Cyber Security

Research and answer all of the following questions or items below.

What is Encryption and how does it work?

*List some types of encryption and the differences.

What is a IDS & IPS?

*List some common types of IDS and IPS.

What is incident response?

*Give a brief an example of how to implement an incident response policy and plan.

List some security best practices for managing an environment and tools that can be used to secure a network or environment.

Describe ethical hacking and why it is important for the cyber security industry.

List some tools that can be used to identify vulnerabilities and how they work.

What is NIST and why is it important?

What are CVE and CVSS and explain the difference.

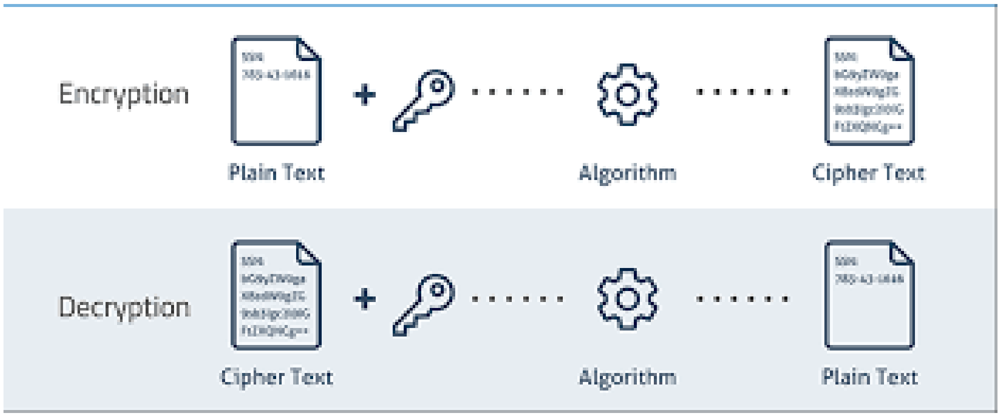
What is a STIG and what are they used for?

What is compliance and why is it important in the Cyber Security industry?

Encryption

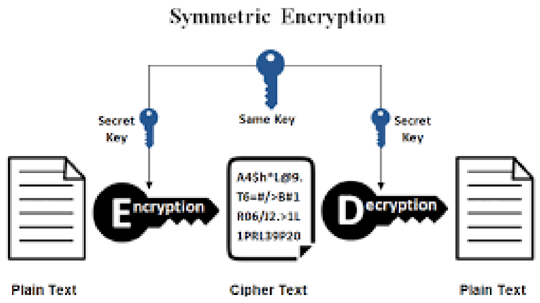
Encryption is a method of securing data by encoding it mathematically so that it can be read, or decrypted, by the intended recipient with the correct key or cipher. Encryption is defined as the process of converting human-readable plaintext into incomprehensible text, or ciphertext. Encryption gets readable data and modifies it to be displayed randomly with the use of a cryptographic key. A cryptographic key is a string of characters used within an encryption algorithm for changing data so that it appears random. Like a physical key, it locks or encrypts data with a set of mathematical values that both the sender and the recipient of an encrypted message agree on. The sender’s mathematical value can be considered as a lock and the recipient’s mathematical value can be seen as a key to unlock or decrypt the data.

The following diagram shows a depiction of the encryption process.



Asymmetric and symmetric encryption are the two main types of encryptions used today. Symmetric encryption is a widely used data encryption technique where data is encrypted and decrypted using the same cryptographic key that is shared between the sender and recipient. With Symmetric encryption the data is encrypted by using a single private key. This same private key is used to decrypt the data making the process easy to use but less secure. It also requires a safe method to transfer the key from the sender to the recipient. Once the data is encrypted into ciphertext, the data can't be read or otherwise understood by anyone who doesn't have the key. This means that you and the party you're communicating with both need to have an identical copy of the key to communicate securely.

The following diagram shows a depiction of the symmetric encryption process.



sender recipient

Block ciphers are very important in the designing of many cryptographic algorithms and are widely used to encrypt the bulk of data in chunks. By chunks, it means that the cipher takes a fixed size of the plaintext in the encryption process and generates a fixed size ciphertext using a fixed-length key. An Encryption algorithm's strength is determined by its key length.

