Google Cybersecurity Notes

Foundations of Cybersecurity

1 Common Attacks and Their Effectiveness

Early cyberattacks such as the LoveLetter (ILOVEYOU) virus and the Morris Worm played a significant role in shaping the cybersecurity industry. One major outcome of these attacks was the creation of Computer Security Incident Response Teams (CSIRTs). Understanding common attack methods and evolving threat actor techniques is essential for protecting organizations and individuals.

1.1 Phishing

Definition

Phishing is the use of digital communication to trick individuals into revealing sensitive information or deploying malicious software.

1.1.1 Common Types of Phishing

- Business Email Compromise (BEC): Emails impersonating trusted sources to request sensitive or financial information.
- Spear Phishing: Targeted phishing attacks aimed at specific individuals or groups.
- Whaling: Spear phishing attacks targeting senior executives.
- Vishing: Voice-based phishing using phone calls or voice messages.
- Smishing: SMS-based phishing using text messages.

1.2 Malware

Definition

Malware is software designed to damage devices, systems, or networks, often for financial or intelligence gain.

1.2.1 Common Types of Malware

- Viruses: Require user interaction and embed themselves into files to spread.
- Worms: Self-replicate and spread automatically across networks.
- Ransomware: Encrypts data and demands payment for recovery.
- Spyware: Collects sensitive information without user consent.

1.3 Social Engineering

Definition

Social engineering is a manipulation technique that exploits human trust and error to gain unauthorized access or information.

1.3.1 Why Social Engineering Is Effective

- Authority
- Intimidation
- Social proof
- Scarcity
- Familiarity
- Trust
- Urgency

Key Takeaways

- Phishing, malware, and social engineering are common cyberattack methods.
- Social engineering is effective due to psychological manipulation.
- Understanding attack techniques improves defense strategies.

2 Determine the Type of Attack

Cybersecurity attacks can be categorized using the Certified Information Systems Security Professional (CISSP) security domains. These domains help organize a security analyst's responsibilities and provide a structured approach to managing risk. Understanding how different attacks align with these domains improves an organization's ability to prevent and respond to security incidents.

2.1 Password Attacks

Definition

A password attack is an attempt to gain unauthorized access to password-protected devices, systems, networks, or data.

2.1.1 Common Forms

- Brute Force Attack: Attempts all possible password combinations until the correct one is found.
- Rainbow Table Attack: Uses precomputed tables of hashed passwords to speed up password cracking.

Related CISSP Domain: Communication and Network Security

2.2 Social Engineering Attacks

Definition

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.

2.2.1 Common Forms

- Phishing
- Smishing
- Vishing
- Spear phishing
- Whaling
- Social media phishing
- Business Email Compromise (BEC)
- Watering hole attacks

- USB (Universal Serial Bus) baiting
- Physical social engineering

Related CISSP Domain: Security and Risk Management

2.3 Physical Attacks

Definition

A physical attack is a security incident that impacts both digital systems and the physical environments in which those systems operate.

2.3.1 Common Forms

- Malicious USB cables
- Malicious flash drives
- Card cloning and skimming

Related CISSP Domain: Asset Security

2.4 Adversarial Artificial Intelligence

Definition

Adversarial artificial intelligence is a technique that manipulates artificial intelligence and machine learning systems to conduct attacks more efficiently.

Related CISSP Domains:

- Communication and Network Security
- Identity and Access Management

2.5 Supply-Chain Attacks

Definition

A supply-chain attack targets systems, applications, hardware, or software by exploiting vulnerabilities introduced through third-party vendors or services.

Because most products and services involve multiple third parties, security breaches can occur at any point in the supply chain. These attacks

are particularly costly because they can impact multiple organizations and individuals simultaneously.

Related CISSP Domains:

- Security and Risk Management
- Security Architecture and Engineering
- Security Operations

2.6 Cryptographic Attacks

Definition

A cryptographic attack targets secure communication mechanisms between a sender and an intended recipient.

2.6.1 Common Forms

- Birthday attacks
- Collision attacks
- Downgrade attacks

Related CISSP Domain: Communication and Network Security

Key Takeaways

- Cyberattacks can span one or more CISSP security domains.
- Data breaches range from simple to highly complex incidents.
- Understanding attack classification strengthens prevention and response strategies.
- The attack types discussed represent only a subset of known cybersecurity threats.

3 Understand Attackers

A threat actor is any individual or group that presents a security risk to an organization or its assets. Understanding the different types of threat actors, along with their motivations and intentions, helps security professionals anticipate attacks and design effective defenses.

3.1 Threat Actor Types

3.1.1 Advanced Persistent Threats (APTs)

Definition

Advanced Persistent Threats (APTs) are highly skilled individuals or groups that gain unauthorized access to networks and remain undetected for extended periods of time.

APTs typically conduct extensive research on their targets, such as large corporations or government entities.

Common motivations include:

- Damaging critical infrastructure, such as power grids or natural resources
- Gaining access to intellectual property, including trade secrets and patents

3.1.2 Insider Threats

Definition

Insider threats are individuals who abuse their authorized access to systems or data in ways that harm an organization.

Common motivations include:

- Sabotage
- Corruption
- Espionage
- Unauthorized data access or leaks

3.1.3 Hacktivists

Definition

Hacktivists are threat actors motivated by political, ideological, or social agendas who use digital technology to achieve their goals.

Common objectives include:

- Demonstrations and protests
- Propaganda dissemination
- Social or political change campaigns
- Gaining public attention or fame

3.2 Hacker Types

Definition

A hacker is any person who uses computers to gain access to systems, networks, or data. Hackers may have varying skill levels and motivations.

3.2.1 Primary Hacker Categories

- Authorized (Ethical) Hackers: Follow legal and ethical guidelines to evaluate organizational risk and improve security. Their goal is to protect systems and users from malicious threats.
- Semi-Authorized Hackers: Often considered security researchers. They identify vulnerabilities but do not exploit them for personal gain.
- Unauthorized (Unethical) Hackers: Malicious actors who violate laws and ethical standards to steal, exploit, or sell confidential data, usually for financial gain.

Note: Many hackers may fall into more than one category depending on context and intent.

3.2.2 Other Hacker Profiles

- New and Unskilled Threat Actors: Often motivated by learning, revenge, or opportunity. They commonly rely on existing malware, scripts, and publicly available tools.
- Contract Hackers: Individuals hired to perform hacking tasks. Their work may be legal or illegal depending on the nature of the contract.

- Vigilante Hackers: Hackers who believe their actions help protect systems or society by targeting unethical hackers.

Key Takeaways

- Threat actors are defined by malicious intent.
- Hackers are defined by technical skill and motivation.
- Understanding attacker motivations improves detection, prevention, and response strategies.
- Different threat actors require different defensive approaches.

