

CompTIA Security+

Lecture 01

SY0-701

Fundamentals and Basic Concepts of Security

By
Dr. Khaled ELMenshawy

Lecture

01

LEARNING OUTCOMES

- Understanding CIA triad.
- Understanding Important security terminologies such as assets, vulnerability, and threat .
- Recognize different types of Threat Actors.
- Understanding Open-source intelligence (OSINT).
- Understanding the concept of dark web.
- Understanding Threat intelligence Sharing.
- Understanding Threat Vectors.
- Recognize Security Controls.

Why we need Security?

Confidentiality:

The secured information is accessible only to authorized users and prevents the disclosure of information to unauthorized parties. *Revealing the data only to authorized users.*

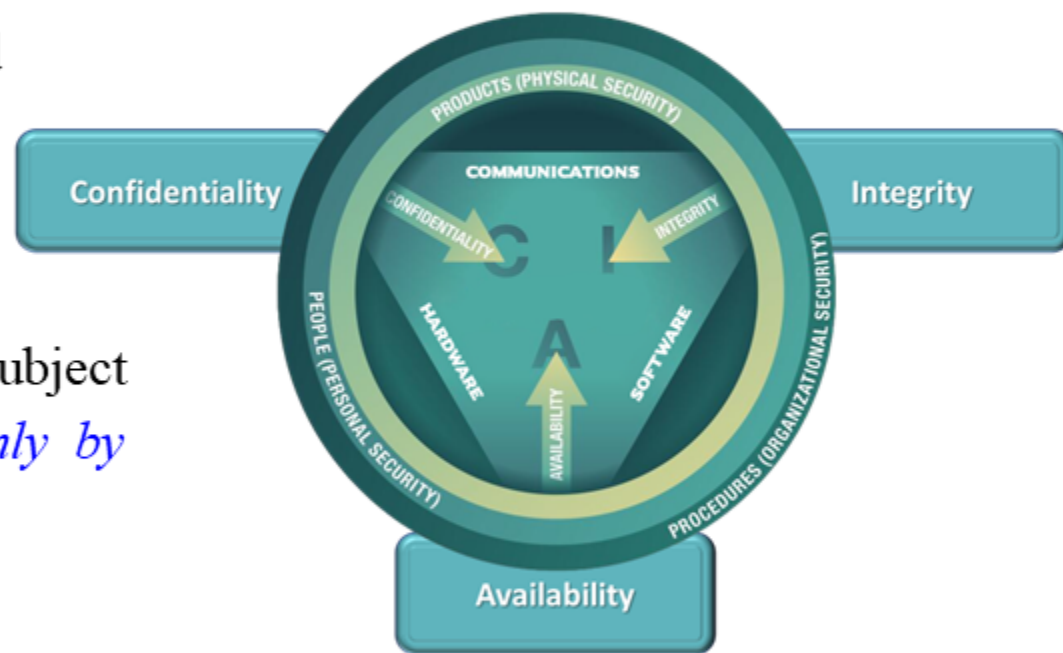
Integrity:

Information must be remained accurate, consistent, and not subject to unauthorized modification. *changes need to be done only by authorized users and through authorized mechanisms.*

Availability:

Information is always available for authorized users. *The computer system remains work without degradation of access, provide resources to authorized users when they need it.*

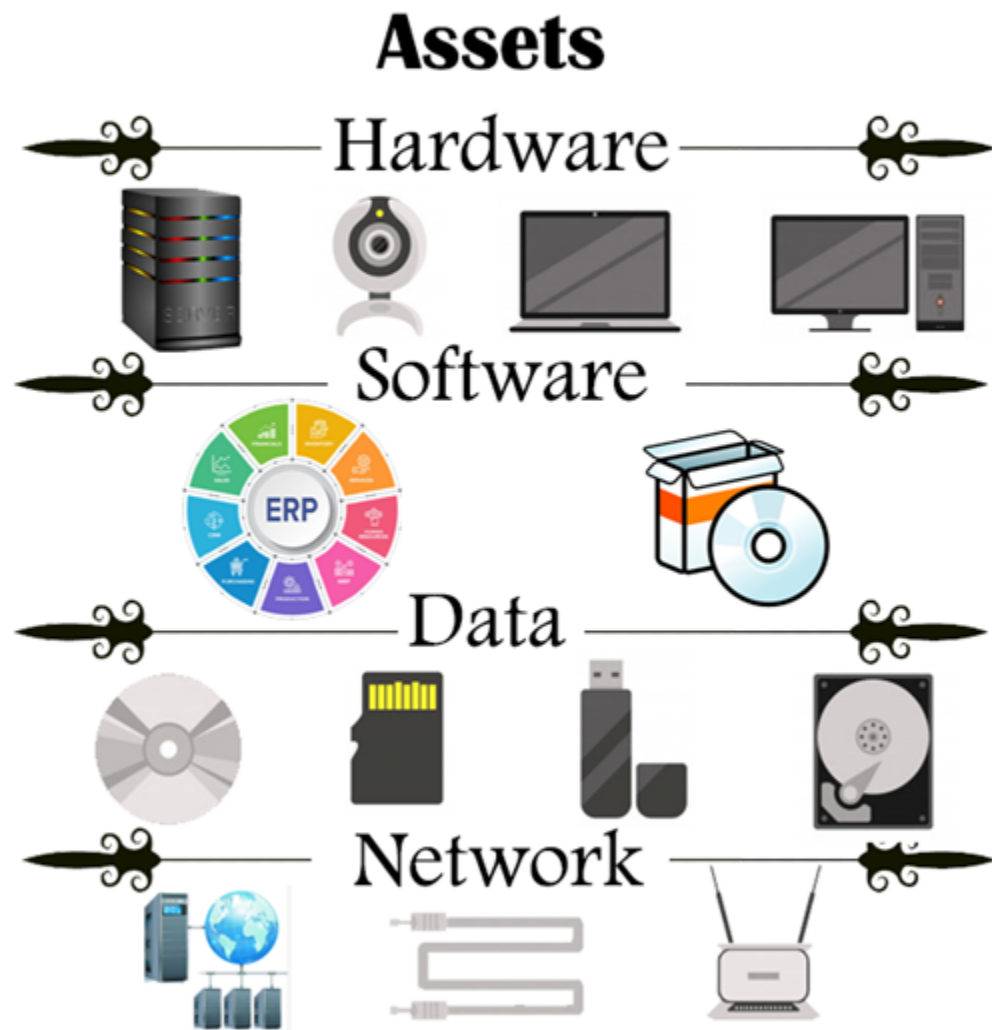
The backbone principles of cybersecurity



What is Assets?

Assets are *any part of our infrastructure* that we are worried about getting harmed such as:

- Hardware.
- Software.
- Data.
- Communication and Network



Assets is more than just IT devices and equipment

The meaning of *assets is gone behind IT devices and equipment*, they can be extended to cover other things such as:

- Human resources like the key developers or administrators.
- Doors of important rooms like data centers or servers' room.
- Intangibles like the reputation of the company.

Assets	Confidentiality	Integrity	Availability
Hardware	-	-	Equipment or device is stolen or disabled, thus denying service.
Software	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task	Programs are deleted, denying access to users.
Data	An unauthorized read of data is performed.	Existing files are modified, or new files are fabricated.	Files are deleted, denying access to users.
Communication and Network	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.	Messages are destroyed or deleted. Communication lines or networks are unreachable.