If the plaintext is shorter than the block length, then it is padded out to the desired length before encryption. At the other end, the recipient of the message will decrypt it and then remove the padding to restore the original message.

If a plaintext is longer than the block length, then it is broken up into multiple different chunks for encryption. A block cipher mode of operation defines how these chunks are related to one another.

The downside of this is that blocks with the same plaintext produce the same ciphertext.

Stream Ciphers

The other type of symmetric encryption algorithm is a stream cipher. Unlike a block cipher, a stream cipher encrypts a plaintext one bit at a time.

A stream cipher is designed based on the only completely unbreakable encryption algorithm: the one-time pad (OTP). The OTP takes a random secret key the same length as the plaintext and exclusive-ors (XORs) each bit of the plaintext and key together to produce the ciphertext as shown in the image above

Popular symmetric algorithms

AES (Advanced Encryption Standard)

- Established by the U.S National Institute of Standards and Technology (NIST) in 2001.
- Strongest encryption algorithm to date
- AES is a block cipher. (Encrypting data in blocks to produce ciphertext using a cryptographic key and algorithm)
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

DES (Data Encryption Standard)

- DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text goes as the input to DES
- The same algorithm and key are used for encryption and decryption, with minor differences.
- The key length is 56 bits.
- has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on the decline
- 3DES was developed as a more secure alternative because of DES's small key length.

IDEA (International Data Encryption Algorithm)

- designed by James Massey of ETH Zurich
- uses a fixed-length plaintext of 16 bits and encrypts them in 4 chunks of 4 bits each to produce 16 bits of ciphertext.
- The length of the key used is 32 bits.
- The key is divided into 8 blocks of 4 bits each.

Blowfish (Drop-in replacement for DES or IDEA)

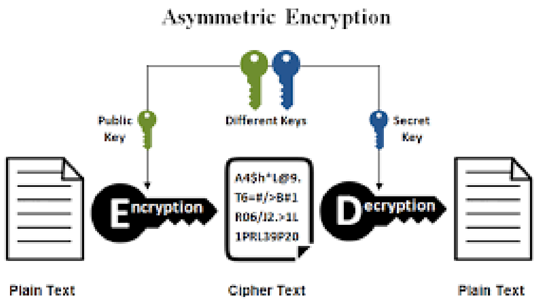
- designed by Bruce Schneier in 1993 as an alternative to DES Encryption Technique.
- block Size: 64-bits
- key Size: 32-bits to 448-bits variable size
- messages that aren't a multiple of eight bytes in size must be padded. (Adding data to the beginning, middle, or end of a message prior to encryption.)

Twofish (Advanced version of Blowfish)

- designed by Bruce Schneier as an improved version of Blowfiish
- a block size of 128 bits and accepts a key of any length up to 256 bits.
- one of the fastest encryption algorithms and is ideal for both hardware and software environments
- Used in modern applications.
- break of the Twofish algorithm has not occurred yet.

Asymmetric encryption requires two cryptographic keys. The sender encrypts data by using the recipients' public key. This public key is a large numerical value that can be viewed by anyone and can only be used for encryption. Once encrypted the data can then be decrypted by the recipients' private key. Asymmetric encryption is more secure due to the recipient's private key not being shared with the sender. Although the public key can be viewed by anyone does point to a security flaw.

The following diagram shows a depiction of the asymmetric encryption process.



sender recipient

Integer-Based Cryptography

Integer-based asymmetric cryptography uses two main "hard" problems. These are the factoring and discrete logarithm problems.

An asymmetric encryption algorithm based on the factoring problem will have a public key calculated using the product of two private keys (large prime numbers).

The difficulty of multiplication grows as the length of polynomials grow with the length of the factors, but the difficulty of factoring grows exponentially. This makes it possible to find a "sweet spot", where a system is usable but essentially unbreakable.

The discrete logarithm problem uses exponentiation and logarithms as its "easy" and "hard" operations. Similar to factoring, the complexity of calculating logarithms grows much more quickly as the size of the exponent increases.