4 Controls, Frameworks, and Compliance

Security frameworks, controls, and compliance regulations work together to help organizations manage risk and protect information systems. Security operates within a continuous security lifecycle, which consists of evolving policies, standards, and processes designed to address emerging threats and vulnerabilities.

4.1 Relationship Between Controls, Frameworks, and Compliance

Definition

The Confidentiality, Integrity, and Availability (CIA) triad is a model used to evaluate and manage risk when designing systems and security policies.

The CIA triad represents three foundational principles used by cybersecurity professionals to establish appropriate security controls that mitigate threats, risks, and vulnerabilities.

- Confidentiality: Ensuring information is accessible only to authorized individuals.
- Integrity: Maintaining the accuracy and reliability of data.
- Availability: Ensuring systems and data are accessible when needed.

4.1.1 Security Controls

Definition

Security controls are safeguards designed to reduce or mitigate specific security risks.

Controls are implemented alongside security frameworks to ensure that security goals are achieved and that regulatory compliance requirements are met.

4.1.2 Security Frameworks

Definition

Security frameworks are structured guidelines used to build and manage security programs that protect data and privacy.

Security frameworks generally consist of four core components:

- Identifying and documenting security goals
- Establishing guidelines to achieve those goals
- Implementing strong security processes
- Monitoring performance and communicating results

4.1.3 Compliance

Definition

Compliance is the process of adhering to internal standards and external laws or regulations.

Higher alignment with compliance requirements generally results in lower organizational risk.

4.2 Key Controls, Frameworks, and Compliance Standards

4.2.1 National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is a U.S.-based agency that develops voluntary frameworks used worldwide to manage cybersecurity risk.

Common NIST frameworks include:

- NIST Cybersecurity Framework (CSF)
- NIST Risk Management Framework (RMF)

Note: Specifications and guidelines may vary depending on the type of organization.

4.2.2 Federal Energy Regulatory Commission – North American Electric Reliability Corporation (FERC–NERC)

FERC–NERC regulations apply to organizations involved in electricity generation, transmission, or the North American power grid. These organizations are legally required to:

- Prepare for and mitigate cybersecurity incidents
- Report incidents that could impact the power grid
- Adhere to Critical Infrastructure Protection (CIP) Reliability Standards

4.2.3 Federal Risk and Authorization Management Program (FedRAMP®)

FedRAMP is a U.S. federal program that standardizes security assessment, authorization, monitoring, and incident handling for cloud services. Its goal is to ensure consistency across government agencies and cloud service providers.

4.2.4 Center for Internet Security (CIS®)

CIS is a nonprofit organization that provides actionable security controls to help organizations defend systems and networks against attacks. CIS controls also guide security professionals during incident response.

4.2.5 General Data Protection Regulation (GDPR)

GDPR is a European Union regulation that protects the personal data and privacy rights of E.U. residents, regardless of where the data is processed.

Key requirements include:

- Transparency about data collection and usage
- Notification of affected individuals within 72 hours of a breach
- Enforcement through financial penalties for noncompliance

4.2.6 Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an international standard that ensures secure handling of credit card data. Its primary objective is to reduce credit card fraud by enforcing secure storage, processing, and transmission practices.

4.2.7 Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a U.S. federal law enacted in 1996 to protect patients' health information.

HIPAA is governed by three rules:

- Privacy
- Security
- Breach notification

Organizations that store Protected Health Information (PHI) are legally required to notify patients in the event of a data breach. Exposure of PHI can lead to identity theft and insurance fraud.

Security professionals must also understand HITRUST®, a framework that helps organizations meet HIPAA compliance requirements.

4.2.8 International Organization for Standardization (ISO)

ISO develops international standards for technology, manufacturing, and management systems. These standards help organizations improve processes, efficiency, and service quality across borders.

4.2.9 System and Organization Controls (SOC 1 and SOC 2)

Developed by the American Institute of Certified Public Accountants (AICPA), SOC reports evaluate an organization's internal controls and risk posture.

SOC reports assess access controls at multiple organizational levels, including:

- Associates
- Supervisors
- Managers
- Executives
- Vendors

They address confidentiality, integrity, availability, privacy, and overall data security. Control failures in these areas can result in fraud.

Key Takeaways

- Controls, frameworks, and compliance work together to manage risk.
- The CIA triad forms the foundation of security decision-making.
- Compliance requirements vary by industry and geography.
- Regulations and standards are frequently updated and must be continuously reviewed.

5 Ethical Concepts That Guide Cybersecurity Decisions

Security ethics are guidelines that help cybersecurity professionals make appropriate, lawful, and unbiased decisions. Acting ethically requires maintaining confidentiality, protecting private data, and responding to security incidents in a way that minimizes harm. A strong ethical foundation enables security professionals to navigate evolving threat actor tactics while protecting organizations and individuals.

5.1 Ethical Concerns and Laws Related to Counterattacks

5.1.1 United States Standpoint on Counterattacks

In the United States, deploying a counterattack against a threat actor is illegal under laws such as the Computer Fraud and Abuse Act (1986) and the Cybersecurity Information Sharing Act (2015). Security professionals are permitted to defend systems but not retaliate.

Counterattacks are considered acts of vigilantism, meaning individuals attempt to stop criminal activity without legal authority. Because threat actors are criminals, counterattacks can escalate situations and cause additional damage.

If the attacker is a state-sponsored or politically motivated actor, counterattacks can also lead to serious international consequences. For these reasons, only authorized federal government employees or military personnel are permitted to conduct counterattacks in the U.S.

5.1.2 International Standpoint on Counterattacks

The International Court of Justice (ICJ) states that a counterattack may be permissible only if all of the following conditions are met:

- The counterattack affects only the original attacker
- The counterattack is a direct communication requesting the attack to stop
- The action does not escalate the situation
- The effects of the counterattack can be reversed

In practice, organizations rarely counterattack because these conditions are difficult to measure and control. Legal uncertainty and the risk of unintended consequences often result in worse outcomes, especially when actions are taken by inexperienced professionals.

For additional international guidance, ethical discussions are outlined in the Tallinn Manual, which is updated regularly.

5.2 Ethical Principles and Methodologies

Because counterattacks are generally illegal or discouraged, the cybersecurity field relies on ethical frameworks and controls—such as the Confidentiality, Integrity, and Availability (CIA) triad—to guide decision-making related to privacy, data protection, and legal compliance.

5.2.1 Confidentiality

Definition

Confidentiality ensures that only authorized individuals can access specific systems, assets, or data.

From an ethical standpoint, confidentiality requires a high level of respect for privacy and the protection of sensitive information.

5.2.2 Privacy Protection

Definition

Privacy protection involves safeguarding personal information from unauthorized access, use, or disclosure.

Two important categories of personal data include:

- Personally Identifiable Information (PII): Information used to identify an individual, such as names or phone numbers.
- Sensitive Personally Identifiable Information (SPII): Data subject to stricter protection requirements, including social security numbers and credit card numbers.