What is Vulnerability?

A weakness in an asset that leave it exploited to violation such as:

- Not changing the default username and password of a router or using weak password.
- Not testing an application for bugs and error.
- Not locking the doors of important IT rooms.

What is Threat?

A potential for violation of security by something that could cause harm to a system or organization.

Threat is always related to vulnerability, because if the vulnerability exists that is mean there is a threat of using such vulnerability to harm the system or stealing important information. Now we can rephrase the definition of vulnerability to:

A vulnerability is a weakness inherent in an asset that leaves it open to a threat.

What is Threat Actor (Agent)?

A threat actor is anyone or anything that has the motive and resources to attack another enterprise's IT infrastructure. There are nine specific types of threat actor:

Internal Threat Actors

- Insiders
- Shadow IT

External Threat Actors

- Hackers
- Hacktivists
- Script kiddies
- Competitors
- Criminal syndicates
- State actors
- Advanced persistent threat

How to measure the capabilities of Threat Actor ?

Internal**External****Funding**

Someone who's on a budget, or a government sized budget that they can actually use for attacking?

Resources

How many different people/tools can they allocate for attacking?

Sophistication

Having a strategic, design thinking-led process, deep understanding of the technology and familiar of new technologies, frameworks and tools.

Capability

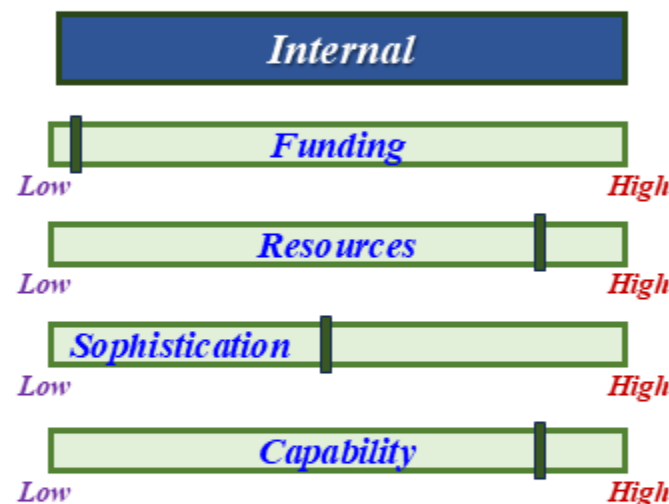
Capability of harming the system.

Threat ActorsWhat is Insider?

Insiders (or insider threats) are people within an organization have substantial physical access and usually have user accounts that give them access to assets. Insiders are often *motivated by revenge or greed*.

What is Shadow IT ?

Shadow IT describes information technology systems installed without the knowledge or consent of the main IT department. The main purpose of Shadow IT is *working around limitations* imposed by IT departments for purposes of security.



Threat ActorsWhat is Hacker?

A threat actor that have the technical skills to gain access to computer system. There are three types of hackers:

- **Black hacker**; Unauthorized person, aim to harm the system.
- **White hacker**; Authorized person who use their skills for good, checking for vulnerabilities and working to eliminate them.
- **Gray hacker**; Semi-authorized person, rarely malicious, but usually do not have the target's consent.

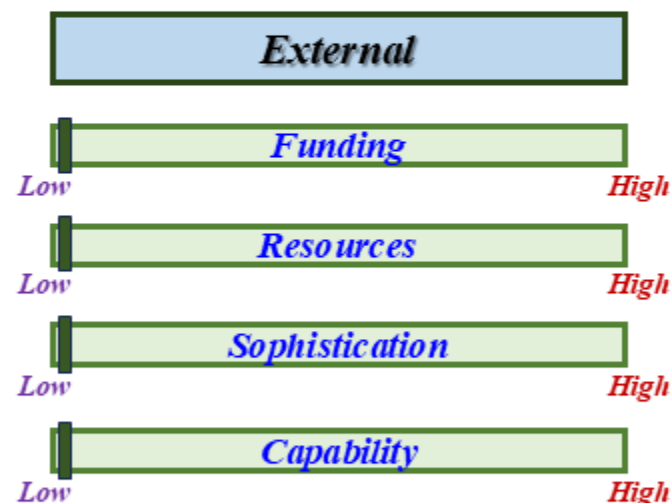
Threat Actors

- **Green hacker**; Beginner hackers seek to learn and improve their skills.
- **Yellow hacker**; Focus on ethical hacking related to social engineering and phishing.
- **Red hacker**; Work as penetration testers to find vulnerabilities before attackers exploit them (Offensive security).
- **Blue hacker**; Monitor, detect, and respond to threats in real time, focus on protecting systems and responding to attacks (Defensive security) .
- **Purple hacker**; Combine offensive (red team) and defensive (blue team) efforts.

Threat ActorsWhat is Hacktivist?

A hacktivist is a hacker and an activist. The activist is an expression for the people who They adopt a specific cause, whether it is political, economical, or a general cause such as:

- Activist who is against online exams of secondary education, may act against exam system.
- Activist who is against Whales fishing, may act against fishing industry.

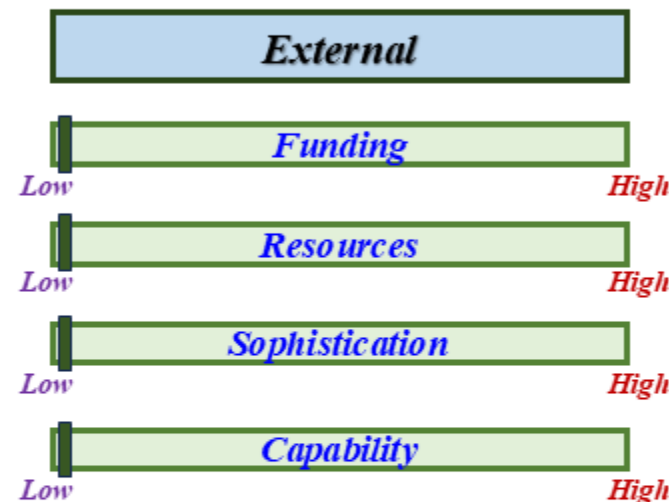


Threat ActorsWhat is Script kiddies?

Script kiddies are *poorly skilled threat actors* who take advantage of relatively easy-to-use open-source attacking tools. Their lack of sophistication makes them *easy to stop*, most of the time.

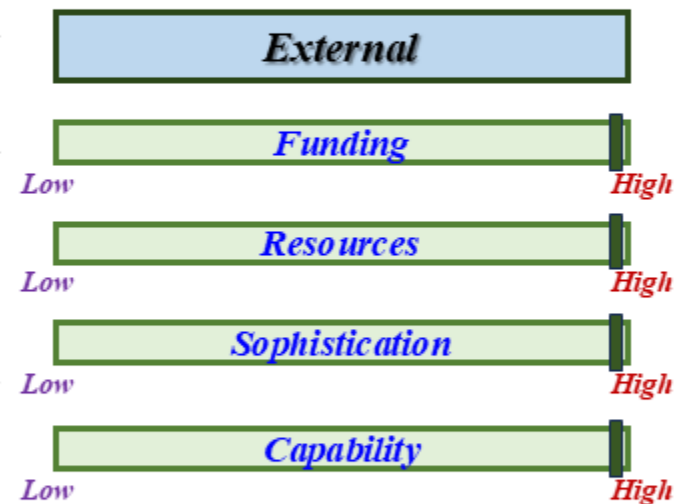
What is Competitors?

