FINAL REPORT

TECHNOLOGY STACK :AI FOR CYBERSECURITY WITH IBM QRADER

PROJECT TITLE: UNDERSTANDING THE CYBER THREATS

Team ID : LTVIP2024TMID11382

Team Size : 2

Team Leader : KAMBALA NAVIN

Team member : SAINI TIRUPATHI

COLLEGE: DR LANKAPALLI BULLAYYA COLLEGE,VISAKHAPATNAM

INDEX

INTRODUCTION

The **cyber threat environment** is the online space where cyber threat actors conduct malicious cyber threat activity. It includes the networks, devices, and processes that are connected to the Internet and can be targeted by cyber threat actors, as well as the methods threat actors use to target those systems.Cyber threat actors are not equal in terms of capability and sophistication. They have a range of resources, training, and support for their activities. Cyber threat actors may operate on their own or as part of a larger organization (i.e., a nation-state intelligence program or organized crime group). Sometimes, sophisticated actors use readily available tools and techniques because they can still be effective for a given task and/or make it difficult for defenders to attribute the activity—for example, by leveraging the commercial security tools used by security researchers.

Advanced persistent threats (APT) refer to threat actors in the top tier of sophistication and skill. APTs are capable of using advanced techniques to conduct complex and protracted campaigns in the pursuit of their goals. This designator is usually reserved for nation-states or very proficient organized crime groups.

State-sponsored cyber threat actors operating on behalf of nation-states primarily use cyber threat activity to advance their geopolitical objectives. They are frequently the most sophisticated threat actors, with dedicated resources and personnel, and extensive planning and coordination. Nation-states without developed cyber programs can use commercial cyber tools and the growing global pool of talent to enable sophisticated cyber threat activity. Some nation-states also have operational relationships with private sector entities and organized criminals.

The activities of state-sponsored cyber threat actors may include espionage against governments, organizations, and individuals **cyber threat surface** refers to all information systems and services a cyber threat actor may exploit in trying to compromise an individual, organization, or network. It includes all Internet-exposed endpoints, including networks, personal computers, mobile devices, Internet of Things (IoT) devices, and servers, in addition to processes that communicate with or rely on information systems connected to the Internet. Individual threat surface is also informed by the amount of personal information shared with online vendors and services; the broader an individual shares their

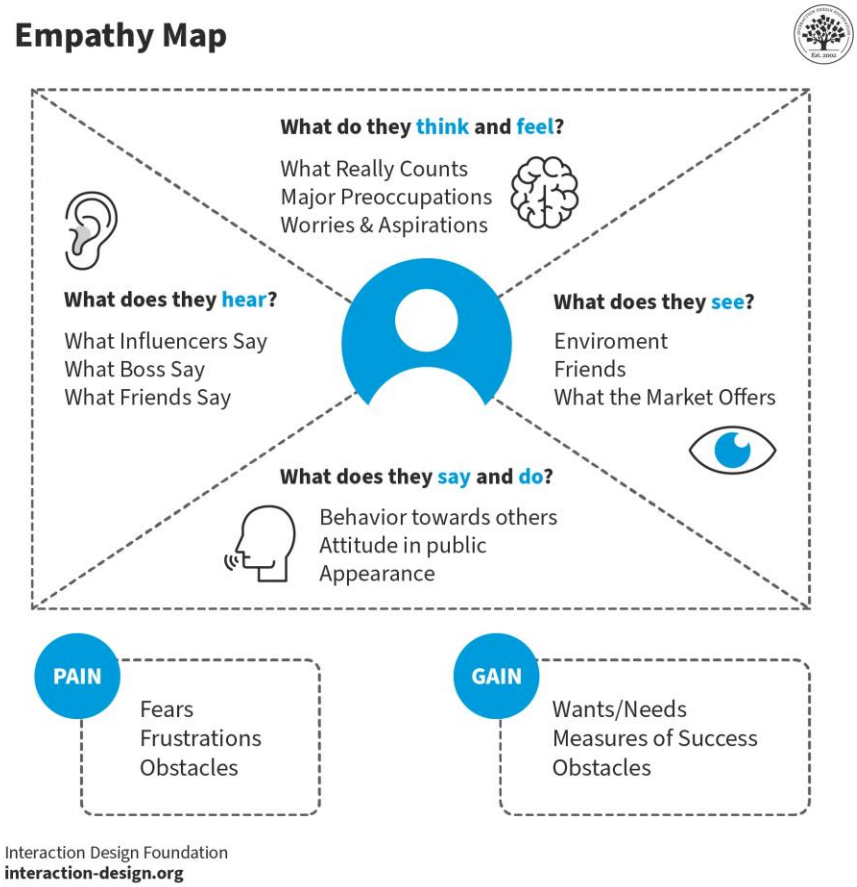
ABSTRACT

At present, most of the economic, commercial, cultural, social and governmental activities and interactions of countries, at all levels, including individuals, non-governmental organizations and government and governmental institutions, are carried out in cyberspace. Recently, many private companies and government organizations around the world are facing the problem of cyber-attacks and the danger of wireless communication technologies. Today's world is highly dependent on electronic technology, and protecting this data from cyber-attacks is a challenging issue. The purpose of cyber-attacks is to harm companies financially. In some other cases, cyber-attacks can have military or political purposes. Some of these damages are: PC viruses, knowledge breaks, data distribution service (DDS) and other assault vectors. To this end, various organizations use various solutions to prevent damage caused by cyber-attacks. Cyber security follows real-time information on the latest IT data. So far, various methods had been proposed by researchers around the world to prevent cyber-attacks or reduce the damage caused by them. Some of the methods are in the operational phase and others are in the study phase. The aim of this study is to survey and comprehensively review the standard advances presented in the field of cyber security and to investigate the challenges, weaknesses and strengths of the proposed methods. Different types of new descendant attacks are considered in details. Standard security frameworks are discussed with the history and early-generation cyber-security methods. In addition, emerging trends and recent developments of cyber security and security threats and challenges are presented. It is expected that the comprehensive review study presented for IT and cyber security researchers will be useful. Cyber-attacks fall into a broader context than what is traditionally called information operations. Information operations integrated use of the main capabilities of electronic warfare, psychological, computer network, military trickery and security operations in coordination with special support and relevant abilities and to penetration, stop, destroy or hijack human decisions and It is one of the decision-making processes of national institutions (Hart et al., 2020). Fig. 1 describes the anatomy of a cyber-attack. From the USNM Strategy for cyberspace operations, computer network operation is composed of the attack, defense, and utilization enabling (Ma et al., 2021). Computer network exploitation enabling operations can also be carried out with the aim of stealing important computers data. In such a context, Trap Sniffers and Doors are beneficial tools for cyber espial (Liu et al., 2021). Trap Doors permit an external user to accessibility software at any time without the knowledge of the computer user. Sniffers are a tool to steal usernames and passwords (Karbasi and Farhadi, 2021). Table 1 describes the basic definitions and concepts of cyberspace. The consequences of cyber warfare can include the following (Khan et al., 2020, Furnell and Shah, 2020, Mehrpooya et al., 2021

EMPATHY MAP CANVAS

The empathy map for UNDERSTANDING THE CYBER THREATS allows us to sum up our learning from engagements with people in the field of design research. The map provides four major areas in which to focus our attention on, thus providing an overview of a person's experience. Empathy maps are also great as a background for the construction of the personas that you would often want to create later.

An Empathy Map consists of four quadrants. The four quadrants reflect four key traits, which the user demonstrated/possessed during the observation/research stage. The four quadrants refer to what the user: Said, Did, Thought, and Felt. It's fairly easy to determine what the user said and did. However, determining what they thought and felt should be based on careful observations and analysis as to how they behaved and responded to certain activities, suggestions, conversations, etc.



BRAINSTORMING AND PRIORITIZATION

Brainstorming is a method design teams use to generate ideas to solve clearly defined design problems. In controlled conditions and a free-thinking environment, teams approach a problem by such means as “How Might We” questions. They produce a vast array of ideas and draw links between them to find potential solutions.

Prioritization is the process by which potential development items are ranked in order of importance. In terms of product management, this means determining which themes, initiatives, or features should get slotted into the product roadmap and the next set of upcoming product releases. Cyber security threats today have become increasingly sophisticated and complex. Organizations, however, have not been able evolve at the same pace. As they move ahead and embrace new technologies without fully comprehending the implications these have on the entire enterprise, they are rendering themselves susceptible to an array of cyber security threats.

As the threat landscape evolves with escalating speed, it takes smarter cyber security services to successfully protect your organization. With the right combination of cyber security services and information security technology, you can operate more successfully in a world where everything is increasingly linked together.

Choosing the right cyber security services partner is critical. You need a partner with deep expertise in defending against a growing universe of threats. You need a partner with broad experience to fill in whatever gaps exist in your security capabilities and know-how. And you need a partner with comprehensive connections to cyber security companies that enable you to put together the perfect mix of defenses for your unique security challenges.