Security professionals have an ethical obligation to protect PII and SPII by identifying vulnerabilities, managing organizational risk, and aligning security practices with business objectives.

5.2.3 Laws and Professional Responsibility

Definition

Laws are rules enforced by governing authorities that define acceptable and unacceptable behavior.

Cybersecurity professionals have an ethical responsibility to protect their organization, its infrastructure, and the individuals associated with it. To fulfill this responsibility, professionals must:

- Remain unbiased and act honestly and responsibly
- Respect and comply with applicable laws
- Be transparent, fair, and evidence-driven
- Stay engaged and committed to their work
- Continuously improve skills and knowledge

5.2.4 Ethics in Practice: HIPAA Example

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. federal law that protects patients' Protected Health Information (PHI). HIPAA prohibits sharing patient data without consent and requires organizations to notify individuals if their healthcare data is breached.

Security professionals play a key role in ensuring that organizations meet both their legal and ethical obligations when handling sensitive health information.

Key Takeaways

- Ethics guide cybersecurity decision-making and professional conduct.
- Counterattacks are generally illegal and discouraged.
- Confidentiality and privacy are core ethical responsibilities.
- Legal compliance and ethical behavior must work together.
- Strong ethics help protect organizations and individuals from harm.

6 Tools for Protecting Business Operations

Security analysts rely on a combination of technical skills and tools to identify, assess, and mitigate risks to business operations. While the specific tools available may vary by organization, familiarity with industry-standard tools is essential for entry-level security analysts and enables them to adapt quickly to new environments.

6.1 An Entry-Level Analyst's Toolkit

Each organization provides a toolkit based on its security requirements, infrastructure, and risk profile. As a future security analyst, it is important to understand how common tools function and how similar tools may be applied in different workplaces.

6.2 Security Information and Event Management (SIEM) Tools

Definition

A Security Information and Event Management (SIEM) tool is an application that collects, correlates, and analyzes log data to monitor critical activities across an organization.

Logs are records of events generated by systems, applications, and network devices. Manually reviewing large volumes of log data can be time-consuming and inefficient. SIEM tools reduce this workload by automatically filtering data and generating alerts for specific threats, risks, and vulnerabilities.

SIEM tools typically provide dashboards that visually organize data into categories, allowing analysts to focus on relevant events and trends. Different SIEM platforms offer varying dashboard views depending on user roles and access permissions.

SIEM solutions can be deployed using different hosting models:

- On-premise: Installed and managed within an organization's own infrastructure.
- Cloud-hosted: Managed by a service provider and accessed remotely.

Organizations may choose a cloud-hosted SIEM when ease of setup, maintenance, and limited in-house expertise are key considerations.

6.3 Network Protocol Analyzers (Packet Sniffers)

Definition

A network protocol analyzer, also known as a packet sniffer, is a tool used to capture and analyze network traffic.

These tools record data packets transmitted across a network, enabling analysts to examine communication patterns, detect anomalies, and identify potential security incidents. Packet sniffers are commonly used during investigations involving suspicious network activity.

6.4 Playbooks

Definition

A playbook is a documented set of procedures that guides analysts through specific operational or security-related tasks.

Organizations maintain multiple playbooks to standardize responses to security incidents and ensure that analysts follow approved processes. Although playbooks vary across organizations, they share a common goal: to provide clear, repeatable steps for handling incidents effectively.

6.4.1 Forensic Investigation Playbooks

During a forensic investigation, analysts often rely on specialized playbooks to ensure evidence is handled correctly and remains admissible.

Chain of Custody Playbook Chain of custody is the process of documenting the possession, handling, and movement of evidence throughout an incident's lifecycle. Analysts must record:

- Who collected the evidence
- What the evidence is
- Where the evidence is stored
- Why the evidence was collected

Evidence must be secured, tracked, and documented every time it is moved to ensure accountability and integrity.

Protecting and Preserving Evidence Playbook Protecting and preserving evidence involves handling fragile and volatile digital data correctly. Analysts follow the order of volatility, which prioritizes data that may be lost if a system powers off.

Improper handling of digital evidence can compromise its integrity and render it unusable. For this reason, analysts preserve evidence by creating copies and conducting investigations on those copies rather than the original data.

Key Takeaways

- Security analysts use a variety of tools to mitigate business risk.
- SIEM tools help monitor and analyze large volumes of log data.
- Packet sniffers enable detailed network traffic analysis.
- Playbooks standardize incident response and forensic procedures.
- Proper evidence handling is critical in forensic investigations.

7 Use Tools to Protect Business Operations

Cybersecurity professionals rely on programming, operating systems, and specialized tools to protect organizations and the people they serve. Understanding how these tools work enables entry-level analysts to detect threats, reduce risk, and respond to security incidents more effectively.

7.1 Tools and Their Purposes

7.1.1 Programming

Definition

Programming is the process of creating a set of instructions that a computer follows to perform specific tasks.

Security analysts commonly use programming languages such as Python to support automation. Automation reduces manual effort when performing repetitive tasks and helps minimize the risk of human error.

Another important programming language used by analysts is Structured Query Language (SQL). SQL is used to create, manage, and retrieve information from databases.

Definition

A database is an organized collection of data that may contain millions of individual data points.

7.1.2 Operating Systems

Definition

An operating system (OS) is the interface between computer hardware and the user.

Common operating systems include Linux, macOS, and Windows. Each operating system provides different functionality and user experiences.

Linux is an open-source operating system, meaning its source code is publicly available and can be modified by contributors. Although Linux is not a programming language, it relies heavily on the use of commands through a command-line interface (CLI).

Definition

A command-line interface (CLI) is a text-based interface that allows users to interact with the operating system by entering commands.

7.1.3 Web Vulnerabilities

Definition

A web vulnerability is a flaw in a web application that can be exploited by threat actors to gain unauthorized access, steal data, or deploy malware.

Security professionals stay informed about critical web vulnerabilities by referencing the OWASP Top 10, which highlights the most common and severe risks to web applications.

7.1.4 Antivirus Software

Definition

Antivirus software, also known as anti-malware, is used to prevent, detect, and remove malicious software from systems.

Depending on the implementation, antivirus software may scan system memory, files, and processes to identify patterns associated with known malware.

7.1.5 Intrusion Detection Systems (IDS)

Definition

An intrusion detection system (IDS) monitors system and network activity and generates alerts when potential intrusions are detected.

IDS tools analyze network packets, which are small units of data transmitted across a network. This analysis helps identify threats such as unauthorized access, data theft, or malicious activity.

7.1.6 Encryption

Definition

Encryption is the process of converting readable data (plaintext) into an encoded format (ciphertext) to prevent unauthorized access.

The primary purpose of encryption is to ensure the confidentiality of data. Ciphertext is difficult to decode without the appropriate cryptographic key.