Competitors are outside organizations *in the same business* that try to gain access to well defined type of secure information they want.



Threat ActorsWhat is Advanced persistent threat (APT)?

APT is a form of threat used by **State Actor** to get into a system and stay there. APT attacks are initiated to steal data rather than cause damage to the target network and maintain ongoing access to required information. APTs typically take the following sequential approach to gain and maintain ongoing access to a target:



1. Gain access
2. Establish a foothold
3. Gain even greater access
4. Move laterally
5. Take the data
6. Remain until they're detected

Threat Actors

What is Criminal syndicates?

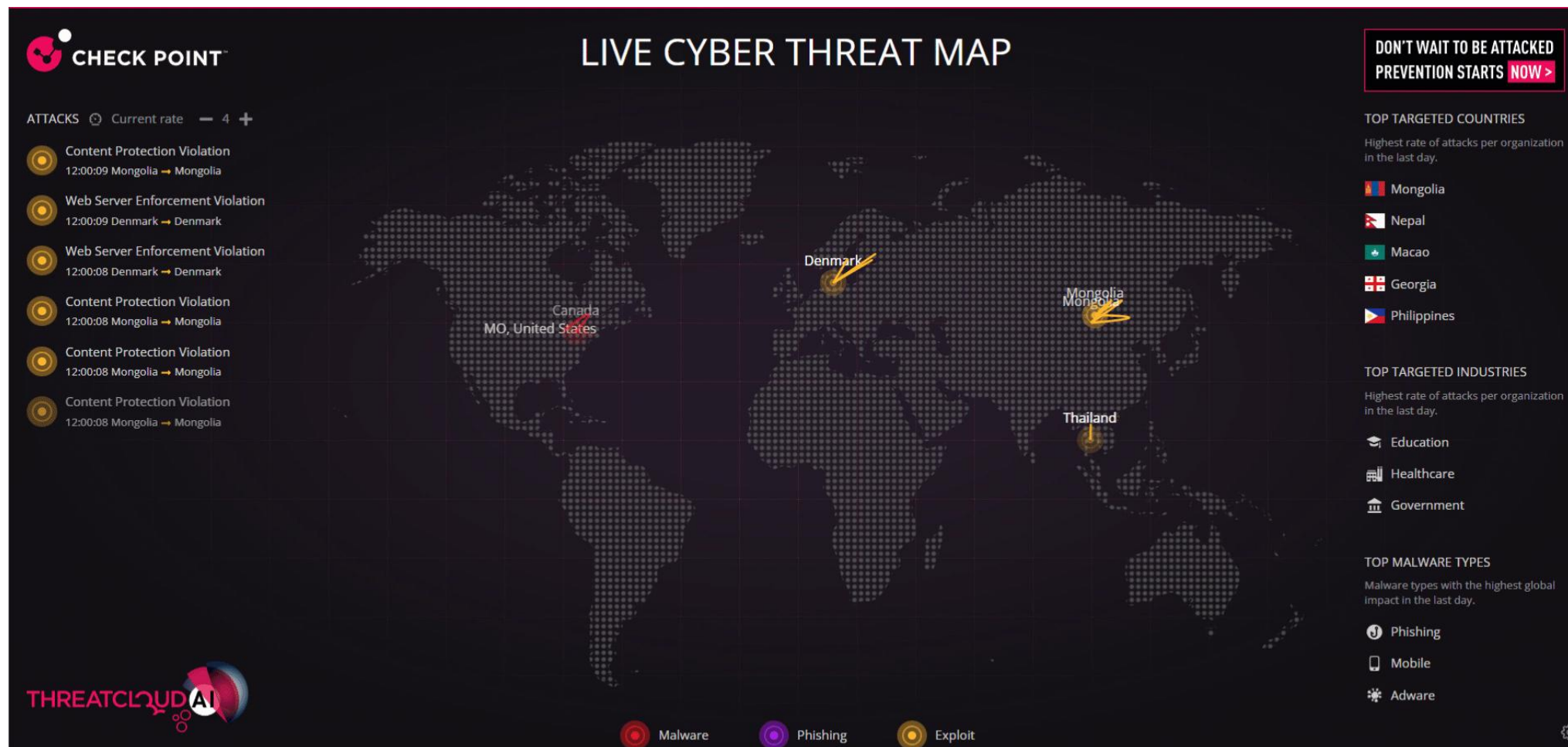
Criminal syndicates also known as organized crime are a huge problem today. These groups are sophisticated, well funded, and cause tremendous damage to vulnerable systems worldwide to make money.

What is State actors?

State actors (nation states) refers to government-directed threat actors, they take advantage of vulnerabilities to acquire intelligence information. Also, they collect *open-source intelligence (OSINT)* which is information from media, public reports, and professional publications. They best funded and most sophisticated of all threat actors.

Important Terminologies

Open-source intelligence (OSINT)



Important Terminologies

Open-source intelligence (OSINT)

**EXPLOIT
DATABASE**

Google Hacking Database

Show 15

Date Added	Dork	Category	Author
2024-01-23	(site:jsonformatter.org site:codebeautify.org) & (intext:aws intext:bucket intext:password intext:secret intext:username)	Files Containing Juicy Info	letmewin cyber
2024-01-23	intitle:"index of" database.properties	Sensitive Directories	Odela Rohith
2024-01-23	filetype:reg reg HKEY_CURRENT_USER SSHHOSTKEYS	Files Containing Juicy Info	web work
2024-01-23	inurl:install.php intitle:"Froxlor Server Management Panel - Installation"	Vulnerable Servers	Nadir Boulacheb (RubX)
2024-01-23	Apache Struts 2.x Path Traversal Vulnerability (CVE-2023-50164) Detection Dork	Vulnerable Servers	Parth Jamodkar
2023-12-21	intitle:"Fleet Management Portal"	Files Containing Juicy Info	Kamran Saifullah
2023-12-21	inurl:"?url=http"	Files Containing Juicy Info	Jeel Patel
2023-12-21	intext:"user" filetype:php intext:"account" inurl:/admin	Files Containing Juicy Info	saurabh kode
2023-12-21	site:.com "index of docker"	Files Containing Juicy Info	Bambang Sutrisna
2023-12-18	Google Dork	Files Containing Juicy Info	Abdulkarim Alsabilah
2023-12-15	Google dorks	Files Containing Juicy Info	Abdulmalik Alharbi
2023-12-14	intext:"userfiles" intitle:"Index Of" site:*.com.*	Files Containing Juicy Info	J. Daniel Elias Valdez
2023-12-14	intitle:"Index of" intext:"php" site:*.com.*	Files Containing Juicy Info	saurabh kode
2023-12-12	GHDB submissions -1	Files Containing Juicy Info	Ajay Naik
2023-12-12	intitle:"Index of" intext:"config" site:*.com.*	Files Containing Juicy Info	J. Daniel Elias Valdez

Showing 1 to 15 of 7,898 entries

FIRST PREVIOUS 1 2 3 4 5 ... 527 NEXT LAST

Customer Login

User Name

Password [Reset Password](#)

☐ Remember me on this computer.

Login

Important Terminologies

Open-source intelligence (OSINT)

[CVE List](#)[CNAs](#)[WGs](#)[Board](#)[About](#)[News & Blog](#)**NVD**

Go to for:

CVSS Scores

CVE Info

Common Vulnerabilities and Exposures

[Search CVE List](#)[Downloads](#)[Data Feeds](#)[Update a CVE Record](#)[Request CVE IDs](#)

TOTAL CVE Records: 222759

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and [CVE Record Format JSON](#) are underway.