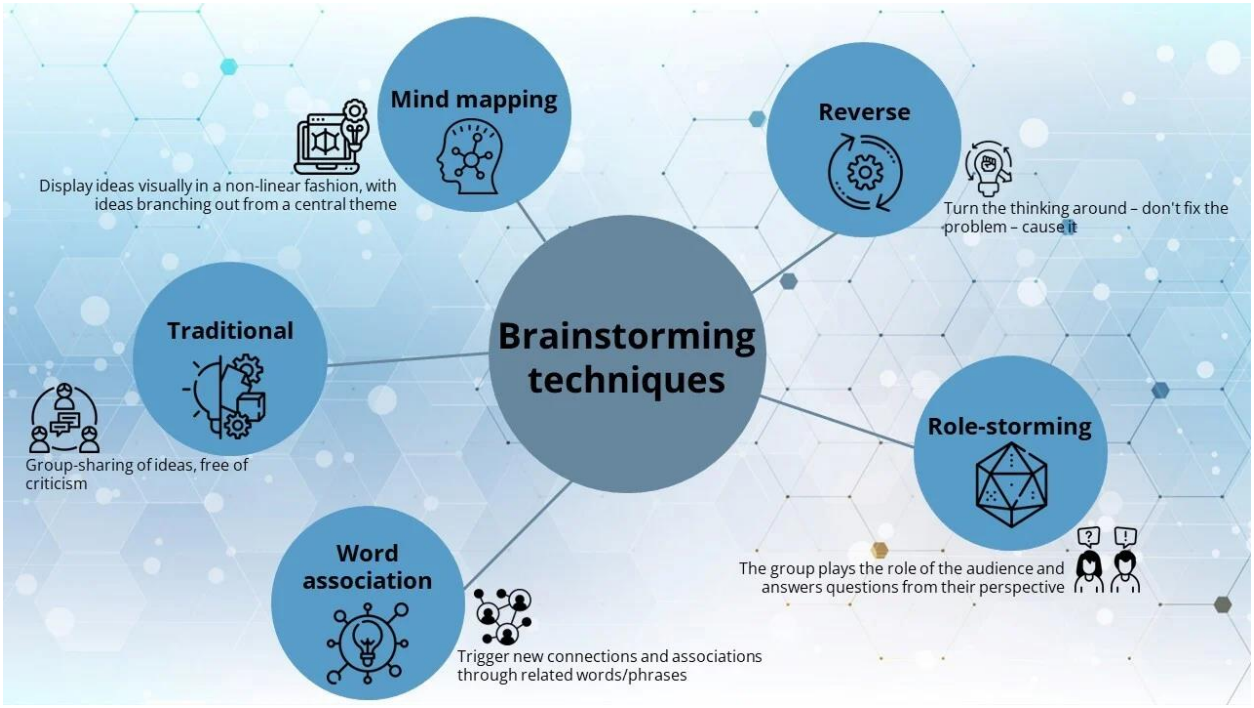
For the purpose of prioritizing threats, the contact frequency is essentially the likelihood that an organization will show up on the threat actor’s radar, and the probability of action is the likelihood that the threat actor will actually target the organization as part of an ongoing campaign.

The vulnerability parameter also comprises two distinct factors:

Threat capability—The probable level of force a threat agent is capable of applying against an asset.

Resistance strength—The strength of a control compared with a baseline measure of force.

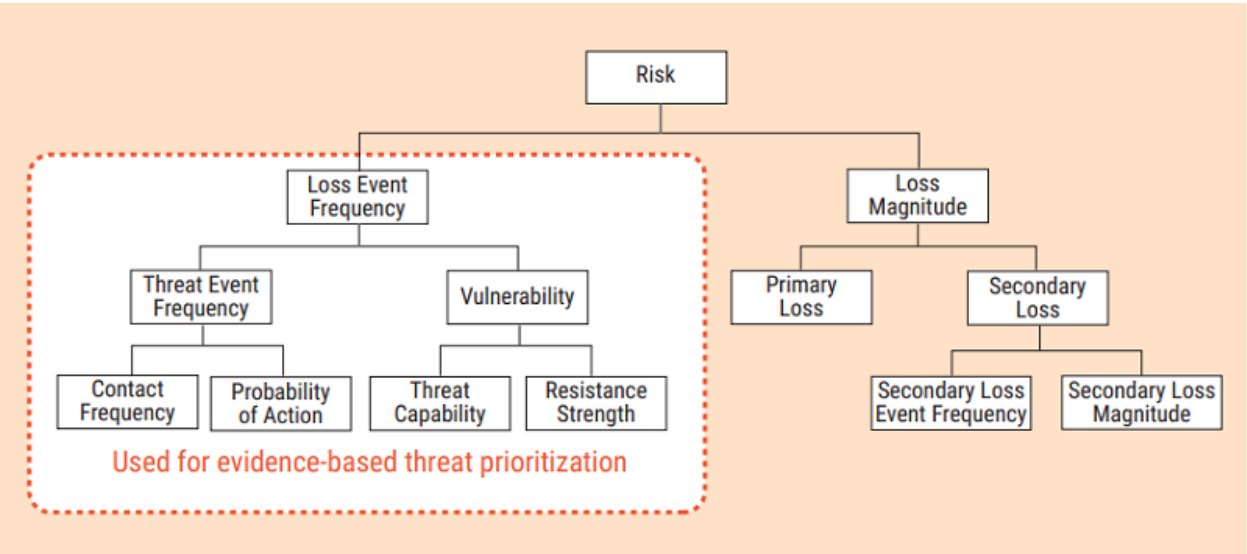
For purposes of evidence-based threat prioritization, these two factors can be combined by mapping the tactics, techniques and procedures (TTPs) the threat actor has employed in this or similar campaigns to the presence and strength of the security controls implemented .



The idea is to assess which techniques and procedures the actor can and cannot successfully execute. Other factors may also be considered, such as the threat actor's resources and adaptability (threat capability) and the patch levels of the organization's technical assets (resistance strength).

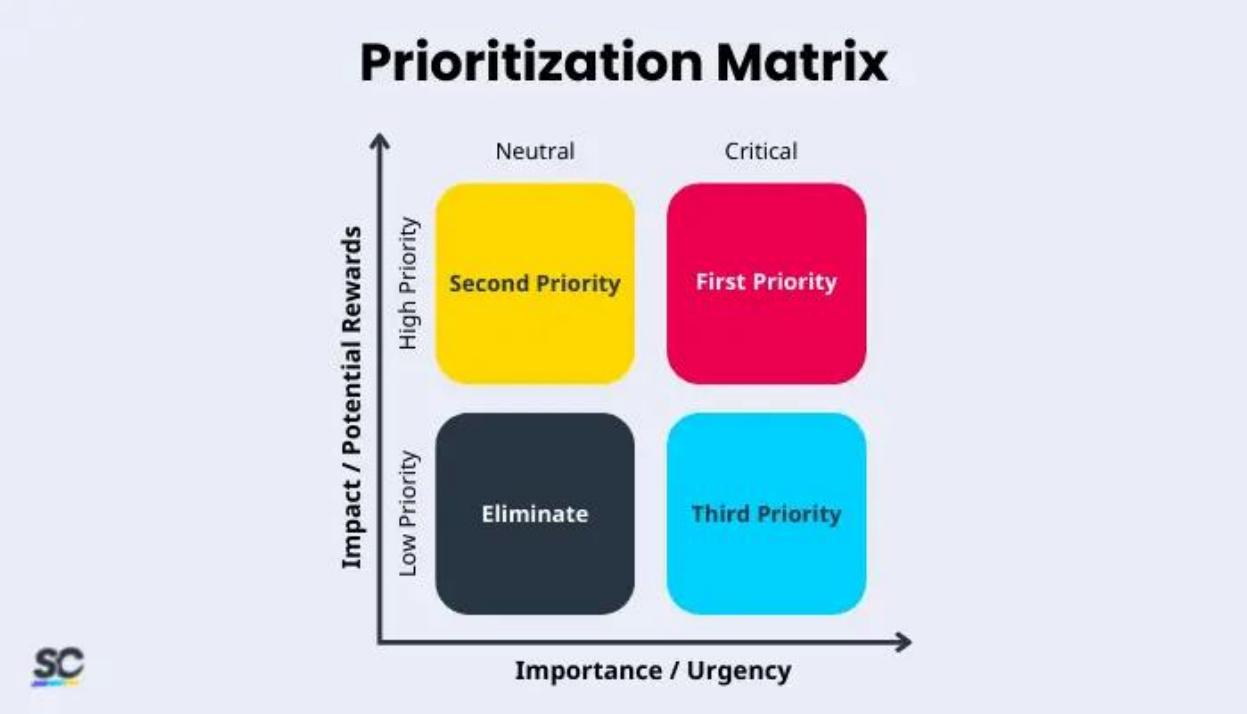
The essential goal of threat prioritization is to determine the likelihood that a specific campaign (carried out by a particular threat actor) will manifest itself within the enterprise under consideration. This likelihood should be deduced from actual threat events observed by the enterprise (e.g., events in its security monitoring systems) or retrieved from external sources (e.g., public threat reports, commercial cyberthreat intelligence [CTI] feeds, closed CTI communities). Typically, risk assessment methodologies do not provide guidance or models to weigh these threat events and make a quantitative appraisal of the risk they pose. However, Factor Analysis of Information Risk (FAIR) provides a model for understanding, analyzing and quantifying cyberrisk that includes a taxonomy of factors contributing to such risk (figure 1).5, 6 The loss event frequency (LEF) leg of the model provides a particularly good starting point for evidence-based threat prioritization.