Note: Encoding and encryption serve different purposes. Encoding uses public conversion algorithms to support data compatibility, whereas encryption is designed to secure data.

7.1.7 Penetration Testing

Definition

Penetration testing, or pen testing, is a simulated cyberattack used to identify vulnerabilities in systems, networks, applications, and processes.

Penetration testing evaluates both internal and external threats and provides a comprehensive assessment of organizational risk.

Key Takeaways

- Programming and automation reduce manual effort and human error.
- Operating systems form the foundation of system interaction.
- Web vulnerabilities expose applications to exploitation.
- Antivirus and IDS tools help detect and prevent attacks.
- Encryption protects the confidentiality of sensitive data.
- Penetration testing identifies weaknesses before attackers do.
- Familiarity with tools increases an analyst's value to an organization.

Play It Safe: Manage Security Risks

8 Security Domains Cybersecurity Analysts Need to Know

Cybersecurity analysts can specialize in different areas of the field. One way to understand these areas is through the Certified Information Systems Security Professional (CISSP) security domains. These domains organize the responsibilities of security professionals and help establish a structured approach to risk management.

8.1 Domain 1: Security and Risk Management

Definition

Security posture refers to an organization's ability to defend critical assets and data while adapting to changing threats and risks.

The security and risk management domain focuses on establishing and maintaining an organization's overall security posture. Key elements of this domain include:

- Security goals and objectives
- Risk mitigation processes
- Compliance requirements
- Business continuity planning
- Legal and regulatory obligations
- Professional and organizational ethics

This domain also includes Information Security (InfoSec), which refers to processes designed to protect information. Common InfoSec design processes include:

- Incident response
- Vulnerability management
- Application security
- Cloud security
- Infrastructure security

Organizations may adjust how they handle data such as Personally Identifiable Information (PII) to comply with regulations like the General Data Protection Regulation (GDPR).

8.2 Domain 2: Asset Security

Definition

Asset security involves managing and protecting physical and digital assets throughout their lifecycle.

This domain covers the storage, maintenance, retention, and destruction of organizational data. Because asset loss or theft increases risk, security analysts must track assets and assess their associated risk.

Key responsibilities include:

- Conducting security impact analyses
- Managing data exposure
- Establishing recovery and backup plans

8.3 Domain 3: Security Architecture and Engineering

This domain focuses on designing and implementing secure systems and processes to protect organizational data and assets. Security architects and engineers are primarily responsible for these activities.

A central concept in this domain is shared responsibility, meaning all individuals involved in system design contribute to reducing risk.

Important design principles include:

- Threat modeling
- Least privilege
- Defense in depth
- Fail securely
- Separation of duties
- Keep it simple
- Zero trust
- Trust but verify

An example is using a SIEM tool to monitor unusual login or user activity that may indicate unauthorized access attempts.

8.4 Domain 4: Communication and Network Security

This domain addresses securing physical networks, wireless communications, and cloud-based connections.

Organizations with remote, hybrid, or on-site work environments must ensure secure access to internal networks. Network security controls, such as restricted network access, help protect data when employees work remotely or travel.

8.5 Domain 5: Identity and Access Management

Definition

Identity and Access Management (IAM) ensures that user identities are authenticated and that access to systems and data is authorized.

IAM applies the principle of least privilege, granting users only the minimum access required to complete their tasks.

For example, customer service staff may be granted temporary access to a customer's phone number while resolving an issue, with access removed once the task is complete.

8.6 Domain 6: Security Assessment and Testing

This domain focuses on identifying and reducing risks, threats, and vulnerabilities through evaluation and testing.

Organizations may conduct:

- Security control testing
- Data collection and analysis
- Security audits

Penetration testers, or pen testers, are often employed to identify vulnerabilities before threat actors can exploit them. Analysts may also audit user permissions to ensure appropriate access levels.

8.7 Domain 7: Security Operations

The security operations domain focuses on detecting, responding to, and recovering from security incidents.

Common activities and tools include:

- Training and security awareness
- Reporting and documentation
- Intrusion detection and prevention
- SIEM tools and log management
- Incident management and playbooks
- Post-breach forensics
- Lessons learned and process improvement

Security operations teams respond to active threats and work to protect sensitive data from unauthorized access.

8.8 Domain 8: Software Development Security

This domain emphasizes secure coding practices throughout the software development life cycle.

Security must be integrated into every phase, including:

- Design
- Development
- Testing
- Deployment and release

Application security testing helps identify vulnerabilities early. Quality assurance teams and pen testers ensure software meets security and performance standards.

For example, an entry-level analyst may be responsible for verifying that encryption is properly configured on a medical device that stores patient data.

Key Takeaways

- The eight CISSP domains organize cybersecurity responsibilities.
- Each domain addresses a specific aspect of security and risk.
- InfoSec and least privilege are foundational concepts.
- Understanding these domains helps analysts navigate the field of cybersecurity effectively.

9 Manage Common Threats, Risks, and Vulnerabilities

Cybersecurity focuses on protecting organizations and individuals from threats, risks, and vulnerabilities. Understanding the current threat landscape enables organizations to design policies and processes that help prevent, detect, and mitigate security issues. Effective risk management prepares security professionals to defend assets against evolving threat actor tactics and techniques.

9.1 Risk Management

A primary objective of organizations is to protect their assets. An asset is any item perceived as having value to an organization and may be physical or digital.

9.1.1 Examples of Digital Assets

- Social Security Numbers (SSNs) or national identification numbers
- Dates of birth
- Bank account numbers
- Mailing addresses

9.1.2 Examples of Physical Assets

- Payment kiosks
- Servers
- Desktop computers
- Office spaces

9.1.3 Common Risk Management Strategies

Organizations use several strategies to manage risk:

- Acceptance: Accepting risk to avoid disrupting business continuity
- Avoidance: Eliminating activities that introduce risk
- Transference: Shifting risk to a third party, such as through insurance
- Mitigation: Reducing the likelihood or impact of known risks

Risk management processes are often guided by established frameworks, such as the NIST Risk Management Framework (RMF) and HITRUST.

9.2 Threats

Definition

A threat is any circumstance or event that can negatively impact an organization's assets.

Security analysts help protect assets from both internal and external threats. Common threats include:

- Insider threats: Employees or vendors abusing authorized access
- Advanced Persistent Threats (APTs): Threat actors maintaining long-term unauthorized access to systems

9.3 Risks

Definition

A risk is anything that can impact the confidentiality, integrity, or availability of an asset.

Risk is commonly evaluated based on the likelihood that a threat will occur. Factors influencing organizational risk include:

- External risk: Threats originating outside the organization
- Internal risk: Current or former employees, vendors, or partners
- Legacy systems: Outdated systems that remain connected and vulnerable
- Multiparty risk: Exposure resulting from third-party access
- Software compliance and licensing: Unpatched or noncompliant software

Resources such as NIST provide extensive lists of cybersecurity risks. Additionally, the OWASP Top 10 highlights the most critical security risks to web applications.