Elliptic-Curve Cryptography

Integer-based asymmetric cryptography uses factoring and discrete logarithm problems to build secure encryption algorithms. Elliptic curve cryptography uses the same problems with a little twist.

Instead of using integers for its calculations, elliptic curve cryptography uses points on an elliptic curve A private key is still a random number, but a public key is a point on the curve.

A few different mathematical operations are defined on these curves. The two important ones here are:

Point Addition (equivalent to integer multiplication)

Point Multiplication (equivalent to integer exponentiation)

On these curves, it is possible to perform calculations that are equivalent to the “easy” operations of the factoring and discrete logarithm problems. This means that the same basic algorithms can be adopted to use with elliptic curves.

Elliptic curve cryptography is useful because smaller key lengths provide the same level of security. This means that elliptic curve cryptography uses less storage, processing power, and energy to protect data at the same level as an equivalent integer-based algorithm. These savings can be important for resource-constrained systems like Internet of Things (IoT) devices or smartphones

Popular asymmetric algorithms

Rivest Shamir Adleman (RSA)

- Published in 1977, RSA is one of the oldest examples of asymmetric encryption. Developed by Ron Rivest, Adi Shamir, and Leonard Adleman
- generates a public key by multiplying two large, random prime numbers together, and using these same prime numbers, generates a private key.

the Digital Signature Standard (DSS), which incorporates the Digital Signature Algorithm (DSA)

- A sender's private key is used to digitally sign a message or file, and the recipient uses the sender's corresponding public key to confirm that the signature originated from the correct sender and not a suspicious or unauthorized source.

Elliptical Curve Cryptography (ECC)

- an RSA alternative that uses smaller key sizes and mathematical elliptic curves to execute asymmetric encryption
- ECC is much faster than RSA in terms of key and signature generation, and many consider it the future of asymmetric encryption, mainly for web traffic and cryptocurrency but for other applications as well.

the Diffie-Hellman exchange method.

- is a key exchange method that two parties who have never met can use to exchange public and private key pairs over public, insecure communication channels.
- These keys could be securely exchanged over public communication channels, where third parties normally extract sensitive information and encryption keys.

TLS/SSL protocol.

- uses asymmetric encryption to establish a secure client-server session while the client and server are generating symmetric encryption keys.
- known as a TLS handshake
- the client-server session keys are used to encrypt the information exchanged in that session.

Differences between Asymmetric and Symmetric key encryption

Symmetric Key Encryption	**Asymmetric Key Encryption**
It only requires a single key for both encryption and decryption.	It requires two keys, one to encrypt and the other one to decrypt.
The size of cipher text is same or smaller than the original plain text.	The size of cipher text is same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.

IDS and IPS

An Intrusion Detection System (IDS) is a system designed to monitor network traffic for potential malicious activity and notifies when activity is discovered. Today IDS systems come in the forms of a software application. These applications scan a network or system for malicious activity or a breach in a company's policy that has been set on a network. Any violation is then sent to a system administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system offers real-time monitoring and analysis of events as well as tracking and logging of security data for compliance or auditing. This system is responsible for filtering the false alarms that an IDS system picks up.

Network Information Detection System (NIDS) are a network-based intrusion detection system used to monitor and analyze network traffic to protect a system form network-based threat. NIDS read packets that are coming into the network and look for any patterns that are deemed suspicious that can possibly be Denial-of-Service attacks, port scanning, or a sharp increase in network traffic. A single sensor can monitor several hosts, but multiple NIDS might be required depending on the amount of traffic going to and from all network devices. NIDS are passive devices meaning they do not interfere with the traffic they monitor. If the device sees anything suspicious, then a network administrator would be alerted, and incident response will begin.