Figure 1—FAIR Risk Taxonomy Focusing on Loss Event Frequency



Threat Capability

Threat capability focuses on different characteristics of the threat actor behind the campaign. For instance, STIX defines seven sophistication levels, ranging from none to strategic.7 In addition, the threat actor's known capabilities.



STAGE-1

TITLE OF THE PROJECT: UNDERSTANDING THE CYBER THREATS:EXPLORING THE NESSUS AND BEYOND SCANNING TOOLS

OVERVIEW:

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called electronic information security or information technology security.

Today's cyber threat landscape is constantly evolving. Modern organizations face a growing number of cyber threats that are increasingly complex. There's no one-size-fits-all formula for deciphering exactly what a cyber threat may be for your organization compared to another. However, understanding your cyber threat landscape, as well as how to prioritize cyber threats for remediation, is a great first step in developing a cybersecurity program. As you understand more about the cyber threats your organization faces and the potential impact on your most critical operations, the more prepared you will be to adapt your cyber hygiene practices and mature your cybersecurity measures over time.

he National Institute of Standards and Technology (NIST) defines a cyber threat as a circumstance or event that could potentially negatively impact operations. For example, if an attacker successfully exploits the threat, it could result in losing the ability to deliver products or services.

As a result, there could be far-reaching impacts on your relationships with your customers, your brand, your vendors, partners, key stakeholders, and, in some extreme cases, the market you're in. A cyber threat can also negatively impact your internal operations and staff. For example, if your organization is a critical infrastructure provider, there may be potential for negative impact on the nation from these threats.

In many cases, a successfully exploited cyber threat can result in a threat accessing a range of important and sensitive data, which the attacker could destroy, make public, change, or create a denial of service (DoS).

LIST OF THE TEAM MATES

S.NO	NAME	COLLEGE	CONTACT
1	KAMBALA NAVIN	DR LB COLLEGE,VSKP	Naveenkambala963@gmail.com
2	SAINI TIRUPATHI	DR LB COLLEGE,VSKP	Tirusaini96@gmail.com

UNDERSTANDING THE CYBER THREATS

Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems. Common categories of cyber threats include malware, social engineering, man in the middle (MitM) attacks, denial of service (DoS), and injection attacks—we describe each of these categories in more detail below.

Cyber threats can originate from a variety of sources, from hostile nation states and terrorist groups, to individual hackers, to trusted individuals like employees or contractors, who abuse their privileges to perform malicious acts.

A cybersecurity threat is a harmful activity committed with the intent of destroying, stealing, or disrupting data, critical systems and digital life in general. Computer viruses, malware attacks, data breaches, and Denial of Service (DoS) assaults are examples of these risk

TYPES OF CYBER SECURITY THREATS

Malware Attacks

Malware is an abbreviation of “malicious software”, which includes viruses, worms, trojans, spyware, and ransomware, and is the most common type of cyberattack. Malware infiltrates a system, usually via a link on an untrusted website or email or an unwanted software download. It deploys on the target system, collects sensitive data, manipulates and blocks access to network components, and may destroy data or shut down the system altogether.

Social Engineering Attacks

Social engineering involves tricking users into providing an entry point for malware. The victim provides sensitive information or unwittingly installs malware on their device, because the attacker poses as a legitimate actor.

Supply Chain Attacks

Supply chain attacks are a new type of threat to software developers and vendors. Its purpose is to infect legitimate applications and distribute malware via source code, build processes or software update mechanisms.

Attackers are looking for non-secure network protocols, server infrastructure, and coding techniques, and use them to compromise build and update process, modify source code and hide malicious content.

Supply chain attacks are especially severe because the applications being compromised by attackers are signed and certified by trusted vendors. In a software supply chain attack, the software vendor is not aware that its applications or updates are infected with malware. Malicious code runs with the same trust and privileges as the compromised application.

Man-in-the-Middle Attack

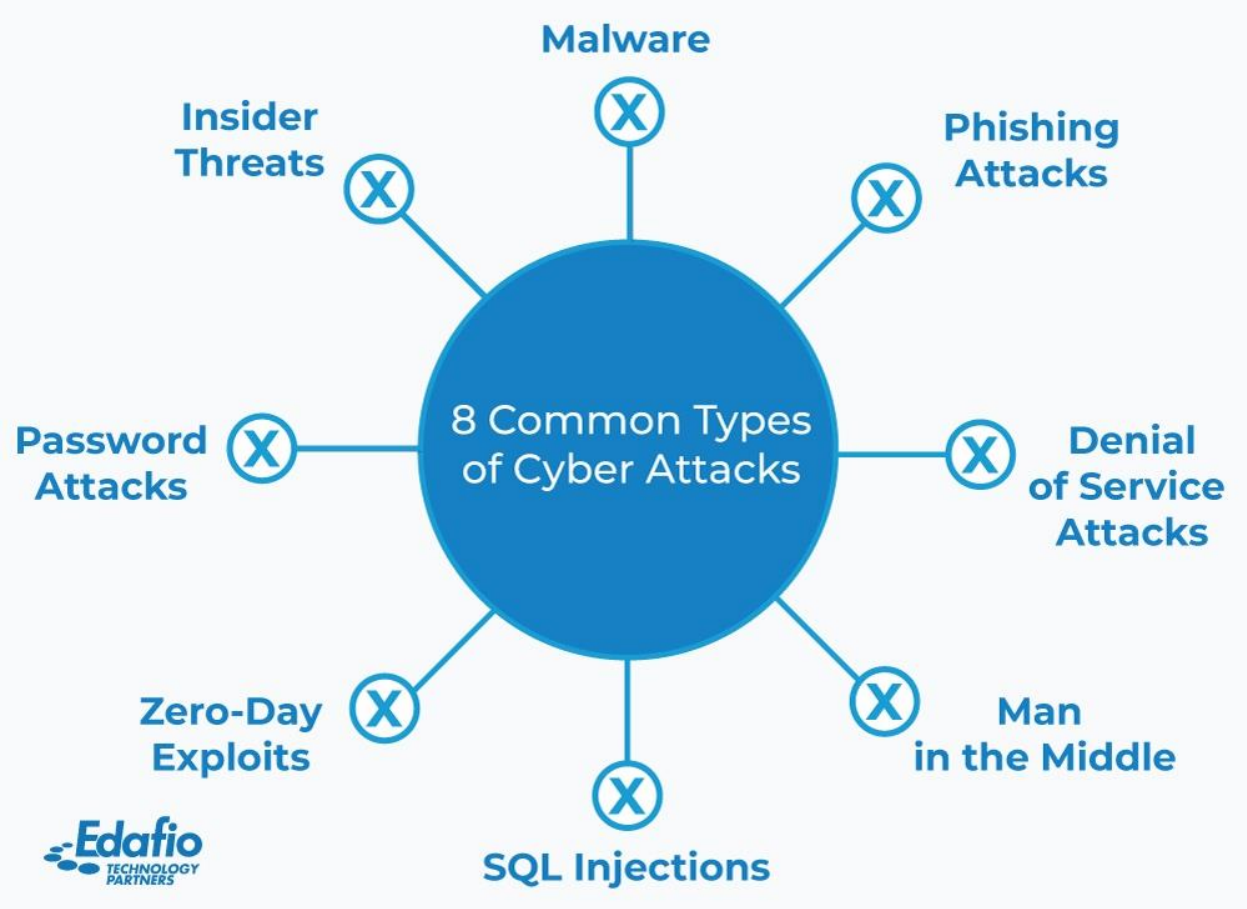
A Man-in-the-Middle (MitM) attack involves intercepting the communication between two endpoints, such as a user and an application. The attacker can eavesdrop on the communication, steal sensitive data, and impersonate each party participating in the communication.

Denial-of-Service Attack

A Denial-of-Service (DoS) attack overloads the target system with a large volume of traffic, hindering the ability of the system to function normally. An attack involving multiple devices is known as a distributed denial-of-service (DDoS) attack.

