because of their training and because they are in an environment that helps to enforce those requirements with affect the system administration and physical security.

2. **Technology:**

   Technology that we need to implement to secure our power grid system are:

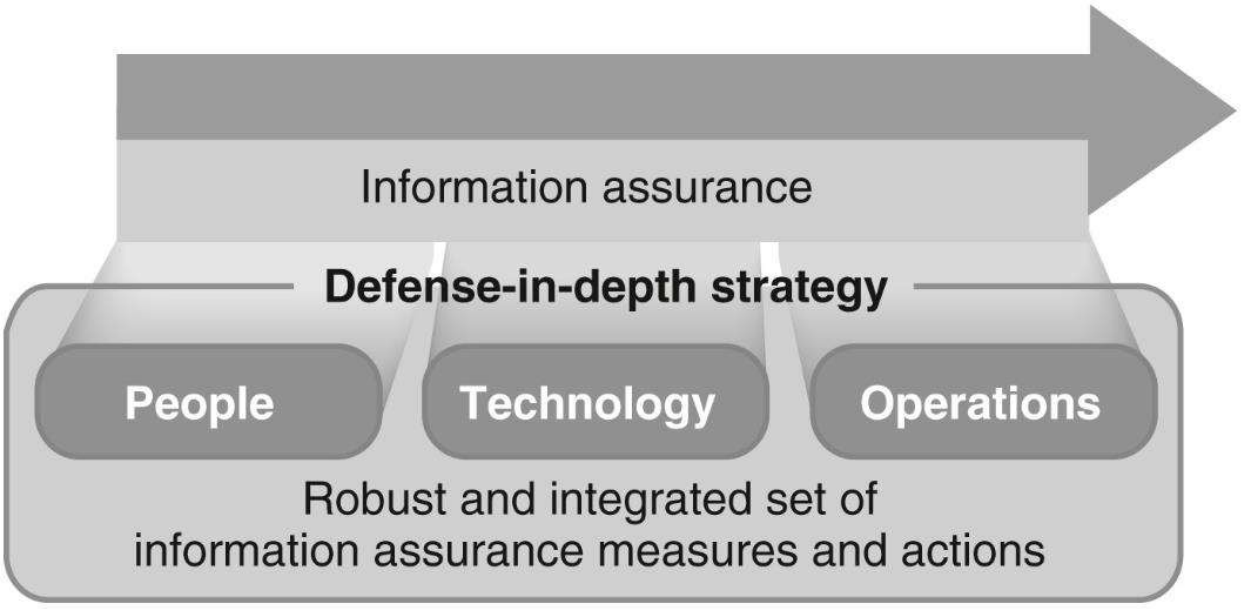
   - Defending the network and infrastructure.

- Defending the enclave boundary.
- Defending the computing environment.
- Supporting infrastructures like key management, public key infrastructure detection, and response.

  According to (1), when one layer of the power grid defense-in-depth fails, it will not affect the other layers. Another word to say is that the use of layer defense networks works together to ensure that the failure of one layer of protection will not expose the data, services, or system to hackers.

3. **Operations:**

The defense-in-depth Operation focuses on security policy, certification & accreditation, security management, key management, readiness assessments, attack sensing, warning, response, and recovery & reconstitution.



Images retrieved from (1)

The Use of A Cryptographic System Or Technique to the Power Grid Computer Network

The use of Cryptography has been around for many years to protect communication from adversaries. It relies on four major concepts confidentiality, data integrity, authentication, and nonrepudiation. There are many applications of Cryptographic Systems such as secure messages, secure voice communication, password hashing and salting (password encryption), and encrypted data storage, ….

This application can be applied in our power grid Defend-in-depth systems such as encrypting any data that is stored in the internal database that includes passwords, emails, and sensitive information. Enforce two steps or three steps authorizations for any application that requires the usernames and passwords to log in (email, web app, etc.). Make sure to follow the four major principles when applying cryptography to our system:

- Confidentiality is the ability to ensure that data are not exposed to those who should not see them. Thus, an Encryption system that cannot be broken by an opponent on time can ensure confidentiality (At least in a reasonable time frame)
- Data integrity: Which is the ability to ensure that data have not been modified either by addition or removal of data.
- Authentication is the ability to verify the identity of a sender.
- Non-reputation requires that it will be possible to prove that the sender did send the file a message. It also means that the sender cannot claim that someone falsely sends a message posing as the sender.

PART IV: Power Grid Computer Network

I- Mission assurance processes:

Western Power Grid should implement both the DOD's Mission Assurance and the NSA cybersecurity functions to ensure the security of its computer network. The DOD mission

assurance is the ability to provide continuous operation despite attacks, system failures, or other disruptions. The DOD's Mission Assurance (3020.45) provides a framework using four processes: identification, assessment, risk management, and monitoring to help protect against attacks on the nation's defense assets as well as civilian capabilities and assets. The NSA's cybersecurity functions are to identify, protect, detect, respond, and recover. These functions are part of a complete cyber security strategy used by the US government (1).

In addition to the use of existing cybersecurity frameworks, other important elements such as making sure the hardware, software, devices, and systems don't contain built-in backdoors or be compromised for other countries or threat actors. Another defense concept that should be applied is the concept that no device or network should be fully trusted (1).