For example, an attacker could have gained access to a network through an open port that contained a vulnerability that the attacker knows how to exploit and gain access. The attacker can then initiate a backdoor onto the network to remain access escalate privileges to that of an Administrator of the network and deploy malicious programs that can steal sensitive information against the organization and encrypt the data that an organization needs access to keep their business running. The attacker will then demand a ransom to the organization so that the business can gain access to their data once again. This is known as a ransomware attack which is very common today. Reports of ransomware incidents increased 62% in 2021 compared to 2020. Ransomware was also the third most used cyberattack method in 2021, accounting for 10% of all data breaches. When conducting an incident response, it is very important to remediate the incident as fast as possible and more important for the incident response team to always be prepared for any intrusions on a network. As newer technology comes out their will be new ways for attackers to gain unwanted access to these networks and systems an incident response team should be familiar with how these new systems work and the vulnerabilities that lead to unwanted access.

Typically, an incident response team will pose the following questions:

- How did the attackers manage to get into the network?
- Is the Incident ongoing?
- What information was stolen or accessed?
- What resources were affected by the incident?
- What did the intrusions detection systems pick up?
- What steps should be performed to patch the network or systems affected?
- How can the organization be protected by similar incidents?

An incident response team will then conduct the following methodology:

Pre-incident preparation

- Take actions to prepare the organization and the incident response team before an incident occurs.

Detection of incidents

- Identify a potential computer security incident. Initial response Perform an initial investigation, recording the basic details surrounding the incident, assembling the incident response team, and notifying the individuals who need to know about the incident.

Formulate response strategy

- Based on the results of all the known facts, determine the best response and obtain management approval. Determine what civil, criminal, administrative, or other actions are appropriate to take, based on the conclusions drawn from the investigation.

Investigate the incident

- Perform a thorough collection of data. Review the data collected to determine what happened, when it happened, who did it, and how it can be prevented in the future.

Reporting

- Accurately report information about the investigation in a manner useful to decision makers.

Resolution

- Employ security measures and procedural changes, record lessons learned and developed long-term fixes for any problems identified.

Security Practices for managing an environment

Install/Monitor Firewalls

A firewall is a piece or set of software or hardware designed to block unauthorized access to computers and networks. A firewall is a series of rules that control incoming and outgoing network traffic. Firewalls can block known ports that are vulnerable to attacks that may not be needed for a business to continue running.

Firewalls are becoming more and more sophisticated (right along with hackers) and the latest are integrated network security platforms that consist of a variety of approaches and encryption methods, all working in tandem to prevent breaches.

Password protection/authentication

Protecting password by using hashing algorithms to store passwords is a recommended approach. By encrypting passwords protects account information that from being stolen. if there were to be an incident and the attacker was able to extract account and password information the information wouldn’t be readable to the attacker and deemed worthless. There are several hashing algorithms that would take a lifetime to crack. Having users authenticate themselves for every login is also recommended this way if their were to be a breach and the attacker were to use stolen credentials to login to a system the users account will be notified and can deny the attacker from gaining unwanted access.

Advanced Endpoint Detection

To respond to the continually evolving online threats in the world today, advanced endpoint detection and response is technology that uses AI to watch for indications of compromise and react accordingly. The technology collects and analyzes information from network devices, endpoint logs and threat intelligence feeds, identifying security incidents, policy violations, fraudulent activity, and other threats. To respond more quickly, these solutions employ a high degree of automation to enable security teams to quickly identify and respond to threats. Indications of compromise include behavior characteristics related to threat actor intrusion, malware, ransomware, and traditional virus-like behavior. More advanced than anti-virus software, endpoint detection and response is part of a modern, layered, proactive approach to cybersecurity to defend against ever-changing cyberattacks.

Create A Virtual Private Network (VPN)

VPNs create a far more secure connection between remote computers (home networks or computers used by people on the road) and other “local” computers and servers.

These networks are essentially only available to people who should have access to your systems, including your wireless network, and to equipment that’s been authorized in your network settings. A VPN can dramatically decrease the likelihood of hackers finding a wireless access point and wreaking havoc on your system.

Employee training

If employees that are using your system aren’t following computer security best practices. Frequent reminders about the risks and the steps to mitigate them will help keep network security top of mind. Educating employees about how to avoid major security risks can help mitigate cyber-attacks.