Note: Recent OWASP updates emphasize emerging risks such as insecure design, software and data integrity failures, and server-side request forgery, demonstrating the evolving nature of cybersecurity.

9.4 Vulnerabilities

Definition

A vulnerability is a weakness that can be exploited by a threat actor.

Organizations must regularly identify and address vulnerabilities within their systems. Examples include:

- ProxyLogon: A pre-authentication vulnerability affecting Microsoft Exchange
- ZeroLogon: A flaw in Microsoft's Netlogon authentication protocol
- Log4Shell: A vulnerability allowing remote code execution in Java applications
- PetitPotam: An NTLM-based attack enabling forced authentication
- Security logging and monitoring failures: Insufficient detection capabilities
- Server-side request forgery (SSRF): Manipulation of server-side requests

9.4.1 Vulnerability Management

Vulnerability management involves continuously monitoring systems to identify and mitigate weaknesses. Even when patches are available, failure to apply updates can leave systems exposed to intrusion.

Timely identification and remediation of vulnerabilities reduce an organization's exposure to risk.

To explore vulnerabilities in greater detail, security professionals refer to resources such as the NIST National Vulnerability Database and the CISA Known Exploited Vulnerabilities Catalog.

Key Takeaways

- Risk management protects valuable organizational assets.
- Threats, risks, and vulnerabilities are closely related concepts.
- Established frameworks support consistent risk management.
- Vulnerability management requires continuous monitoring and patching.
- Staying informed about evolving threats is critical in cybersecurity.

10 The Relationship Between Frameworks and Controls

Organizations rely on security frameworks and controls to protect against threats, risks, and vulnerabilities. Frameworks such as the NIST Risk Management Framework (RMF), the NIST Cybersecurity Framework (CSF), and the Confidentiality, Integrity, and Availability (CIA) triad provide structured guidance for managing cybersecurity risk. Controls are implemented alongside these frameworks to reduce risk and strengthen an organization's overall security posture.

10.1 Frameworks and Controls

Definition

Security frameworks are guidelines used to build and manage security programs that mitigate risk to data and privacy.

Frameworks help organizations align security practices with compliance laws and regulations. For example, organizations in the healthcare industry use security frameworks to support compliance with the Health Insurance Portability and Accountability Act (HIPAA), which requires the protection of patient information.

Definition

Security controls are safeguards designed to reduce specific security risks.

Controls are the practical measures organizations implement to lower the likelihood and impact of threats. For example, requiring multi-factor authentication (MFA) for patient portals is a control that helps healthcare organizations protect sensitive medical data and remain HIPAA-compliant.

10.2 Specific Frameworks

10.2.1 Cyber Threat Framework (CTF)

Definition

The Cyber Threat Framework (CTF) provides a common language for describing and communicating information about cyber threat activity.

Developed by the U.S. government, the CTF enables cybersecurity professionals to consistently analyze and share information about threat actors and their tactics and techniques. This shared language improves collaboration and strengthens an organization's ability to respond to the evolving threat landscape.

10.2.2 ISO/IEC 27001

Definition

ISO/IEC 27001 is an internationally recognized framework for managing information security.

The ISO/IEC 27001 standard is part of the ISO 27000 family and applies to organizations of all sizes and sectors. It provides requirements for an Information Security Management System (ISMS), along with best practices and recommended controls to manage risk.

Although ISO/IEC 27001 does not mandate specific controls, it offers a collection of controls that organizations can select to improve their security posture and protect assets such as:

- Financial information
- Intellectual property
- Employee data
- Third-party information

10.3 Security Controls

Controls are implemented alongside frameworks to prevent, detect, or correct security issues. Controls generally fall into three categories: physical, technical, and administrative.

10.3.1 Physical Controls

- Gates, fences, and locks
- Security guards
- Closed-circuit television (CCTV) and surveillance cameras
- Motion detectors
- Access cards or badges for office entry

10.3.2 Technical Controls

- Firewalls
- Multi-factor authentication (MFA)
- Antivirus and anti-malware software

10.3.3 Administrative Controls

- Separation of duties
- Authorization processes
- Asset classification policies

Additional guidance on controls—particularly those used to protect health-related assets—can be found in resources such as the U.S. Department of Health and Human Services Physical Access Control guidance.

Key Takeaways

- Security frameworks provide structure for managing cybersecurity risk.
- Controls are specific measures used to reduce threats and vulnerabilities.
- Frameworks and controls work together to establish security posture.
- Implementing frameworks and controls supports legal and regulatory compliance.
- Although often voluntary, their adoption is strongly recommended to protect critical assets.

11 Use the CIA Triad to Protect Organizations

The Confidentiality, Integrity, and Availability (CIA) triad is a core cybersecurity model used to evaluate and manage risk. Cybersecurity analysts apply the CIA triad when designing systems, creating policies, and responding to incidents to help organizations maintain a strong security posture.

11.1 The CIA Triad for Analysts

Definition

The CIA triad is a model that guides how organizations consider risk when designing systems and security policies.

The model is built on three foundational principles:

- Confidentiality
- Integrity
- Availability

Designing systems and policies with these principles in mind helps organizations maintain an acceptable level of risk and establish a strong security posture, which is the ability to protect critical assets and adapt to change.

11.2 Confidentiality

Definition

Confidentiality ensures that only authorized users can access specific assets or data.

Organizations enhance confidentiality by implementing access control mechanisms and security design principles such as the principle of least privilege. This principle limits user access to only the information required to perform job-related tasks.

Restricting access reduces the likelihood of unauthorized data exposure and helps protect sensitive information.

11.3 Integrity

Definition

Integrity ensures that data is accurate, authentic, and reliable.

Maintaining data integrity requires protocols that verify data has not been altered without authorization. One method used to support integrity is cryptography, which transforms data so unauthorized parties cannot read or modify it.

Encryption is a common integrity control that converts readable data into an encoded format. For example, encrypting messages on an internal communication platform helps ensure that data cannot be tampered with during transmission.

11.4 Availability

Definition

Availability ensures that authorized users can access data and systems when needed.

Availability works alongside confidentiality to ensure systems remain usable without exposing sensitive information. In practice, this may include enabling secure remote access for employees while still limiting what data they can view.

Access levels are typically based on job roles. For example, an employee in the accounting department may have access to financial systems but not to data related to active development projects.

Key Takeaways

- The CIA triad is fundamental to cybersecurity decision-making.
- Confidentiality limits access to authorized users.
- Integrity ensures data remains accurate and trustworthy.
- Availability ensures systems and data are accessible when needed.
- Applying the CIA triad helps establish and maintain a strong security posture.

12 More About OWASP Security Principles

Cybersecurity analysts use security frameworks, controls, and principles to reduce organizational risk and protect data. The Open Worldwide Application Security Project (OWASP) provides widely accepted security principles that guide secure system and application design. These principles are applied daily by analysts when reviewing logs, monitoring SIEM dashboards, and using vulnerability scanning tools.