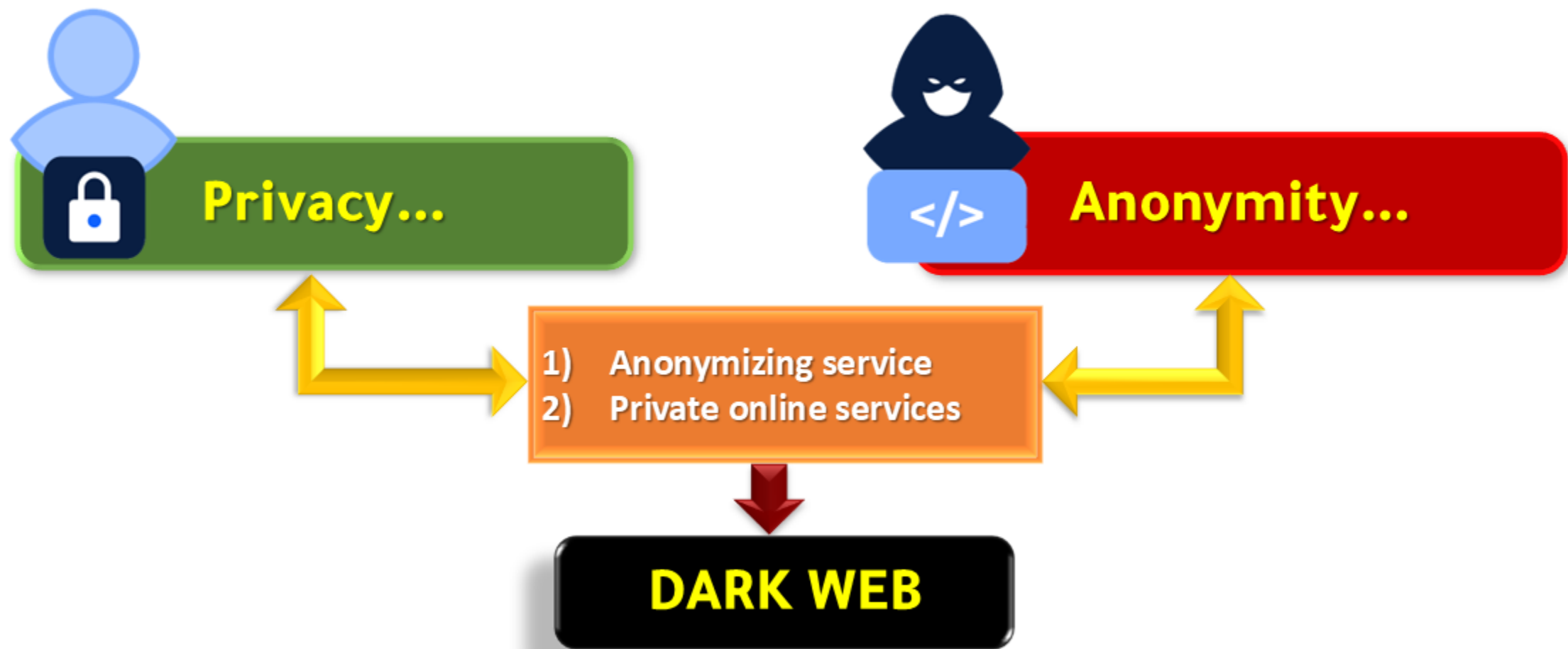
NOTICE: Legacy CVE download formats deprecation is now underway and will end on June 30, 2024.
New CVE List download format is [available now](#).

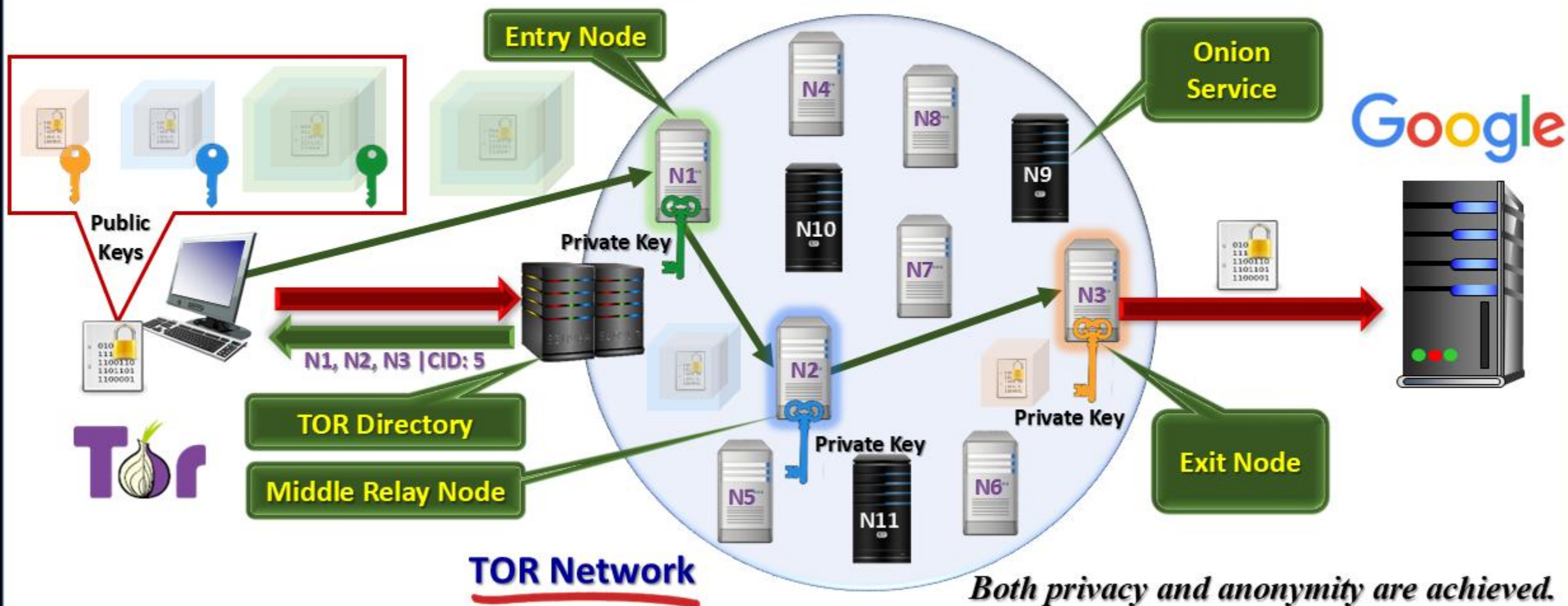
HOME > CVE > SEARCH RESULTS

Search Results

There are 11439 CVE Records that match your search.