Ethical Hacking

Hacking is the technique of finding the weak links or loopholes in the computer systems or the networks and exploiting it to gain unauthorized access to data or to change the features of the target computer systems or the networks. Hacking describes the modification in the computer hardware, software, or the networks to accomplish certain goals which are not aligned with the user goals. In contrast, it is also called breaking into someone's security and stealing their personal or secret data such as phone numbers, credit card details, addresses, online banking passwords etc.

White Hat Hackers

A white hat hacker is a computer security specialist that breaks into and find loopholes in the protected networks or the computer systems of some organization or company and corrects them to improve the security. White Hat Hackers protects the organization before malicious or bad hackers find it and make any harm to the company or the organization. White Hat Hackers are the authorized persons in the industry, although the methods used by them are like those of bad hackers, but they have permission from the organization or the company who hires them to do so.

Black Hat Hackers

A Black Hat Hacker also known as is a computer hardware and software expert who breaks into the security of someone with malicious intent or bad intentions of stealing or damaging their important or secret information, compromising the security of big organizations, shutting down or altering functions of websites and networks. They violate the computer security for their personal gain. These are persons who typically wants proves their extensive knowledge in the computers and commits various cybercrimes like identity stealing, credit card fraud etc.

Grey Hat Hacker

is a computer hacker or security expert who sometimes violates the laws but does not have any malicious intentions. The term Grey Hat is derived from the Black Hat and the White Hat as the white hat hackers finds the vulnerabilities in the computer system or the networks and does not tells anybody until it is being fixed, while on the other hand the black hat hackers illegally exploits the computer system or network to find vulnerabilities and tells others how to do so whereas the grey hat hacker neither illegally exploits it nor tells anybody how. Grey Hat Hackers represents between the white hat hackers who operate to maintain system security and the black hat hackers who operate maliciously to exploits computer systems.

Ethical hacking is used as a common and favored process to analyze the security systems and programs of an organization. It runs parallel with security judgment, red teaming, intrusion testing, and vulnerability. Here are certain important points that will help you understand more about ethical hacking and its necessity.

An ethical hacker usually tends to play the role of a security expert while hacking a computer system. They penetrate systems to detect risks and illegal access of the same. They constantly must face two hurdles — threat and vulnerability. Ethical hacking follows the guidelines of safe hacking for the efficient working of the system. Ethical Hacking comes handy in corporate sectors and organizations, to fight against unlawful practices of breaching systems and to take precautionary actions on hackers. Dangerous software like Trojan horses, viruses and spam email causes disruption and disturbance in the system and storage space. Ethical hacking provides useful here as it helps to uncover these virus attacks against systems and in addition, lends high-level security. The main objective of ethical hacking is to promise safety in wireless infrastructure which constitutes most of the current business companies' aims. Ethical hacking has the privilege of gathering access to a company's network and information system. This automatically provides security to intellectual attacks and threats like viruses. Ethical hacking, as a result, ends up also testing the security levels of the programs and software

Tools used to identify vulnerabilities

OpenVAS

- This is an open-source tool serving as a central service that provides vulnerability assessment tools for both vulnerability scanning and vulnerability management.
- OpenVAS supports different operating systems
- The scan engine of OpenVAS is constantly updated with the Network Vulnerability Tests
- OpenVAS scanner is a complete vulnerability assessment tool identifying issues related to security in the servers and other devices of the network
- OpenVAS services are free of cost and are usually licensed under GNU General Public License (GPL)

Nikto

- Nikto is an open-source web vulnerability scanner employed for assessing probable issues and vulnerabilities.
- It is also used for verifying whether the server versions are outdated, and checks for any problem that affects the functioning of the server
- Nikto is used to perform a variety of tests on web servers to scan different items like a few hazardous files or programs
- It is not considered a quiet tool and is used to test a web server in the least possible time
- It is used for scanning different protocols like HTTPS, HTTPd, HTTP, etc. This tool allows scanning multiple ports of a specific server.