12.1 Security Principles in Practice

Security principles are embedded in everyday cybersecurity tasks. Whether an analyst is investigating alerts, assessing vulnerabilities, or reviewing system configurations, these principles help guide secure and effective decision-making.

Previously introduced OWASP security principles include:

- Minimize attack surface area: Reduce the number of potential entry points a threat actor could exploit.
- Principle of least privilege: Grant users only the minimum access required to perform their tasks.
- Defense in depth: Use multiple layers of security controls to mitigate threats.
- Separation of duties: Divide critical actions among multiple individuals to reduce risk.
- Keep security simple: Avoid unnecessary complexity, as complexity increases the likelihood of security failures.
- Fix security issues correctly: Identify root causes, contain impact, remediate vulnerabilities, and verify fixes through testing.

12.2 Additional OWASP Security Principles

In addition to the principles listed above, OWASP defines several other important security principles that analysts use to protect systems and users.

12.2.1 Establish Secure Defaults

Definition

Secure defaults mean that an application's most secure configuration is enabled by default.

Users should not need to take additional steps to make a system secure. Instead, extra effort should be required to weaken security settings.

12.2.2 Fail Securely

Definition

Fail securely means that when a system or control fails, it defaults to its most secure state.

For example, if a firewall fails, it should block all connections rather than allow unrestricted access.

12.2.3 Don't Trust Services

Definition

Organizations should not automatically trust third-party services or systems.

Third-party vendors may operate under different security standards. Organizations must validate external data before using or sharing it. For instance, an airline should verify customer reward balances received from a third-party vendor before presenting them to customers.

12.2.4 Avoid Security by Obscurity

Definition

Security should not rely on keeping system details or source code secret.

According to OWASP, application security should be based on strong design principles such as:

- Robust password policies
- Defense in depth
- Transaction and usage limits

- Secure network architecture
- Fraud detection and auditing controls

Relying solely on secrecy increases risk and does not provide reliable protection.

Key Takeaways

- OWASP security principles guide secure system and application design.
- Analysts apply these principles during daily security tasks.
- Secure defaults and fail-safe behavior reduce risk.
- Third-party services must be validated, not trusted.
- Strong security relies on design, not secrecy.

13 More About Security Audits

Security audits help organizations evaluate whether their security controls, policies, and procedures are effective and aligned with organizational goals and regulatory requirements. Audits play a critical role in maintaining a strong security posture and identifying areas for improvement.

13.1 Security Audits

Definition

A security audit is an independent review of an organization's security controls, policies, and procedures against a defined set of expectations.

Audits evaluate whether an organization meets:

- Internal criteria: Policies, procedures, and best practices
- External criteria: Laws, regulations, and compliance standards

Security audits also assess the effectiveness of existing security controls, which are safeguards designed to reduce specific security risks.

Audits support daily security operations by validating that monitoring activities—such as reviewing SIEM dashboards—are performed correctly. If issues are identified, a remediation process must be in place to address them.

13.2 Goals and Objectives of an Audit

The primary goal of a security audit is to ensure that an organization's information technology (IT) practices align with industry standards and organizational requirements.

Audit objectives include:

- Identifying security gaps and control failures
- Highlighting areas for remediation and improvement
- Providing clarity and direction for corrective actions

Audits also help organizations avoid penalties and fines from regulatory bodies. Audit frequency depends on local laws, federal regulations, and industry requirements.

13.3 Factors That Affect Audits

Several factors influence the type and scope of audits an organization conducts:

- Industry type
- Organization size
- Applicable government regulations
- Geographic location
- Business decisions to follow specific compliance standards

13.4 The Role of Frameworks and Controls in Audits

Security frameworks and controls play a critical role in audit readiness. Frameworks such as the NIST Cybersecurity Framework (CSF) and the ISO 27000 series help organizations prepare for internal and external audits.

When frameworks are implemented alongside appropriate controls, organizations can:

- Reduce audit preparation time
- Align with regulatory requirements
- Improve consistency in security practices

During an audit, three main categories of controls are reviewed:

- Administrative (or managerial) controls
- Technical controls
- Physical controls

13.5 Audit Checklist

Creating an audit checklist before conducting an audit ensures a structured and consistent review process.

13.5.1 Define the Audit Scope

The audit scope should:

- Identify assets to be assessed (e.g., firewalls, PII, physical security)
- Explain how the audit supports organizational goals
- Specify how frequently audits should occur
- Evaluate policies, procedures, and employee adherence

13.5.2 Complete a Risk Assessment

A risk assessment evaluates organizational risks related to:

- Budget constraints
- Security controls
- Internal processes
- External regulations and standards

13.5.3 Conduct the Audit

During the audit, analysts assess the security of assets defined in the scope and evaluate control effectiveness.

13.5.4 Create a Mitigation Plan

Definition

A mitigation plan is a strategy designed to reduce risk and minimize potential costs, penalties, or security impacts.

13.5.5 Communicate Results to Stakeholders

Audit results are documented in a report that includes:

- Identified risks and control gaps
- Recommended improvements
- Applicable compliance standards and regulations

13.6 Control Categories

Controls are grouped into three primary categories.

13.6.1 Administrative / Managerial Controls

These controls address the human component of cybersecurity and include policies and procedures that define responsibilities and data handling requirements.

Examples include:

- Least privilege
- Password policies
- Access control policies
- Account management policies

- Separation of duties
- Disaster recovery plans

13.6.2 Technical Controls

Technical controls use technology to protect systems and data.

Examples include:

- Firewalls
- Intrusion Detection and Prevention Systems (IDS/IPS)
- Antivirus software
- Encryption
- Backups
- Password management tools

13.6.3 Physical Controls

Physical controls limit unauthorized physical access to assets.

Examples include:

- Locks and locking cabinets
- Surveillance cameras (CCTV)
- Badge readers
- Adequate lighting
- Fire detection and prevention systems

13.7 Control Types

Controls can also be classified by their purpose:

- Preventative: Stop incidents before they occur
- Detective: Identify incidents in progress or after occurrence
- Corrective: Restore systems after an incident
- Deterrent: Discourage malicious activity

These control types work together to provide defense in depth.

Key Takeaways

- Security audits evaluate controls, policies, and procedures.
- Audits support compliance and risk reduction.
- Frameworks and controls improve audit readiness.
- Checklists ensure consistent and effective audits.
- Multiple control categories and types work together to protect assets.

14 The Future of SIEM Tools

Security Information and Event Management (SIEM) tools play a critical role in protecting organizational operations by monitoring and analyzing security-related data. As threat actor tactics and technologies evolve, SIEM tools are also changing to better support security teams and protect organizations and the people they serve.