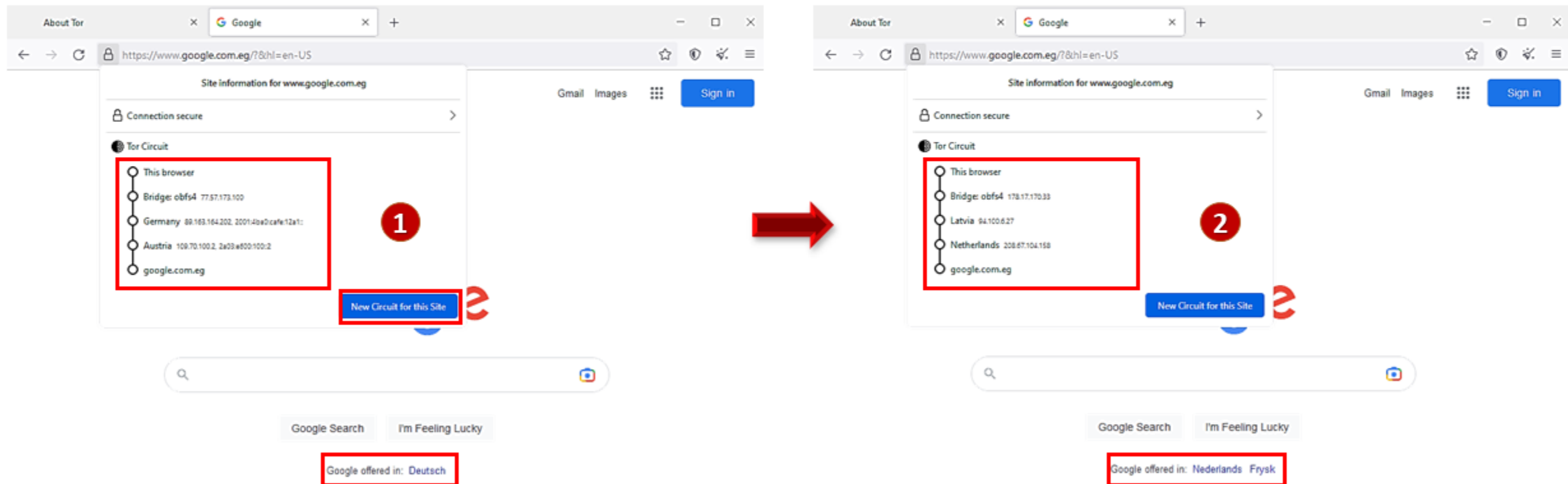
Name	Description
CVE-2024-23678	In Splunk Enterprise for Windows versions below 9.0.8 and 9.1.3, Splunk Enterprise does not correctly sanitize path input data. This results in the unsafe deserialization of untrusted data from a separate disk partition on the machine. This vulnerability only affects Splunk Enterprise for Windows.
CVE-2024-23331	Vite is a frontend tooling framework for javascript. The Vite dev server option `server.fs.deny` can be bypassed on case-insensitive file systems using case-augmented versions of filenames. Notably this affects servers hosted on Windows. This bypass is similar to CVE-2023-34092 -- with surface area reduced to hosts having case-insensitive filesystems. Since `picomatch` defaults to case-sensitive glob matching, but the file server doesn't discriminate; a blacklist bypass is possible. By requesting raw filesystem paths using augmented casing, the matcher derived from `config.server.fs.deny` fails to block access to sensitive files. This issue has been addressed in vite@5.0.12, vite@4.5.2, vite@3.2.8, and vite@2.9.17. Users are advised to upgrade. Users unable to upgrade should restrict access to dev servers.
CVE-2024-22410	Creditcoin is a network that enables cross-blockchain credit transactions. The Windows binary of the Creditcoin node loads a suite of DLLs provided by Microsoft at startup. If a malicious user has access to overwrite the program files directory it is possible to replace these DLLs and execute arbitrary code. It is the view of the blockchain development team that the threat posed by a hypothetical binary planting attack is minimal and represents a low-security risk. The vulnerable DLL files are from the Windows networking subsystem, the Visual C++ runtime, and low-level cryptographic primitives. Collectively these dependencies are required for a large ecosystem of applications, ranging from enterprise-level security applications to game engines, and don't represent a fundamental lack of security or oversight in the design and implementation of Creditcoin. The blockchain team takes the stance that running Creditcoin on Windows is officially unsupported and at best should be thought of as experimental.
CVE-2024-22190	GitPython is a python library used to interact with Git repositories. There is an incomplete fix for CVE-2023-40590. On Windows, GitPython uses an untrusted search path if it uses a shell to run `git`, as well as when it runs `bash.exe` to interpret hooks. If either of those features are used on Windows, a malicious `git.exe` or `bash.exe` may be run from an untrusted repository. This issue has been patched in version 3.1.41.
CVE-2024-21320	Windows Themes Spoofing Vulnerability
CVE-2024-21316	Windows Server Key Distribution Service Security Feature Bypass
CVE-2024-21313	Windows TCP/IP Information Disclosure Vulnerability
CVE-2024-21311	Windows Cryptographic Services Information Disclosure Vulnerability
CVE-2024-21310	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability

The Dark Web

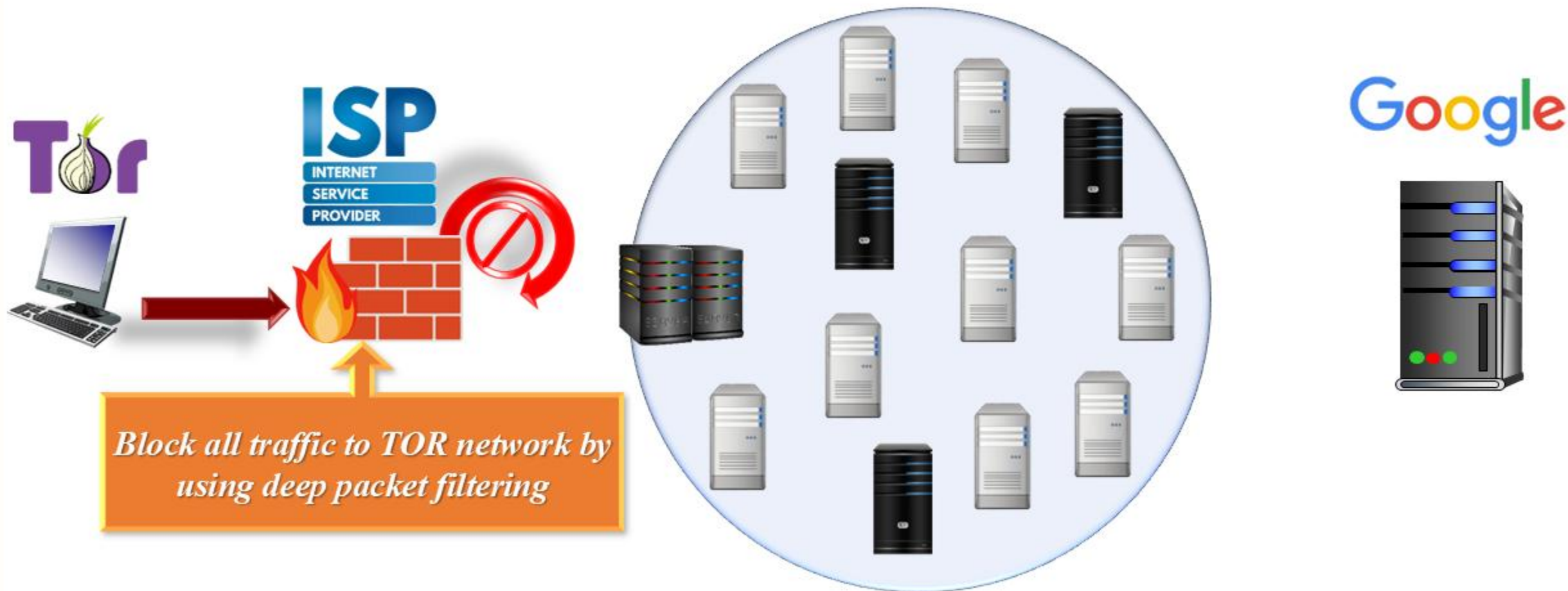
The Dark Web

The Dark Web

Configuring TOR Browser For Maximum Security & Anonymity



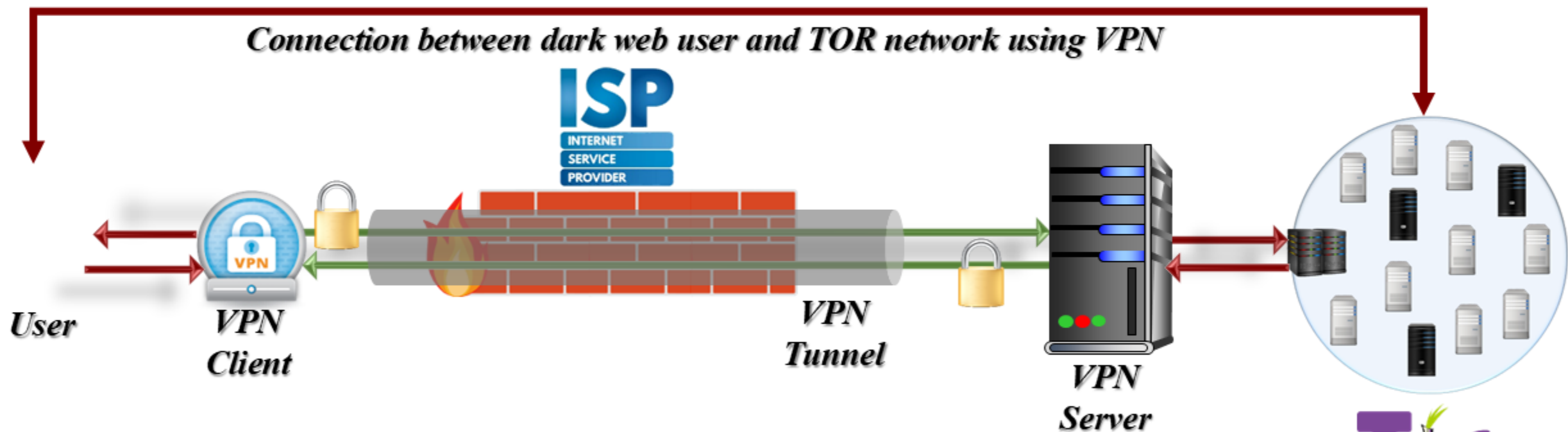
Selecting new nodes for the current website

The Dark Web

Important Terminologies

The Dark Web

Connection between dark web user and TOR network using VPN



Kaspersky VPN

AVG VPN

ZSVPN clients

✓ Use well known VPN providers.

✓ Avoid free providers.

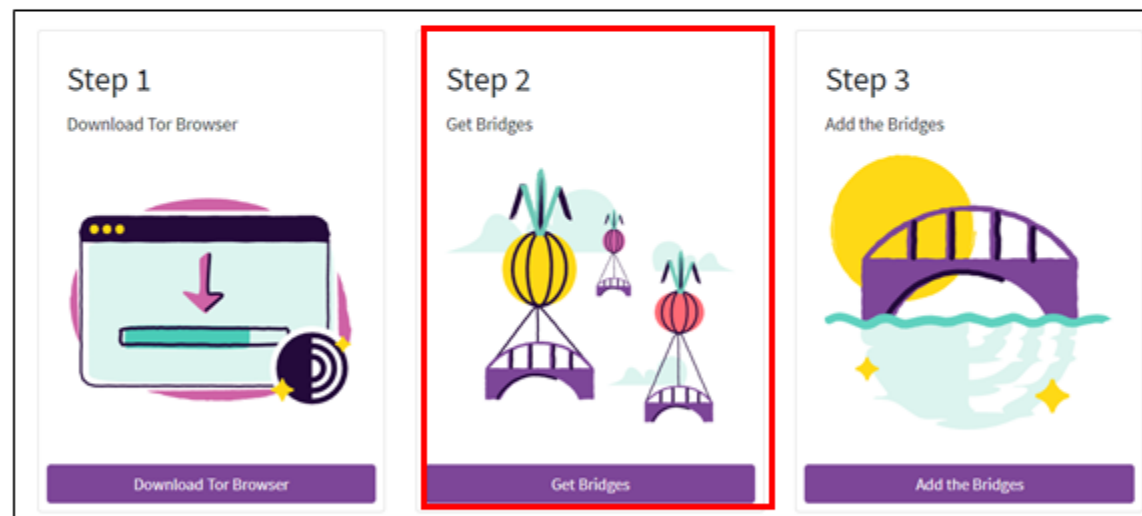
✓ Make sure they keep no logs.



The Dark WebConnecting to TOR Network using bridges/pluggable transports.

TOR **bridges** are secret Tor relays (*they don't appear in any public list*) that keep your connection to the Tor network hidden (*the ISP doesn't know which addresses to block*):

- Request a bridge on <https://bridges.torproject.org/> or then click on “*Get Brides*”.



Threat intelligence Sharing

Automated Indicator Sharing (AIS):

It is the automated way that threat intelligence information can be shared among many different software programs and many different enterprises.

This uses a specialized format called the *Structured Threat Information Expression* or *STIX* format that understood among many dissimilar systems.

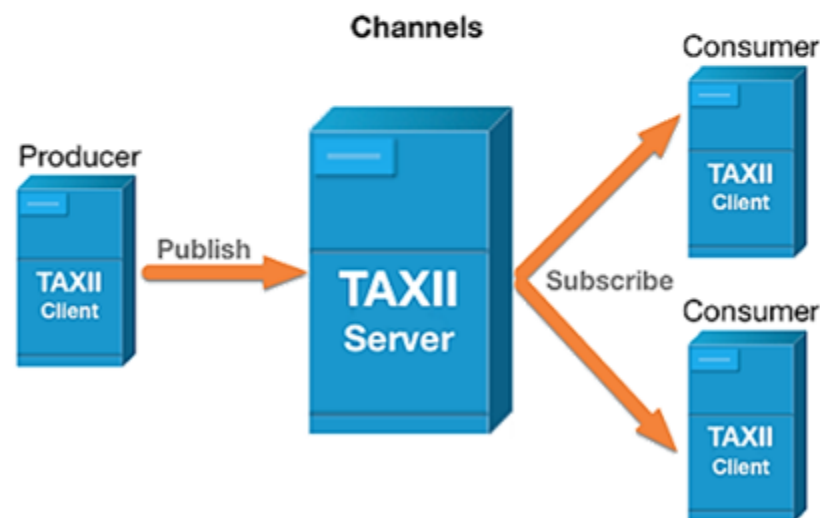
```
{
  "type": "bundle",
  "id": "bundle--56be2a3b-1534-4bef-8fe9-602926274089",
  "objects": [
    {
      "type": "indicator",
      "spec_version": "2.1",
      "id": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4f",
      "created": "2014-06-29T13:49:37.079Z",
      "modified": "2014-06-29T13:49:37.079Z",
      "name": "Malicious site hosting downloader",
      "description": "This organized threat actor group operates to crea",
      "indicator_types": [
        "malicious-activity"
      ],
      "pattern": "[url:value = 'http://x4z9arb.cn/4712/']",
      "pattern_type": "stix",
      "valid_from": "2014-06-29T13:49:37.079Z"
    },
    {
      "type": "malware",
      "spec_version": "2.1",
      "id": "malware--162d917e-766f-4611-b5d6-652791454fca",
      "created": "2014-06-30T09:15:17.182Z",
      "modified": "2014-06-30T09:15:17.182Z",
      "name": "x4z9arb backdoor",
      "description": "This malware attempts to download remote files aft",
      "malware_types": [
        "backdoor",
        "remote-access-trojan"
      ],
      "is_family": false,
      "kill_chain_phases": [
        {
          "kill_chain_name": "mandiant-attack-lifecycle-model",
          "phase_name": "establish-foothold"
        }
      ]
    }
  ]
}
```