Wireshark

- Wireshark is an extensively used network protocol analyzer considered to be the most powerful tool in the security practitioner's toolkit.
- Wireshark is used across different streams like government agencies, enterprises, educational institutions, etc. to investigate the network packets that are coming in and out of the network
- It captures the issues online and executes the analysis offline
- Wireshark can detect vulnerabilities based on the behavior of the network packets that are coming through the network and what port the packets are coming through
- Wireshark uses a color code scheme to make it easier for security professionals to identify vulnerabilities at a faster rate
- It runs on different platforms like Linux, macOS, Windows, Solaris, etc.

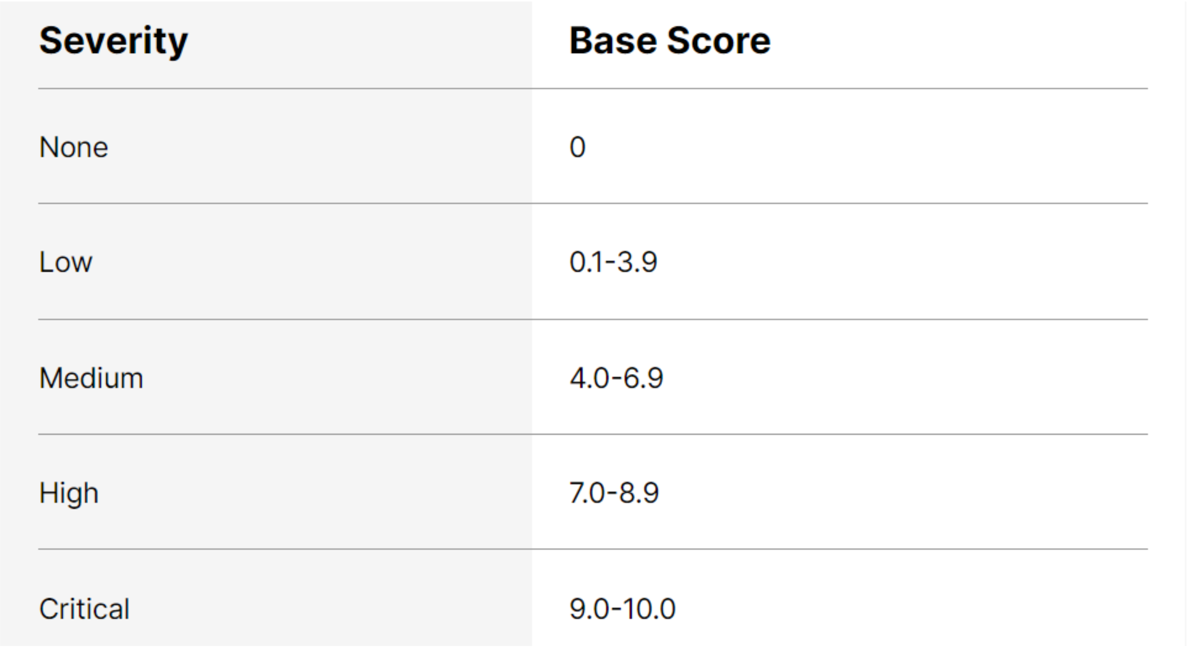
NIST

The National Institute of Standards and Technology is a non-regulatory government agency that develops technology, metrics, and standards to drive innovation and economic competitiveness at U.S.-based organizations in the science and technology industry. NIST produces standards and guidelines to help federal agencies meet the requirements of the Federal Information Security Management Act (FISMA). NIST guidance provides the set of standards for recommended security controls for information systems at federal agencies. These standards are endorsed by the government, and companies comply with NIST standards because they encompass security best practices controls across a range of industries – an example of a widely adopted NIST standard is the NIST Cybersecurity Framework. NIST standards are based on best practices from several security documents, organizations, and publications, and are designed as a framework for federal agencies and programs requiring stringent security measures. The initial benefit of NIST compliance is that it helps to ensure an organization's infrastructure is secure. NIST also lays the foundational protocol for companies to follow when achieving compliance with specific regulations such as HIPAA or FISMA. It's important to keep in mind, however, that complying with NIST is not a complete assurance that your data is secure. That's why NIST guidelines begin by telling companies to inventory their cyber assets using a value-based approach, to find their most sensitive data and prioritize protection efforts around it.