14.1 Current SIEM Solutions

Definition

A Security Information and Event Management (SIEM) tool is an application that collects and analyzes log data to monitor critical activities within an organization.

SIEM tools provide real-time monitoring and tracking of security event logs generated by systems, applications, and network devices. This data is analyzed to identify potential threats, risks, and vulnerabilities.

Modern SIEM platforms offer multiple dashboard views that help security teams visualize and manage large volumes of organizational data. However, many current SIEM solutions still rely heavily on human interaction to investigate and interpret security events.

14.2 The Evolution of SIEM Tools

As cybersecurity environments grow more complex, organizations increasingly rely on cloud technologies. SIEM tools have evolved to support both cloud-hosted and cloud-native deployments.

14.2.1 Cloud-Hosted SIEM

Cloud-hosted SIEM tools are maintained and managed by vendors. The infrastructure required to operate these tools is handled by the service provider, and organizations access the SIEM through the internet.

This approach is well suited for organizations that prefer not to invest in building and maintaining their own infrastructure.

14.2.2 Cloud-Native SIEM

Cloud-native SIEM tools are also vendor-managed and accessed online, but they are specifically designed to take advantage of cloud computing

capabilities such as:

- High availability
- Scalability
- Flexibility

These tools are optimized for modern cloud environments and large-scale data processing.

14.3 Emerging Technologies and SIEM

The continued growth of interconnected devices—commonly referred to as the Internet of Things (IoT)—has expanded the cybersecurity attack surface. As the number of connected devices increases, so does the volume and diversity of data that SIEM tools must analyze.

Advancements in artificial intelligence (AI) and machine learning (ML) are expected to enhance SIEM capabilities by improving:

- Threat detection accuracy
- Recognition of threat-related patterns and terminology
- Dashboard visualization
- Data storage and analysis efficiency

14.4 Automation and SOAR Integration

Automation is becoming a key component of modern SIEM solutions. Security Orchestration, Automation, and Response (SOAR) refers to a collection of tools and workflows that automate responses to security events.

By integrating SIEM tools with SOAR platforms, organizations can:

- Respond more quickly to common security incidents
- Reduce reliance on manual intervention
- Free analysts to focus on complex and uncommon threats

Although automation significantly improves efficiency, not all incidents can be automated. Complex cases still require human expertise and judgment. Additionally, while interoperability between cybersecurity platforms is improving, full system-to-system integration remains an ongoing challenge.

Key Takeaways

- SIEM tools are essential for monitoring and analyzing security data.
- Cloud-hosted and cloud-native SIEM solutions are increasingly common.
- IoT growth expands the attack surface and data volume.
- AI and ML enhance SIEM detection and analysis capabilities.
- SOAR integration enables faster, automated incident response.
- Future SIEM tools will emphasize integration, automation, and scalability.

15 More About Cybersecurity Tools

Cybersecurity professionals rely on a wide range of tools to monitor, detect, and respond to potential threats, risks, and vulnerabilities. These tools may be open-source or proprietary, and each type plays an important role in modern security operations.

15.1 Open-Source Tools

Definition

Open-source tools are software applications whose source code is publicly available and can be used, modified, and distributed according to their license.

Open-source tools are often free to use and highly customizable. Because they are developed collaboratively by the public, these tools can be more secure and adaptable. Users can modify the software to meet specific needs, leading to the creation of new services and enhancements built on top of the original codebase.

Software engineers create open-source projects to improve software and make it widely accessible. In addition to the source code, training materials and documentation are often available, enabling users to learn from and contribute to the project.

15.2 Proprietary Tools

Definition

Proprietary tools are software products that are owned and controlled by an individual or organization.

Users typically pay licensing or subscription fees to access proprietary tools and related training. Only the owners of proprietary software can modify the source code, which means users must wait for vendor-issued updates and may be charged additional fees for new features.

Proprietary tools often allow limited customization to meet organizational needs. Common examples include Splunk® and Google SecOps (Chronicle) SIEM platforms.

15.3 Common Misconceptions

A common misconception is that open-source tools are less secure or less effective than proprietary tools. In reality, many open-source projects have become industry standards and are widely trusted.

Although threat actors may attempt to exploit open-source tools, their publicly available source code allows security professionals to quickly identify and fix issues. Broad community visibility and rapid response often reduce the likelihood of long-term exploitation.

15.4 Examples of Open-Source Tools

Many widely used cybersecurity tools are open-source and freely available. Two common examples are Linux and Suricata.

15.4.1 Linux

Definition

Linux is an open-source operating system that serves as the interface between computer hardware and the user.

Linux allows users to customize the operating system through a command-line interface (CLI). It is commonly used in security environments due to its flexibility, stability, and transparency.

Multiple Linux distributions exist to support different use cases. Linux and its CLI will be explored in greater detail later in the certificate program.

15.4.2 Suricata

Definition

Suricata is an open-source network analysis and threat detection tool.

Suricata inspects network traffic to identify suspicious behavior and generate network data logs. It analyzes activity across users, systems, and IP addresses to help uncover threats, risks, and vulnerabilities.

Suricata is developed and maintained by the Open Information Security Foundation (OISF), a nonprofit organization committed to keeping the project free and publicly available. The tool is widely used across public and private sectors and integrates with many SIEM and security platforms.

Key Takeaways

- Cybersecurity tools may be open-source or proprietary.
- Open-source tools offer flexibility, transparency, and community support.
- Proprietary tools provide vendor-managed solutions and support.
- Open-source tools are not inherently less secure than proprietary tools.
- Linux and Suricata are widely used open-source cybersecurity tools.

16 Use SIEM Tools to Protect Organizations

Security Information and Event Management (SIEM) tools help cybersecurity professionals monitor organizational activity and identify potential threats, risks, and vulnerabilities. By analyzing dashboard data, security analysts can gain visibility into system behavior and respond to security incidents more effectively.

16.1 Splunk

Splunk provides multiple SIEM solutions, including Splunk Enterprise and Splunk Cloud. Both platforms allow security professionals to review organizational data through interactive dashboards.

Splunk collects, searches, monitors, and analyzes log data from multiple sources to provide visibility into an organization's daily operations. This visibility enables analysts to detect suspicious behavior and investigate security incidents.

16.1.1 Security Posture Dashboard

The security posture dashboard is designed for use in Security Operations Centers (SOCs). It displays notable security-related events and trends from the previous 24 hours.

Security analysts use this dashboard to verify whether security infrastructure and policies are functioning as intended and to monitor potential threats in real time, such as suspicious network activity from a specific IP address.

16.1.2 Executive Summary Dashboard

The executive summary dashboard provides a high-level overview of the organization's security health over time. This dashboard is commonly used to share insights with stakeholders.

Security analysts may generate summaries of security incidents and trends to support decision-making and improve long-term risk reduction strategies.

16.1.3 Incident Review Dashboard

The incident review dashboard helps analysts identify suspicious patterns associated with security incidents. It highlights high-risk items that

require immediate attention and provides a visual timeline of events leading up to an incident.