Threat intelligence SharingTrusted Automation Exchange of Intelligence Information (TAXII):

It transmits that specially formatted threat intelligence information (STIX) across a network for machine-to-machine communications. TAXII is a transport protocol that supports transferring STIX insights over Hyper Text Transfer Protocol Secure (HTTPS).

Two key concepts in TAXII :

- A collection is a set of STIX packages organized and managed by a single entity.
- A channel allows organizations to access a specific collection, such as through an API, or file exchange.



Threat intelligence SharingWhy is STIX/TAXII important?

- *Improve threat intelligence sharing*: STIX/TAXII provides a common language for organizations to share and exchange threat intelligence.
- *Increase intelligence accuracy*: STIX/TAXII framework helps ensure that intelligence data is consistent, complete, and accurate.
- *Automate support*: The use of common language and standards in STIX/TAXII makes it easier for organizations to automate threat detection, analysis, and response processes, which results in improving efficiency and reducing the risk of human error.

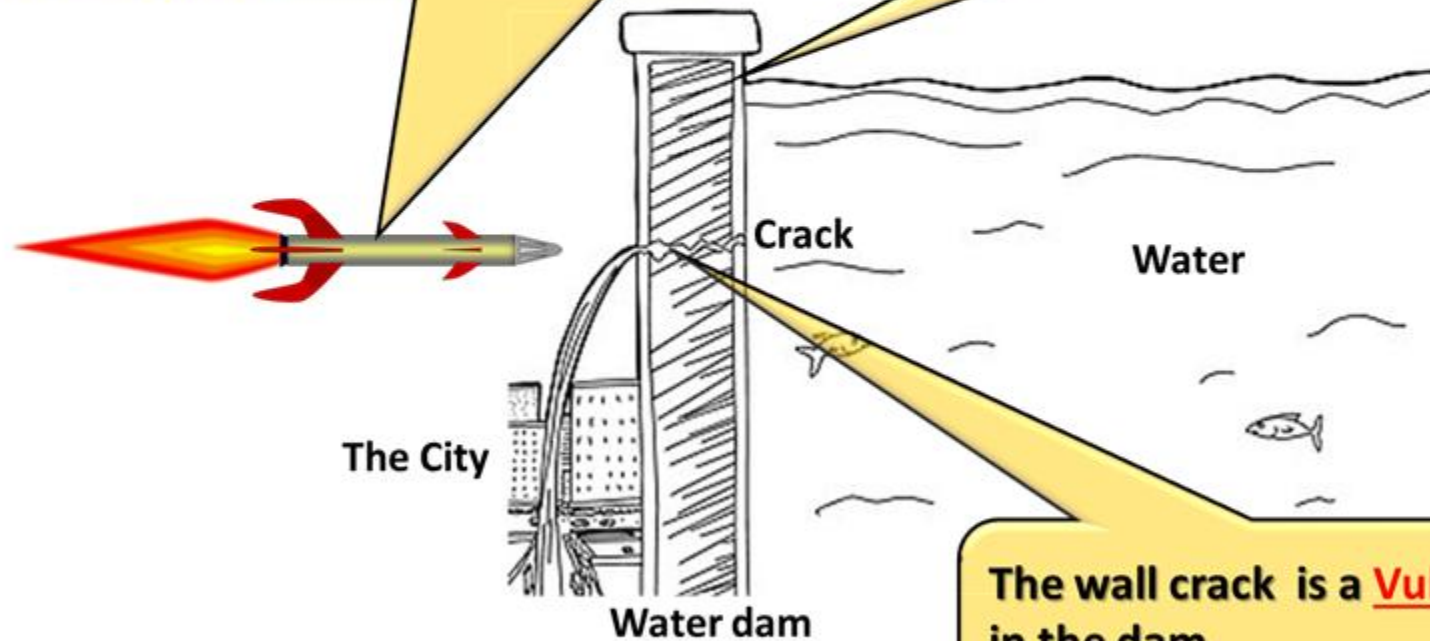
Important Terminologies

Threat Actors attacks the dam using the wall crack (Vulnerability)

Ex. (Computer) attacker sending malicious software to the open port to harm the system

Crossing the water behind the dam to the City is a Threat.

Ex. (Computer) System failures



The wall crack is a Vulnerability in the dam.

Ex. (Computer) Open ports

What is the threat vector ?

A threat vector is the means or pathway by which an attacker can *gain unauthorized access* to a computer or network to deliver a malicious payload or carry out an unwanted action.

The attack surface represents the *sum of all potential vulnerabilities* and entry points that an attacker could exploit (e.g. messages, Images, files, voice calls, unsecured network, etc.).

Critical IT System:

- The network
- Payment system.
- Email.
- Web applications.
- Bluetooth (*Blue Borne or Blue Smack*).

Third Party vendor:

- Supply chain Vendors
- Business Partners.
- Remote access Clients.

Physical Vectors:

- Building access control.
- Servers Room.
- Removable devices.
- Mobile devices

Tactics, Techniques, and Procedures (TTPs):

Tactics, Techniques, and Procedures (TTPs) are the specific methods and patterns of activities or behaviors associated with a particular threat actor or group of threat actors.

Deception and Disruption Technologies :

Deception and disruption technologies are designed to *mislead*, *confuse* and *divert attackers away from critical assets* while simultaneously detecting and neutralizing threats. By creating a dynamic environment or presenting false information.

The four commonly used deception and disruption technologies are *honeypots*, *honeynets*, *honey files*, and *honeytokens*.

Honeypots:

A honeypot is a decoy system or network set up to attract potential hackers. used to *mimic a real system* with vulnerabilities that seem attractive to attackers and designed to *log all interactions and transactions* in order to provide valuable insights into the threat landscape.

Installation of a honeypot on the enterprise network should *locate within a screen subnet of the network or an isolated segment of the network* that can be easily accessed over the internet by a potential attacker.



Honeynet :

A honeynet is essentially a network of honeypots to create a more complex system that is designed to mimic an entire network of systems including servers, routers, and switches.

Honeynets are often *used by a large organizations and research institutions* to study the behavior of threat actors in a more controlled environment like a honeypot.

A honeynet *logs all activities* to provide us with a wealth of data about both the successful and unsuccessful attacks being attempted against our network.

Honey file :

A honey file is a decoy file placed within a system to lure in potential attackers.

Honey file should appear to contain valuable or sensitive information that will entice a threat actor to go after the data, but in reality, it serves as a trap and contains fake data.