Denial-of-Service Attack

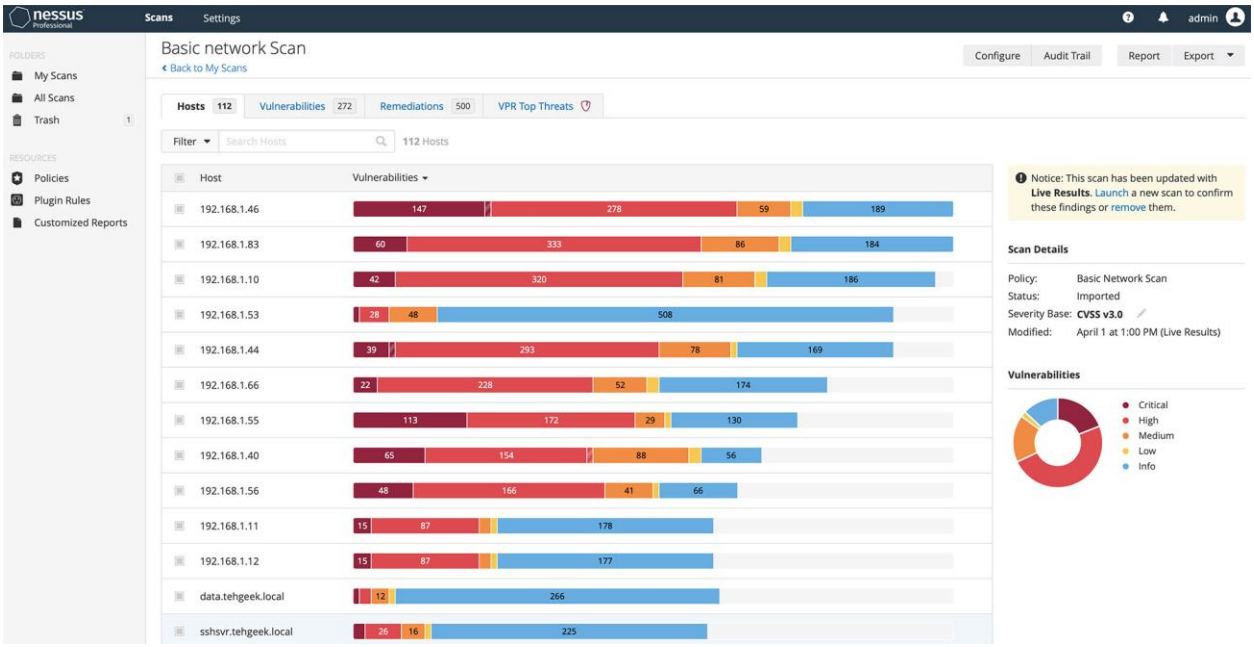
A Denial-of-Service (DoS) attack overloads the target system with a large volume of traffic, hindering the ability of the system to function normally. An attack involving multiple devices is known as a distributed denial-of-service (DDoS) attack.



There are several types of cybersecurity, each addressing specific threats and vulnerabilities Cybersecurity offers a myriad of opportunities for those interested in protecting the digital realm. If you're a job seeker looking to get started in the field, we are here to help! Our free employment programs offer hands-on work experience in various fields, online Cybersecurity offers a myriad of opportunities for those interested in protecting the digital realm. If you're a job seeker looking to get started in the field, we are here to help! Our free offer hands-on work experience in various fields, online and offline, in 17 countries around the world.

REPORT

IP ADRESS WITH VULNERABILITY CO RELATED WITH CYBER THREATES



Top features of Nessus

- The software is highly configurable and a good fit for more technical users
- Consistently detects the most recent CVEs while still keeping track of legacy vulnerabilities
- Pre-built policies and templates, customizable reporting, group “snooze” functionality, and real-time updates

open-source vulnerability scanning engine which is fast, extensible, and covers a wide range of weaknesses. It’s popular with bug bounty hunters, pen testers and researchers who want repeatable checks for serious weaknesses. These experts, working with Nuclei’s team at ProjectDiscovery, combine their knowledge and insights about cutting-edge weaknesses to produce checks extremely fast.

Nuclei is simple to get up and running without having to read a lot of documentation, but it’s most popular with bug bounty hunters, penetration testers and researchers who want to produce repeatable checks for serious weaknesses.

```
fuzzing:
  - part:
    query (default) - url query fuzz

  - fuzz:
    - {{variable to be replaced / fuzz}}

  - type:
    replace (default) - replaces the value of parameter with payload
    prefix - append the payload to existing parameter value
    postfix - prepend the payload to existing parameter value
    infix - place the payload in between the existing parameter value

  - mode:
    multiple (default) - multiple / all values to be replaced at once
    single - one parameter value to be replaced at a time

  - keys:
    list of parameter names to fuzz (exact match)

  - keys-regex:
    list of parameter regex to fuzz

  - values:
    list of value regex to fuzz
```

UNDERSTANDING THE NESSUS REPORT

A Nessus vulnerability scan report can be delivered in these formats:

- HTML (default)
- PDF
- CSV (used in spreadsheets, databases)

The HTML and PDF formats appear very similar, and can contain multiple chapters:

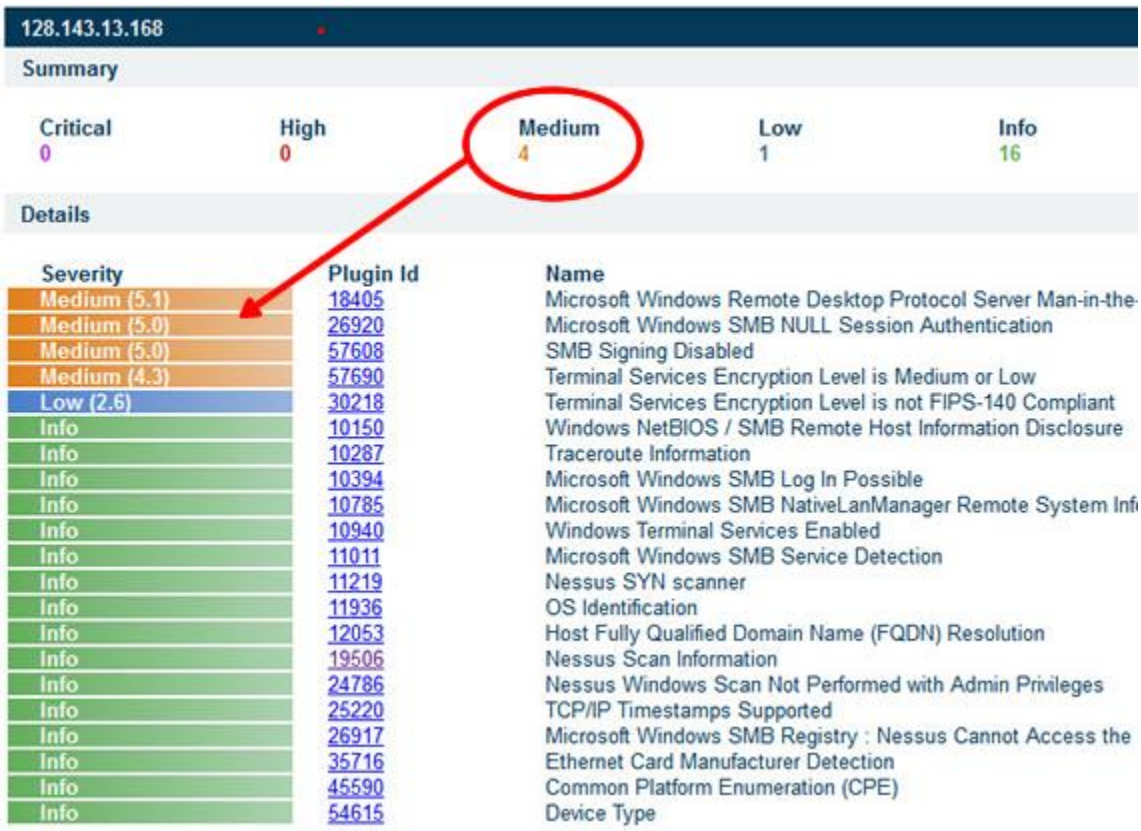
1. Hosts Summary
2. Vulnerabilities by Host
3. Vulnerabilities by Plugin

What's a Plugin?

A plugin is analogous to the virus definitions that are added and updated regularly to a virus protection program on a personal computer. They are different because they include what sort of output to expect when an active port on a server is given a certain input. The result will indicate whether there could be a weakness to hacking activities. The result does not indicate that hacking has taken place. A system administrator would need to investigate further to find evidence of an actual breach.

Host Summary

Click on an IP address listed under the Host Summary. The information shows the risk level associated with each scanner plugin. There is a legend at the beginning of the display for the color assignments. In the example, there were 4 medium-risk and 1 low-risk vulnerabilities found. In addition, 16 plugins reported information that would be of interest to a system administrator. Each plugin ID is a link that leads to a definition on the Tenable Nessus website.