The interconnection power grid of the Western Interconnection is a wide-area synchronous grid and one of the two major alternating currents (AC) power grids in the North American power transmission grid. The disruption of power to 11 states will bring significant damage to the United States. Thus, the mission assurance of protecting the power grid computer network should be identified as MAC II (which exceeds the common industry standard)

II- Industrial control systems (ICS)

Another big challenge is the attack on Industrial Control System (ICS). Since ICS are rarely patched and updated, they are less secure than traditional computing infrastructure. ICS includes supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and programmable logic controllers (PLCs).

According to (1), Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control remote equipment. SCADA is very common in industries that require remote monitoring such as natural gas pipelines, power production, distribution infrastructure,

and water supply control system. An attack against SCADA systems may target the feedback provided to the central control system or the local sensor & control unit to perform incorrect actions (shutdown, overproduction, or delay).

Distributed Control Systems (DCSs) use a combination of sensors and feedback systems to control and adjust processes as they receive feedback. Thus, providing incorrect feedback can result in a shutdown, overproduction, or delay in the system at a critical time (1).

Programmable Logic Controllers (PLCs) are designed to handle specialized input and output systems. The Modbus communication protocol between PLCs and their controller could be attacked, allowing the attacker to disable protective control and then make the system work in ways it was not intended to. Operational technology like Modbus, BACnet, And OPC Classic continues to be significant targets for attackers. The number of vulnerabilities that have been discovered each year has continued to be high, with hundreds of vulnerabilities found per year (1).

III- Necessary network defense technologies, such as firewalls, an intrusion prevention system (IPS), and SIEM devices

Necessary intrusion prevention systems (IPS) will consist of a Palo Alto IPS device that will be placed directly behind the firewall and will analyze network traffic between the firewall and the LAN. It will utilize signature-based detection such as exploit-facing signatures and vulnerability-facing signatures as well as Anomaly-based detection and Policy-based detection. Additionally, a network intrusion prevention system (NIPS) will be utilized to monitor the entire network for suspicious traffic utilizing a collection of known attacks and the capability to alert administrators to potential attacks. A wireless intrusion prevention system (WIPS) will also be deployed to prevent and detect potential attacks from threats who are utilizing a wireless vector. These two items together will provide for strong network protection and overall network health.

Host-based intrusion privation (HIPS) will be deployed on each host to scan activity and events within the host to actively prevent intrusions at the host level. Systems administrators will also be notified if any of the host systems detect anomalies.

A Log point security information and event management (SIEM) tool will be used to collect host, server, network, and firewall activity logs for consolidation, event review, and management.

IV- Network operational procedures

Procedures will be developed for maintaining patches for network hardware, firewalls, servers, hosts, and other devices on the network for firmware, 3rd party software on the systems, and operating system updates.

Procedures for hardening all devices on the network so that only the ports and services that are necessary will be open or active and connection points are limited. Administrative privileges will also be limited to minimal personnel and credentials will be reviewed regularly with password updates required per the decided schedule.

Log point has been selected as the SIEM and will be utilized for a periodic review of administrative access, user access, and specifically denials that have occurred on each system located on the network. The logs include the firewall, network hardware, servers, and host machines.

Disaster recovery procedures will be created in the event of an unforeseen event where the network, servers, data, or hosts are irreversibly disabled or destroyed and the plan to recover along with an estimate of labor, time, and material cost to resume normal operation.

A procedure will be developed to isolate, freeze, and investigate firewall, network, server, and/or host intrusions when detected. This may include isolation of certain network

nodes, temporary loss of external connectivity, host or server isolation, or a combination of several methods. The intent is to halt any loss of IP or data, preserve log information, and halt any future attacks.

References

Chapple, M., & Seidl, D. (2023). *Cyberwarfare: Information Operations in a Connected World* (Second). essay, Jones & Bartlett Learning. (1)

Knake, R., (2017) *A Cyberattack on the U.S. Power Grid*. Retrieved from https://cdn.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf (3)

Cerulus, L., (Feb 2019) *How Ukraine became a test bed for cyberweaponry*. Retrieved from https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/ (4)

Wikipedia (n.d.) *Western Interconnection*. Retrieved from https://en.wikipedia.org/wiki/Western_Interconnection#Consumption (2)

10 BEST Network Detection and Response (NDR) Vendors in 2022. (n.d.). Software Testing Help. Retrieved September 23, 2022, from https://www.softwaretestinghelp.com/best-network-detection-and-response-vendors/ (5)

Top Cybersecurity Companies for 2021 | eSecurity Planet. (2020, January 3). ESecurityPlanet. https://www.esecurityplanet.com/products/top-cybersecurity-companies/ (6)

List of Top Intrusion Detection Systems 2022. (n.d.). TrustRadius. https://www.trustradius.com/intrusion-detection (7)

What is the cyber kill chain? | Crowdstrike (2021, April 22). Crowdstrike. https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/ (8)

Invincea, (2015) *Know Your Adversary: An Adversary Model for Mastering Ciber-Defense Strategies.* Retrieved from https://www.ten-inc.com/presentations/invincea1.pdf (9)

Argonne National Laboratory. *Lack of Patch Management Leads to Increase in Cybercrime* (2015, November, 23). Retrieved October 17, 2022, from https://coar.risc.anl.gov/lack-of-patch-management-leads-to-increase-in-cybercrime/ (10)

What is an Intrusion Prevention System? Palo Alto. Retrieved November 1, 2022, from https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips (11)