CVE and CVSS

CVE stands for Common Vulnerabilities and Exposures. CVE is a glossary that classifies vulnerabilities. The glossary analyzes vulnerabilities and then uses the Common Vulnerability Scoring System (CVSS) to evaluate the threat level of a vulnerability. The CVE glossary is a project dedicated to tracking and cataloging vulnerabilities in consumer software and hardware. It is maintained by the MITRE Corporation. Once evaluated and identified, vulnerabilities are listed in the publicly available MITRE glossary. After listing, vulnerabilities are analyzed by the National Institute of Standards and Technology (NIST). All vulnerability and analysis information is listed on NIST's National Vulnerability Database (NVD). When a CVE vulnerability is made public, it is listed with its ID, a brief description of the issue, and any references containing additional information or reports. As new references or findings arise, this information is added to the entry.

The current version of CVSS is v3.1, shows how severe a vulnerability is scored:



Severity	Base Score
None	0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

STIG

Security Technical Implementation Guides (STIGs) are configuration standards developed by the Defense Information Systems Agency (DISA). They are designed to make device hardware and software as secure as possible, safeguarding the Department of Defense (DoD) IT network and systems. Hardening the configuration of IT solutions helps to mitigate vulnerabilities and lower the risk of cybersecurity incidents. The creation of a STIG will also be key to gaining approval for a product to be used within the network. For IT products deployed within DoD agencies. STIGs are the source of configuration guidance for network devices, software, databases, and operating systems. The aim is to lower the risk of cybersecurity threats, breaches, and intrusion by making the set-up of the network as secure as possible. Organizations that connect to DoD systems or networks must be STIG compliant. This applies to defense agencies, defense contractors that connect to DoD systems, and other federal agencies. STIG controls focus on being highly secure, which can impact functionality of software and applications. Vendor involvement in the development of a STIG means a balance of functionality and security. When an IT solution is no longer supported, the relevant guidance becomes a 'sunset STIG'. This means DISA is no longer actively updating the STIG, though the guidance is still available for legacy tools and software.

Compliance

IT compliance is the process of meeting a third party's requirements with the aim of enabling business operations in a particular market or aligning with laws or even with a particular customer. Often, these external rules ensure that a given organization can deal with complex needs. Sometimes, compliance requires an organization to go beyond what might be considered reasonably necessary. These objectives are critical to success because a lack of compliance will result in:

- At minimum, a loss of customer trust and damage to your reputation.
- At worst, legal, and financial ramifications that could result in your organization paying hefty fees or being blocked from working in a certain geography or market.
- Areas where compliance is a key business concern:
- Countries with data/privacy laws like GDPR, the California Consumer Privacy Act, and more
- Markets with heavy regulations, such as healthcare or finance
- Clients with high confidentiality standards

These areas almost always demand a high level of compliance. Importantly, IT compliance can apply in domains other than IT security. Complying with contract terms, for example, might be about how available or reliable your services are, not only if they're secure.

When is compliance necessary?

Complying with certain regulations depends on many factors:

HIPAA is a U.S. law that defines how the healthcare industry protects and shares personal health information.

SOX is a financial regulation in the U.S. that applies to a broad spectrum of industries.

Payment Card Industry Data Security Standards (PCI-DSS) are a group of security regulations that protect consumer privacy when personal credit card information is transmitted, stored, and processed by businesses.

ISO 27001, is a standard that companies can opt into by aligning with these InfoSec standards.

Other standards you must comply might not be law or opt-in—some might originate directly with your customers. A high-profile client may require the business to implement very strict security controls to award their contract.

Compliance & GRC

Compliance is only one section of a greater scheme of ensuring an organization is compliant with industry, government, or other regulations. These are summed up in the acronym GRC.

Governance. Before compliance is possible, organizations need to make plans that are directed and controlled. Setting direction, monitoring developments, and evaluating outcomes are all key to effective governance.

Risk. Danger is everywhere and it needs to be recognized. Compliance needs for risks to be identified, analyzed, and controlled as much as is possible.

Compliance. When appropriately governed and risk-managed, an organization can evaluate its compliance. Standards are not just set but evaluated and managed at every step.