128.143.13.168

Summary

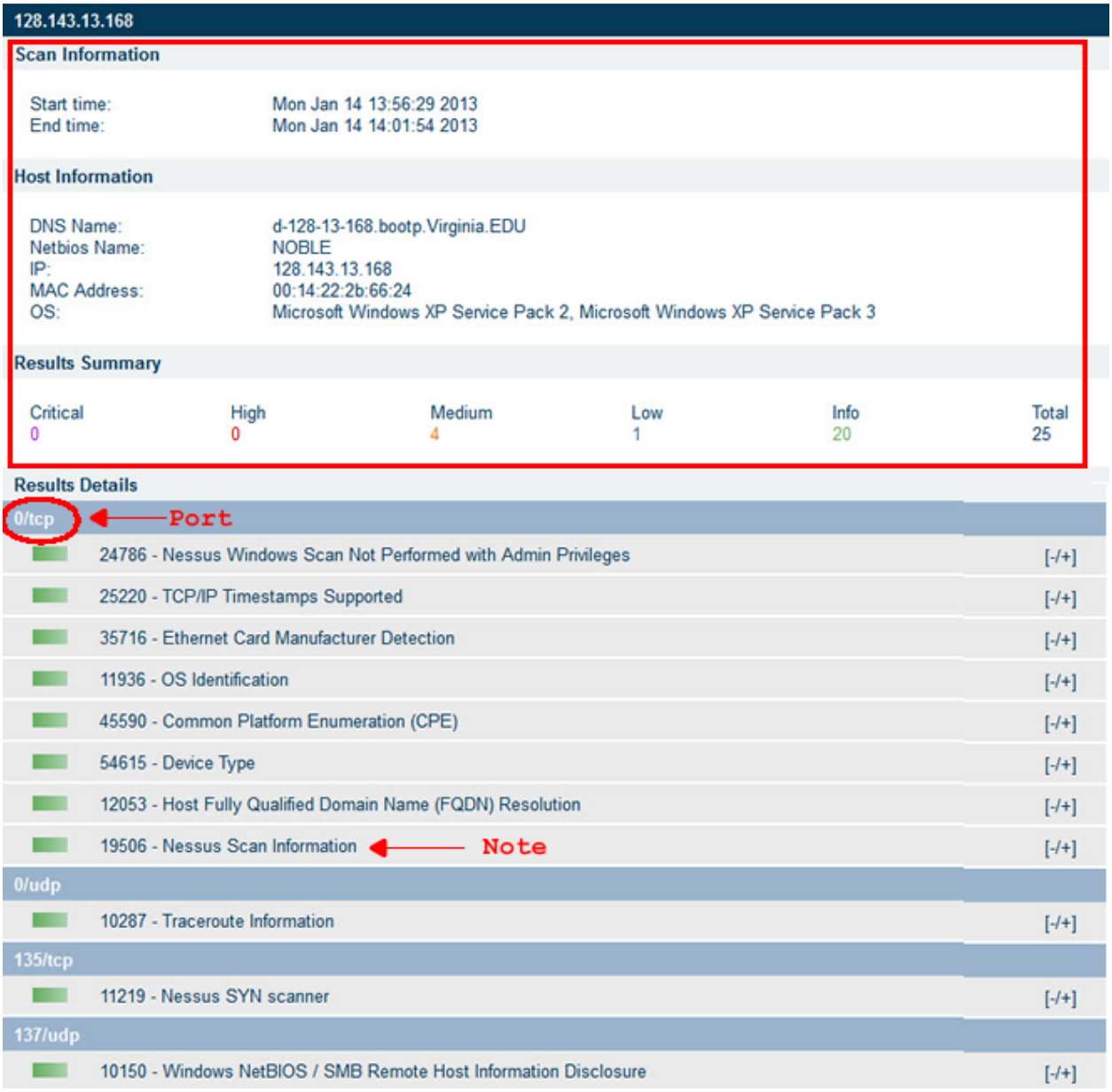
Critical	High	Medium	Low	Info
0	0	4	1	16

Details

Severity	Plugin Id	Name
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Inf
Info	10940	Windows Terminal Services Enabled
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

Vulnerabilities by Host

Click on an IP Address listed under Vulnerabilities By Host. The information about that host will displayed in two sections. The top section has information about that particular host, including the time the scan was performed on the specific host. The second section is a list of the plugins, organized by the port used for the scan activities. Activities not closely related to a specific port are listed under port 0/TCP.



PLANNING AND PREPARING

SCOPING AND SCANIND

In terms of cyber security, scanning is the methodical process of inspecting systems, applications, and networks to find any potential flaws, incorrect setups, or vulnerabilities. It entails using a variety of methods and tools to examine and probe the intended infrastructure in search of weaknesses that attackers might exploit. Companies can proactively identify and reduce security risks by carrying outscans, assuring the protection of their digital assets.

Types of Scanning

In cyber security, a variety of scanning techniques are employed. Let's look at a few of the most typical ones:

Port Scanning

Port scanning includes checking the status of each port on the system of interest to see if it is open, closed, or filtered. It assists in identifying the services and apps that are active on the intended system, potentially disclosing flaws or incorrect setups.

Vulnerability Scanning

The goal of vulnerability scanning is to find applications, systems, and network flaws. It compares the target infrastructure to a catalog of known vulnerabilities to identify places that need quick care.

Network Scanning

Network mapping and analysis are used in network scanning to locate hosts, devices, and other elements of a network. It gives a description of the network's architecture and aids in locating potential points of entry for attackers.

Web Application Scanning

Finding web application-specific vulnerabilities like SQL injection, cross-site scripting (XSS), or unsafe direct object references is the goal of web application scanning. Organizations may make certain their online interfaces are safe and devoid of vulnerabilities by scanning web apps.

Malware Scanning

Malware scanning is a key component of cybersecurity and is essential for identifying and reducing threats from malicious software. Viruses, worms, Trojan horses, ransomware,

spyware, and adware are just a few examples of dangerous software referred to as malware, sometimes known as malicious software. To detect and eliminate any possible threats and maintain the safety and soundness of your digital setting, it is crucial to run routine malware scans on your devices and systems.

Scanning Tools and Techniques

There are several scanning tools and methodologies available to carry out efficient scans and find vulnerabilities. Let's examine some well-known examples:

1. OpenVAS

An effective open-source vulnerability scanner called OpenVAS (Open Vulnerability Assessment System) aids businesses in locating and evaluating the weaknesses in their networks and systems. It is frequently employed in the cybersecurity sector and offers a complete set of scanning capabilities.

2. Nessus

A well-known commercial vulnerability detection tool called Nessus provides a number of functions to evaluate network and system vulnerabilities. To assist businesses in fixing vulnerabilities, it regularly refreshes its vulnerability list and gives thorough reports.

3. Nmap

The network scanning tool Nmap (Network Mapper) is flexible and reliable. On their networks, it enables businesses to find hosts, services, and open ports. Nmap provides a command-line interface with a wide range of parameters to personalize scans to meet particular needs.

STAGE-2

OVERVIEW: Vulnerability scanning

Vulnerability scanning is one of the initial steps of most penetration tests where a scope of multiple hosts is included as it is a fast way to check multiple hosts and to provide an initial list of vulnerabilities that can be further tested by the consultant. In order to perform vulnerability scanning, a vulnerability scanning tool is required. Luckily, there are many commercial and open-source scanners available for most platforms and a Google search will return many results. There is a list of available scanner on the SecTools.org website at http://sectools.org/tag/vuln-scanners/.

One free open-source scanner that can be used is OpenVAS that is available from http://www.openvas.org.

Vulnerability scanners are provided with a list of IP address or resolvable hostnames and they perform the process of scanning by first ascertaining the availability of the host before performing a service discovery via various port scanning techniques. Once the hosts and services are confirmed the scanner then moves onto performing an analysis of the hosts, looking for software vulnerabilities and configuration vulnerabilities. Most vulnerability scanners allow what is termed as a credential scans to be carried out. This is a vulnerability scan where the scanner can be given administrative rights so that it can map drives to the target hosts and also interrogate items such as the hosts registry in order to provide a much more detailed level of assessment.

A software vulnerability is an identified bug in an installed piece of software, either commercial or open source. One example of a software vulnerability may be the existing of the Conficker vulnerability that Microsoft announced in their security bulletin MS08-067. This is a well-known Windows Server vulnerability (that amazingly the authors still find in commercial networks) and Microsoft fixed it in a security patch. The vulnerability scanner knows how to identify this vulnerability from its plugin database and it will report it along with the corresponding risk details in the scanning management interface. A software vulnerability is an identified bug in an installed piece of software, either commercial or open source. One example of a software vulnerability may be the existing of the Conficker vulnerability that Microsoft announced in their security bulletin MS08-067.

A configuration vulnerability is related to the way a piece of software is configured, or more appropriately, misconfigured. Various software applications require configuration. It is hoped that software vendors today issue software with a default secure configuration but this has not always been the case with many historical providers releasing software that is insecure, relying on the user to secure it. This can be referred to an open or closed configuration. It is preferred to start with a closed configuration and open that parts needed. However, the easiest solution is to start with an open configuration and close the parts that are not needed but far too often these parts never get closed and this then leads to a configuration vulnerability which will always be exploited by a serious penetration tester or worse, a potential attacker. An example of a configuration vulnerability may be a network device, such as router or switch, with the insecure connection method of Telnet enabled rather than the secure method of SSH. This may also be further compounded if no password is required in order to gain access to the device. Both of these are configuration vulnerabilities that can be remedied through correct configuration of the device.