Some honey files have embedded code that allows them to begin *enumerating the attacker's network* once the file is open. these could be *any type of file* including word processing documents, spreadsheets, presentation files, images, database files, or even executables. These honey files are typically *embedded with unique identifiers* or watermarks to help track the file if it is stolen or copied.

Honeytoken :

A honeytoken is a piece of data or a resource that has no legitimate value or use, but is monitored for access or use.

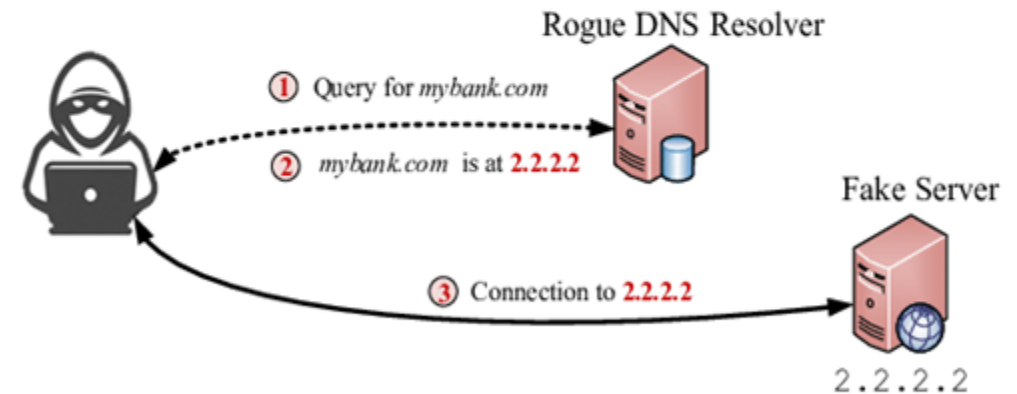
A honeytoken could be a *fake user account or a dummy database record*. If the honeytoken is accessed or used, this is a clear indication that a security breach is likely occurring.

Honeytokens are particularly useful for *detecting insider threats*. Since they have no legitimate use, any interaction with them is suspicious.

Bogus DNS entries:

Bogus DNS entries is disruption technology and strategies that create a fake DNS entries introduced into the system DNS server.

By adding these deceptive entries, administrators can *mislead attackers into accessing non-existent domains or trap systems* to waste the attacker's time and resources while *simultaneously alerting the defenders* about potential malicious activities.



Decoy directories:

Decoy directories are fake folders and files placed within a system storage.

When unauthorized user attempts to access or modify these directories, the system can *raise an alert* and the *attacker is misled by false data* and made to think that they have successfully gained access to your organization's genuine resources.

Dynamic page generation:

Generating dynamic pages, websites can present ever-changing content to web crawlers to *confuse and slow down the threat actor*. This tactic can be especially effective *against automated scrubbing tools* that trying to index or steal content from the organization's website.

Port triggering:

Port triggering is a security mechanism where *specific services or ports on a network device remain closed* until a specific outbound traffic pattern is detected. *Once the pattern is observed, the service or port is opened temporarily.*

This method ensures that *certain services remain invisible* and inaccessible to potential attackers scanning for open ports but become *available for legitimate users when needed.*

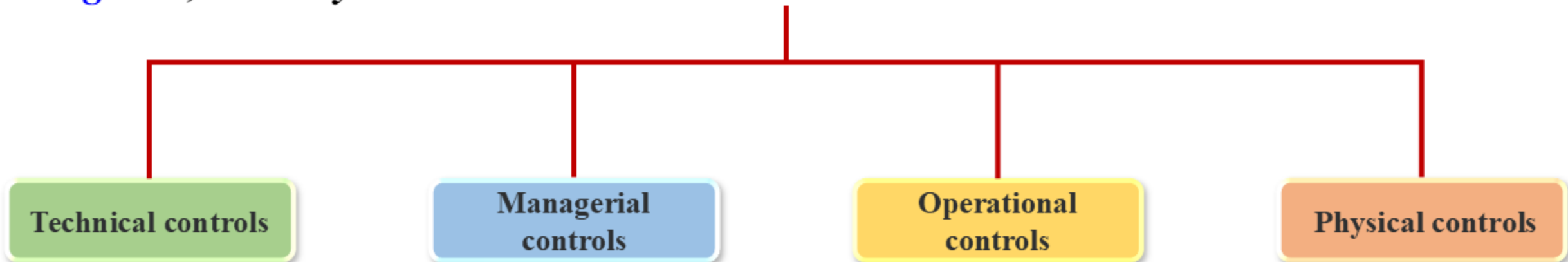
Spoofing fake telemetry data:

When an attacker try to attach the organization network, it can be configured to respond by sending out fake telemetry or network data. This data can be used to confuse an attacker.

What is Security Control?

Any type of safeguard or countermeasure used to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

*There are **six types of security controls**, they could be categorized into **four main categories**, and they are:*



What is Technical controls?

Technical controls are the technologies, hardware, and software mechanisms that are implemented to manage and reduce risk. They operate within a systems technology layer.

Preventative	Detective	Corrective
- Antivirus - Firewall - Intrusion Prevention System (IPS) - Multi-factor authentication (MFA)	- Honeypot - Intrusion Detection System (IDS)	- Vulnerability patching - Quarantine a virus. - Reboot a System.

What is Managerial controls?

Managerial controls are actions taken to manage the development, maintenance, and use of the system security, including system-specific policies, procedures, and rules of behavior, individual roles and responsibilities.

Preventative	Detective	Corrective
▪ Hiring and Termination policy. ▪ Separation of duties. ▪ Data classification.	▪ Review access rights. ▪ Audit logs and unauthorized changes.	▪ Implement business continuity plan. ▪ Having an incident respond plan.

What is Operational controls?

Operational controls are the procedures and measures that are designed to protect data on a *day-to-day basis*, and they're mainly governed by internal processes and human actions.

Preventative	Detective	Corrective
▪ Standard Operating Procedures ▪ Periodic and timely maintenance. ▪ Security Awareness Training Policy. ▪ Mobile Device Policy.	▪ Audit security procedures and measures. ▪ Security Information and Event Management (SIEM).	▪ Disaster Recovery Policy ▪ Having an incident respond plan.

What is Physical controls?

Physical controls are anything tangible that's used to prevent or detect unauthorized access to physical areas, systems, or assets.

Preventative	Detective	Corrective
▪ Fences and Building light. ▪ Gates and Locks. ▪ Mantraps and Access control vestibule. ▪ Biometric devices, hard tokens, ID badges	▪ Surveillance cameras. ▪ Closed Circuit Television (CCTV)	▪ Reissue the access cards. ▪ Repair physical damage.

The other three types of security controls?

Deterrent Controls are administrative mechanisms (such as policies, procedures, standards, guidelines, laws, and regulations) that are used to guide the execution of security within an organization.



NO USB DRIVES

NO USB DRIVES

NO USB DRIVES

⚠ NO USB DRIVES



Compensating Controls are technical mechanisms that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time or address any weaknesses of existing controls.

Example: *Running a legacy system that simply can't support the latest form of wireless encryption known as WPA3.*

In this case, you might instead choose to implement WPA2 and use a VPN on top of that from your endpoint to your internal servers to act as a compensating control.

Directive Controls are in the form of policies and guidelines that establish the rules and standards that an organization must follow to maintain a secure environment.

Example: *Policy that provides guidelines on how employees are permitted to use company-owned IT assets. Some tools may use with directive controls such as Exception reports and performance review.*

Security Controls