REMIDATION AND MIGRATION

PRIORITIZATION REMIDATION EFFORT

stablishing a risk-based prioritization framework

A risk-based prioritization framework allows organizations to focus their efforts on addressing the most critical vulnerabilities first. Here are key steps to establish an effective risk-based prioritization process:

Categorize and classify vulnerabilities:

Group vulnerabilities based on their nature (e.g., software, configuration, human factors).

Classify vulnerabilities by severity, taking into account the Common Vulnerability Scoring System (CVSS) or other relevant metrics.

Understand Exploitation Potential:

Assess the ease with which a vulnerability could be exploited.

Consider factors such as the presence of known exploits, the level of skill required, and the existence of active threats targeting the vulnerability.

Evaluate business impact:

Determine the potential impact on business operations and data.

Consider the criticality of affected systems, the sensitivity of data, and the potential regulatory implications.

Prioritize based on risk score:

Combine the severity, exploitation potential, and business impact scores to create an overall risk score for each vulnerability.

Prioritize vulnerabilities with the highest risk scores for immediate remediation.

Implementing a remediation plan

Once vulnerabilities are prioritized based on their risk scores, organizations can create a remediation plan to systematically address each flaw. Here are key strategies for effective remediation:

Patch management:

Prioritize the deployment of patches for software vulnerabilities.

Implement an efficient patch management process to ensure timely updates and minimize the window of exposure.

Configuration management:

Address configuration-related vulnerabilities by reviewing and adjusting system configurations.

Implement secure configuration practices to reduce the attack surface.

INLEMENTING THE SECURITY CONTROL

security controls are preventive, detective, defensive, and corrective measures or guardrails that protect the information systems, networks, and data assets within an organization from security risks or threats.

The cloud is like a bank. One keeps their money in a bank for security and accessibility. Robbers often target banks, because that's the repository.

Attacks against the cloud impact multiple businesses objectives. Here are some reasons why a strong posture is essential.

TESTING AND VALIDATION

Security testing and validation are the processes of verifying that your applications and systems meet the security requirements, standards, and policies that apply to them. Security testing and validation can cover different aspects of security, such as authentication, authorization, encryption, input validation, output sanitization, error handling, logging, auditing, and more. Security testing and validation can be performed at different stages of the development and deployment lifecycle, such as design, coding, testing, deployment, and maintenance.

Security testing and validation are the processes of verifying that your applications and systems meet the security requirements, standards, and policies that apply to them.

Security Validation provides you with visibility and performance data to report on your organization's security posture and overall competency. This approach allows you to prioritize your risk optimization strategy based on the knowledge of which threats matter most to your organization.

REPORT

TARGETED WEBSITE: https://www.youtube.com/

IP ADDEASS: 143.250.191.78

LIST OF THE VULNERABILITIES:

S.NO	VULNERABILITY NAME	SEVERITY	PLUGINS
1	HTTP SERVER TYPE AND VERSION	NONE	ID-43111
2	HYPER TEXT TRANSFER PROTOCOL INFORMATION	NONE	ID-10386

3	HTTP METHOD ALLOWED	NONE	ID-43111
4	HTTP REDIRECT INFORMATION	NONE	ID-91634

VURNABILITY NAME: HTTP SERVER TYPE AND VERSION

SERVESE: NONE

PLUGINE: ID-43111

DESCRIPTION: Exposing the version and type of the HTTP Server can be exploited by malicious users to identify if there are any security vulnerabilities known for that type of HTTP Server.

VULRNABILITY NAME: HYPER TEXT TRANSFER PROTOCOL INFORMATION

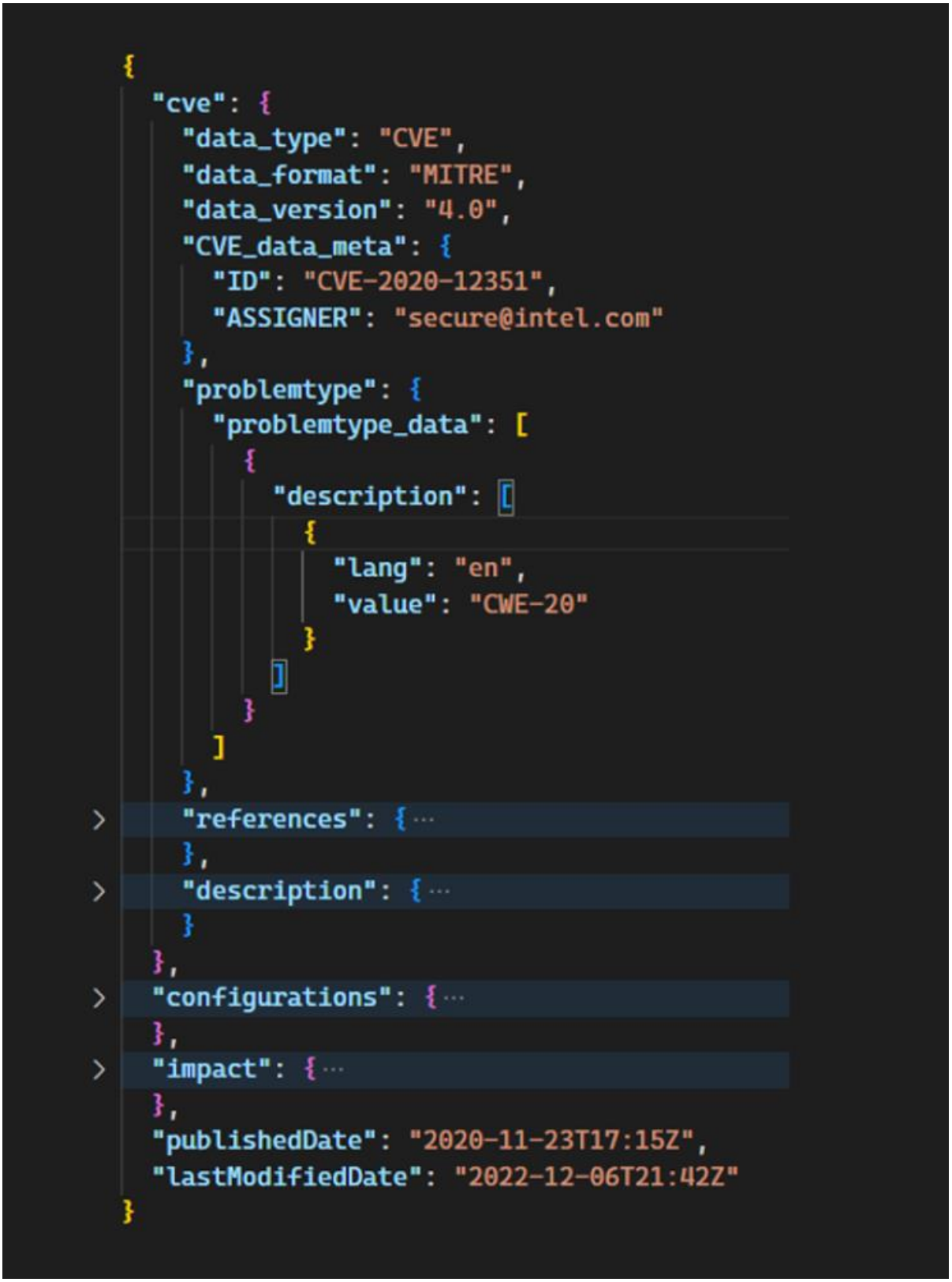
SERVER : NONE

PLUGIN: ID-43111

DESCRIPTION:

- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.

client and server exist only during the current request and response time only.



- **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

VULRNABILITY NAME : HTTP METHOD ALLOWED

SERVER: NONE

PLUGIN: ID-43111

DESCRIPTION:

_ HTTP defines a set of request methods to indicate the desired action to be performed for a given resource. Although they can also be nouns, these request methods are sometimes referred to as HTTP verbs.


```
"references": {
  "reference_data": [
    {
      "url": "https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00435.html?wapkw=CVE-2020-12351",
      "name": "https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00435.html?wapkw=CVE-2020-12351",
      "refsource": "MISC",
      "tags": [
        "Third Party Advisory"
      ]
    },
    {
      "url": "http://packetstormsecurity.com/files/162131/Linux-Kernel-5.4-BleedingTooth-Remote-Code-Execution.html",
      "name": "http://packetstormsecurity.com/files/162131/Linux-Kernel-5.4-BleedingTooth-Remote-Code-Execution.html",
      "refsource": "MISC",
      "tags": [
        "Exploit",
        "Third Party Advisory",
        "VDB Entry"
      ]
    }
  ]
},
```


STAGE-3

INTEGRATION AND AUTOMATION

AUTOMATING SCANNING WORFLOW

What is Automation?

Automation is defined as making equipment, processes or systems operate automatically with minimal human input. It can take simple tasks and automate them, using tools to streamline and speed up the process.

Everyday examples of automation solutions:
Phone apps enable users to streamline many processes such as shopping lists, online shopping, banking, ordering food, and paying in-store. These applications are often shared with another user.

Voice/virtual assistants such as Amazon Alexa or Siri. These devices enable users to speak directly to their devices. They can add items to their shopping list, ask a question, and play music all synced to the user's phone.

Other examples in your home include your washing machine, dishwasher and fridge.

What is Integrated Automation?

Integrated automation can be defined as software workflows that operate independently and constantly with minimal human input after parameters have been set.

An integrated automation Platform or an IAP is a technology infrastructure that enables systems to integrate with one another. Software or machines copy human tasks and repeat these actions. Integrated Automation Platforms will provide API orchestration tools allowing different parts of the infrastructure to coordinate the distribution and processing of data. For example, Cyclr is an embedded integration platform with a library of **API connectors** that can be used to create integrated automation.

An example would be using Pipedrive, your customer relationship management API to extract your customers. The Eventbrite API retrieves the attendees for an event you are hosting. Followed by the action of true or false. This then prompts Mailchimp to either add the contact to the attendee list or the non-attendee list. Thus allowing data to be shared and coordinated between the APIs. Rather than manually extracting the data from Pipedrive and entering the data into Eventbrite and MailChimp.

LEVERAGING THREATS INTELLIGENCE:

In the ever evolving digital world, threat actors are constantly trying to outmanoeuvre the latest cybersecurity measures. Therefore, data on a malicious actor's next move is key to tailoring your organisation's defences and preventing future attacks.

Cyber threat intelligence shines a light on the unknown, allowing cybersecurity teams to make more informed decisions.

Cyber threat intelligence empowers cybersecurity stakeholders by revealing threat actor's tactics, motives, techniques, and procedures.

Cyber threat intelligence helps cybersecurity professionals understand the malicious actor's decision-making process.

Cyber threat intelligence informs business stakeholders, such as boards, CIOs, CISOs, and CTOs; to make better decisions and invest wisely.

1. Continuous Monitoring for Threat Detection

Continuous monitoring is key in threat detection. Continuously monitoring IT networks and systems allows cybersecurity teams to detect security threats, non-compliance problems, or performance issues in an automated manner. The aim is to identify potential threats and/or issues in real-time to address them quickly.

RiskXchange is the only platform that provides a complete 360-degree view of your attack surface, including that of your vendors. It will continuously monitor your complete attack surface, highlight any risk, and enable you to fix any issues before the attacker discovers them.

2. Vulnerability Scanning and Assessment

Vulnerability scanning and assessment is the process of pinpointing, analysing, and reporting on vulnerabilities and security flaws. Vulnerability scans are conducted using automated vulnerability scanning tools to identify

potential attack vectors and risk exposures across an organisation's software, hardware, networks, and systems.

3. Incident Response Planning and Execution

Incident response planning contains specific directions for different attack scenarios, reducing recovery time, avoiding further damages, and mitigating cybersecurity risk. Incident response procedures focus on being prepared for cybersecurity breaches and how a business will recover from them.

4. Proactive Threat Hunting

Proactive threat hunting is the process of proactively searching for threats that are lurking undetected in a network or system. Threat hunting is a deep dive into a network to locate threat actors in an organisation's ecosystem that have managed to get past initial endpoint security defences.

5. Intelligence Sharing and Collaboration

Intelligence sharing and collaboration allows an organisation to access and share real-time threat information and cyber threat intelligence without revealing sensitive details about their own systems or networks. This allows businesses to share information and collaborate without compromising their own cybersecurity.

6. Threat Intelligence Feed Integration

A threat intelligence feed can be an important step in bolstering cybersecurity measures within any organisation. A threat intelligence feed provides a constant stream of data about potential attacks, aka threat intelligence, from an external source. Organisations can use threat intelligence feeds to ensure their cybersecurity defences are updated and ready for the latest attacks.

7. Cyber Threat Intelligence Training and Education

Cyber threat intelligence training and education is key to winning the war against hackers in today's digital age. Training and education are fundamentally important to not only ensuring that cybersecurity

professionals are up to date with the latest advancements, but their analytical skills are sharpened.

8. Contextualizing Intelligence for Effective Decision-Making

Contextualizing intelligence for effective decision-making is key. Understanding how best to incorporate the insights received is the most important part of building up defences. Cyber intelligence is a mixture of defence and physical espionage with modern information technology. With such complexities, effective decision-making can be blinded unless expert operational teams or external cybersecurity firms are brought in to help bolster cybersecurity measures. Cyber threat intelligence management is key in today's complex cybersecurity landscape.

9. Automating Cyber Threat Intelligence Processes

Automating cyber threat intelligence processes allows for the detection and response to threats in real-time. Automating the process helps cybersecurity operations teams react to alerts quickly and more efficiently. The impact of AI on cybersecurity management has already had a profound effect and as the technology advances, malicious actors are finding that they just can't match the pace of artificial intelligence and machine learning.

SCALABILITY AND FLEXIBILITY:

Scalability refers to an organisation's ability to handle increased demands or workload without compromising performance or efficiency. It is a critical aspect of business strategy as it directly impacts the company's growth potential. A scalable business model allows a company to expand and increase its output in response to rising demand. This could mean adding new employees, expanding physical locations, or investing in technology to automate processes. Without scalability, a business may struggle to meet increased demand, leading to customer dissatisfaction and potential loss of market share.

Flexibility, on the other hand, is the capacity of an organisation to adapt to changes in the business environment. This could be changes in market trends, customer preferences, regulatory requirements, or technological advancements. A flexible organisation can quickly pivot its strategies, processes, or products to respond to these changes. This adaptability is crucial in today's fast-paced and unpredictable business environment. Without flexibility, a business may become obsolete or irrelevant as it fails to keep up with the changing needs and expectations of its customers or the evolving market dynamics.

Scalability and flexibility are extremely important considerations for technology solutions, especially for growing organizations. Here are some reasons why:

• Growth - As your organization grows, you will likely need to scale your technology use, data storage, system throughput, and user base. Solutions that cannot scale cost-effectively as needed will quickly become inadequate.

• Changing Needs - Organizational needs and priorities are always evolving. Flexible technologies can adapt and reconfigure to meet new or unforeseen requirements. Inflexible solutions may become obsolete quickly.

• Future-Proofing - Investing in scalable and flexible technologies helps "future-proof" your investment by ensuring solutions can meet your long-term needs, not just current requirements. This extends the useful life of the technology.

• Cost Savings - Scaling technologies easily and flexibly helps avoid expensive "forklift upgrades" where you have to completely replace a system. Incremental upgrades are more cost-effective.

BEST PRACTICE AND FUTURE TRENDS:

BEST PRACTICE IN VULNERABILITYES MANAGEMENTS:

Vulnerability management is a key component of enterprise cybersecurity architecture. It focuses on identifying, managing, and remediating various vulnerabilities in IT environments. Some of these **security vulnerabilities** include misconfigured cloud applications and unpatched software.

These vulnerabilities pose serious security risks, because exposed, overprivileged, and penetrable IT assets can increase the likelihood of attacks from cybercriminals. If you don't address them, you're leaving the door wide open. Employing a robust vulnerability management process is one way to rectify the situation.

A typical vulnerability management process features a five-step lifecycle: discover, prioritize, remediate, validate, and report. Vulnerability management can strengthen your overall security posture, prevent data breaches and leaks, enhance operational efficiency, empower developers and other teams, and improve compliance for cloud-based businesses of all scales and backgrounds.The program should encompass every stage of a vulnerability management lifecycle. This includes:

- the identification of vulnerabilities across clouds and workloads
- prioritization based on business context and scoring systems
- remediation
- program optimization with insights from reports
- bound by business-specific KPIs

EMERGING TRENDES IN VULNERABILITY MANAGEMEBT:

In 2024, vulnerability management will continue to evolve, even in a dynamic threat landscape. Several vital trends shape how businesses approach and prioritize vulnerability management to safeguard their digital assets.

Collaborative Threat Intelligence Sharing

It’s becoming increasingly common for organizations to share information about potential cyber-attacks with each other so they can better prepare and protect themselves. They can strengthen their defences against these threats by working together to share this information.

By 2024, this collaborative effort will become even more widespread, resulting in a safer digital environment for everyone.

Mobile Security Emphasis

Mobile security is gaining importance as firms rely more on mobile devices. To address this concern, firms are taking steps to secure mobile applications, devices, and networks, considering the unique challenges and threats in the mobile ecosystem.

It will have more advancement in 2024.

Embracing Risk-Based Prioritization

Until recently, when it came to cyber security, most organizations tried to fix every vulnerability they found as quickly as possible. However, this approach could have been more practical and effective.

In the future, in 2024, the focus will be on identifying and prioritizing the security threats that pose significant risk to the organization. This means looking at things like how likely a particular threat is to occur, how severe the consequences could be, and how much effort it would take to fix it.

To figure all this out, organizations will need to use advanced tools to help them accurately assess the risks and threats they face.

Also Read: AI-Driven Solutions for Proactive Vulnerability Management

AI and ML Take the Lead

Automating the process of vulnerability management is crucial in today’s digital world. Technology like Artificial Intelligence (AI) and Machine Learning (ML) are helping us tackle this challenge. AI-powered tools can examine large

amounts of data on vulnerabilities and threats and take over time-consuming tasks like scanning and patching.

They can also predict potential future vulnerabilities. It can help prevent problems before they even happen. Additionally, ML algorithms can help prioritize vulnerabilities so that the most important ones are addressed first, making the process even more efficient.

Continuous Vulnerability Assessment

In the past, computer security experts would check for weaknesses in software by running scans at set times. But now, tech has advanced to the point where firms can monitor systems and software in real time, catching problems as soon as they appear.

This is called continuous vulnerability assessment (CVA), and it's becoming more and more common. By constantly monitoring our computer systems, we can quickly find and fix any issues before hackers can exploit them.

This is especially important because new software weaknesses are constantly discovered, so we need to stay vigilant to keep our systems secure.

DevOps and Security Synergy

The gap between software developers and people who ensure it's safe and secure is getting smaller. By 2024, we'll see more tools that help both groups work together better.

These tools will help find and fix problems with the software early on before it goes out to everyone who uses it. People will need tools that can automatically fix problems and check how secure the software is.

Regulatory Landscape Tightens

Regulatory bodies and governments and are becoming increasingly concerned about the safety of our online data. As a result, they are creating

stringent rules and requirements for companies to follow when protecting our sensitive data.

Businesses that don't take these rules seriously can face legal consequences and harm their reputation. In 2024, it will be essential for companies to understand and comply with these regulations to keep our data safe

Human Factors Remains Crucial

While technology is essential to protect against cyber threats, it's crucial to remember that people play a vital role in keeping digital systems safe. Educating employees about cybersecurity and how to protect themselves and the company best is necessary.

Creating a culture of security awareness and regularly training staff can help prevent cyber attackers from exploiting vulnerabilities through tactics such as social engineering. We can all help keep our systems and sensitive data safe by working together.

CONCLUSION AND RECOMMENDATION:

Conclusions and recommendations

The interpretations given by the researcher of the significance of the findings of a research project for the client's business, along with recommendations for action. These recommendations will be based on the research and on any other relevant information available to the researcher, including their own past experience in a market or in business.

Conclusions and recommendations usually form an important part of a project debrief and of any report or documentation, and are a key part of the value offered to clients by professional market research.

Related Terms

Debrief

Report

CONCLUCTION

Today’s cyber threat landscape is constantly evolving. Modern organizations face a growing number of cyber threats that are increasingly complex. There’s no one-size-fits-all formula for deciphering exactly what a cyber threat may be for your organization compared to another. However, understanding your cyber threat landscape, as well as how to prioritize cyber threats for remediation, is a great first step in developing a cybersecurity program. As you understand more about the cyber threats your organization faces and the potential impact on your most critical operations, the more prepared you will be to adapt your cyber hygiene practices and mature your cybersecurity measures over time.

ere are many types of cyber threats, and they’re constantly changing and evolving, especially as organizations adopt and implement new technologies, like cloud services.

While not all-encompassing, here are a few examples of common cyber threats:

Exploitation of misconfigurations and unpatched systems

Phishing: Sending fake emails that look like they're from real sources to trick people into revealing information like usernames, passwords and payment info.

Credential stealing: Because people often use the same usernames and passwords across many sites, attackers can collect usernames and passwords from one breach and then use them to access other sites.

Malware: Malicious software that gives attackers system access.

Denial of Service (DoS) and Distributed Denial of Service (DDoS): Flooding attacks that use up bandwidth so systems can't respond to actual service requests.

Cross-Site Scripting (XSS): Putting malicious code on websites to target visitors.

Man-in-the-Middle (MitM) attacks: Compromising users through unsecure networks like public Wi-Fi.

SQL Structured Query Language (SQL) Injection: Putting malicious code on a server and then using SQL to access sensitive information that otherwise wouldn't be accessible.

Zero day exploits: Exploiting a system after a threat is publicly announced but before a patch or other fix is released.

Spam: Attackers send unwanted and unsolicited messages, usually in great volume, to lure a user into clicking a malicious link, downloading a malicious file, or giving up sensitive information, such as credentials.

Cloud vulnerabilities: A cloud security vulnerability is a weakness within a cloud computing environment, for example an insecure API, poor access management, or system misconfigurations.

Misconfigured code: A growing number of hackers are successfully finding security weaknesses within code where a misconfiguration early on is missed during code development and testing, opening the door to exploit that weakness.

Insider threats: While many insider threats take the form of a disgruntled employee or employee who has been lured (for example, by financial incentives) to commit actions that can harm an organization, unintentional actions by employees or connected partners may also introduce insider risks.

Malicious links: These links are generally part of emails or websites where a would-be attacker has intentionally created a link that leads to things such as viruses or malware to enable them to access devices or convince a user to provide credentials.

Lost or stolen assets: Lost or stolen assets, especially those not protected with passwords and/or encrypted are cyber threats. This isn't just a lost

FUTURE SCOPE

The future of cybersecurity: Trends, threats, and more

Speculating on the future of cybersecurity is inherently challenging. From new attacks and techniques to technology and defenses, it's always changing.

Still, our cybersecurity analysts have provided their best insights on what the future may hold, looking at this calendar year and beyond.

More attention on prevention and preparedness

In the next five to ten years, prevention and preparedness will be more vital than ever.

If 2023 taught the cybersecurity industry anything, it's that proactively planning for a cybersecurity incident or data breach is critical.

We expect to see a greater emphasis on incident preparedness and response playbooks, not to mention greater investment in employee education and training at all levels.

Continued development of regulations

What's more, evolving privacy and security concerns are expected to become far more urgent as laws come into full force.

Beyond the European Union General Data Privacy Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and the California Consumer Privacy Act (CCPA), additional state- or region-level regulations are being introduced at a rapid pace.

Plus, the greater scrutiny of cybersecurity controls could lead to further impacts for in-scope companies and organizations.

Companies that work with personally identifiable information should prioritize compliance moving forward. Ensuring cybersecurity programs comply with existing or forthcoming regulations and align with accepted frameworks is and will continue to be a top-of-mind concern.

Cyber insurance will drive demand for cybersecurity assessments

The cyber insurance market has faced many challenges, most notably the difficulty of assessing and pricing cyber risk due to the lack of historical data, the dynamic and evolving nature of cyber threats, and the potential for systemic and catastrophic losses.

To ease this burden, we expect cyber insurance providers to require or incentivize their clients to undergo cybersecurity assessments as part of the underwriting process or the policy conditions. This could help the insurers to evaluate the risk profile and premium of the clients, as well as to provide recommendations and guidance for improving their cybersecurity.

These assessments can demonstrate a client's compliance with the cyber insurance policy requirements or lower their premiums by showing their security maturity and use of best practices.

Cloud-based services: A growing target

Companies are using more cloud services than ever before. This is a mix of moving some traditionally on-premises services like email and file sharing/storage to the cloud and the rise of popular cloud-only collaboration and customer relationship management platforms.

These services are generally set up for the optimal balance between security and productivity. While more secure settings are possible, they often require extra steps that few organizations have the time or technical know-how to take.

This is part of a greater issue regarding the shared responsibility model used by cloud service providers. In this model, both provider and user are partially responsible for the management and cybersecurity considerations of the service, the extent of which is dependent on the service type.

However, organizations using these services may not fully understand where their responsibilities start and stop, leaving a gap in implementing security measures that make the organization more vulnerable than necessary.

REFEREENCES

https://www.tenable.com/principles/cyber-threats-principles

https://cybersecurityvalidation.com/what-is-security-validation/

https://www.tenable.com/products/nessus

https://www.spiceworks.com/it-security/data-security/articles/what-is-nessus-scanne/

https://www.google.com/search?q=understanding+the+cyber+threats%3Aexploring+the+nessus+and+beyond+scanning+tools+future+scope&oq=&gs_lcrp=EgZjaHJvbWUqCQgAECMYJxjqAjIJCAAQIxgnGOoCMgkIARAjGCcY6gIyCQgCECMYJxjqAjIJCAMQIxgnGOoCMgkIBBAjGCcY6gIyCQgFECMYJxjqAjIJCAYQIxgnGOoCMgkIBxAjGCcY6gLSAQkxNDI4ajBqMTWoAgiwAgE&sourceid=chrome&ie=UTF-8