This dashboard supports efficient investigation and root cause analysis.

16.1.4 Risk Analysis Dashboard

The risk analysis dashboard identifies risk levels for individual risk objects such as users, computers, or IP addresses.

Analysts use this dashboard to detect changes in behavior, such as logins outside normal business hours or unusually high network traffic. This information helps prioritize mitigation efforts for critical assets.

16.2 Chronicle

Chronicle is a cloud-native SIEM tool developed by Google. It retains, analyzes, and searches large volumes of log data to identify security threats, risks, and vulnerabilities.

Chronicle enables log analysis based on:

- Specific assets
- Domain names
- Users
- IP addresses

The platform offers multiple dashboards that help analysts monitor logs, configure alerts, and track suspicious activity.

16.2.1 Enterprise Insights Dashboard

The enterprise insights dashboard highlights recent alerts and identifies suspicious domain names, known as indicators of compromise (IOCs).

Each alert includes a confidence score and severity level. Analysts use this dashboard to monitor unusual access attempts involving critical assets, such as logins from unexpected locations or devices.

16.2.2 Data Ingestion and Health Dashboard

The data ingestion and health dashboard displays metrics related to log volume, log sources, and data processing success rates.

Security analysts use this dashboard to verify that log sources are properly configured and that data is being ingested without errors, ensuring visibility into organizational activity.

16.2.3 IOC Matches Dashboard

The IOC matches dashboard displays top threats, risks, and vulnerabilities identified within the organization.

Analysts monitor trends involving domain names, IP addresses, and devices to focus efforts on the highest priority threats. This dashboard supports further investigation of related activity following alerts.

16.2.4 Main Dashboard

The main dashboard provides a high-level overview of data ingestion, alerting, and event activity over time.

Security professionals use this dashboard to identify trends such as spikes in failed login attempts across devices, locations, and log sources.

16.2.5 Rule Detections Dashboard

The rule detections dashboard displays statistics for incidents based on frequency, severity, and detection rules.

Analysts can review alerts triggered by specific rules, such as those detecting malicious email attachments, to manage recurring incidents and refine mitigation strategies.

16.2.6 User Sign-In Overview Dashboard

The user sign-in overview dashboard tracks user authentication behavior across the organization.

Security analysts use this dashboard to detect anomalies such as simultaneous logins from multiple geographic locations. These insights help mitigate risks related to compromised user accounts.

Key Takeaways

- SIEM dashboards help analysts organize and prioritize security data.
- Splunk and Chronicle provide visibility into organizational activity.
- Dashboards support real-time monitoring and incident investigation.
- Risk-focused dashboards help prioritize mitigation efforts.
- Effective SIEM usage reduces organizational risk through timely response.

17 More About Playbooks

Playbooks are essential tools used by cybersecurity professionals to identify, manage, and respond to security incidents. They provide clear guidance that helps ensure responses are consistent, timely, and aligned with organizational and legal requirements.

17.1 Playbook Overview

A playbook is a manual that outlines operational actions to be taken in response to a specific event. It contains a predefined and regularly updated list of steps that security professionals follow when handling an incident.

Playbooks are supported by a strategy and a plan. The strategy defines the expectations and responsibilities of team members, while the plan describes how tasks outlined in the playbook must be executed.

Playbooks are treated as living documents. They are frequently updated through collaboration among security team members to reflect new threats, industry changes, and lessons learned.

Updates may be required when:

- A failure or oversight is identified in procedures or policies
- Industry standards, laws, or compliance requirements change
- Threat actor tactics and techniques evolve

17.2 Types of Playbooks

Playbooks may be designed to address specific incidents or vulnerabilities, such as ransomware, vishing, or business email compromise (BEC). While incident and vulnerability response playbooks are common, organizations often maintain multiple playbooks tailored to different operational needs.

Playbook content varies between organizations and may depend on:

- Organizational policies and procedures
- Regulatory and compliance requirements
- Geographic location and applicable laws
- The type of data or assets affected

17.3 Incident and Vulnerability Response Playbooks

Incident and vulnerability response playbooks are commonly used by entry-level security analysts. These playbooks are developed in alignment with

an organization's business continuity plan, which defines how operations continue following a disruption such as a security incident.

These playbooks provide step-by-step guidance to ensure responses comply with legal, regulatory, and organizational standards. They also reduce human error and help ensure critical actions are completed within required timeframes.

The level of urgency during an incident depends on the risk to organizational assets. Risk is influenced by the likelihood of a threat and the potential impact on those assets. Proper adherence to playbooks is especially important during forensic investigations, as improper handling of data can compromise evidence.

17.4 Common Playbook Phases

Incident and vulnerability response playbooks typically include the following stages:

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery

Additional activities may include post-incident analysis and coordination among teams throughout the response process.

Key Takeaways

- Playbooks provide structured and consistent incident responses.
- They support compliance with legal and organizational standards.
- Playbooks must be updated regularly to reflect new threats.
- Incident response playbooks reduce error and response time.
- Continuous improvement strengthens future incident handling.

18 Playbooks, SIEM Tools, and SOAR Tools

Security teams routinely encounter threats, risks, vulnerabilities, and security incidents. To respond effectively, they rely on playbooks in combination with Security Information and Event Management (SIEM) tools and Security Orchestration, Automation, and Response (SOAR) tools. These technologies work together to improve consistency, speed, and accuracy during incident response.

18.1 Playbooks and SIEM Tools

Playbooks are used by cybersecurity teams when a security incident occurs. They ensure that a predefined and consistent set of actions is followed, regardless of which analyst is handling the incident.

Playbooks may be highly detailed and can include flowcharts, tables, and decision trees that clarify which actions should be taken and in what order. They are also commonly used for recovery procedures, such as responding to ransomware attacks.

Different incident types have dedicated playbooks that specify:

- The actions required
- The order in which tasks must be completed
- The individuals or teams responsible

Playbooks are typically used alongside SIEM tools. When a SIEM tool flags unusual or suspicious activity—such as abnormal user behavior—the associated playbook provides analysts with step-by-step instructions for investigating and responding to the issue.

18.2 Playbooks and SOAR Tools

Playbooks are also used in conjunction with SOAR tools. SOAR tools support threat monitoring and extend SIEM functionality by automating repetitive and time-consuming tasks.

SOAR software is designed to automate responses triggered by SIEM tools or managed detection and response (MDR) systems. For example, if a user attempts to log in multiple times with incorrect credentials, a SOAR tool can automatically lock the account to prevent a potential intrusion.

After automated actions are taken, analysts consult a playbook to guide the remaining response steps, such as investigating the cause of the incident and restoring legitimate access.

Key Takeaways

- Playbooks provide structured guidance during security incidents.
- SIEM tools detect and alert on suspicious activity.
- SOAR tools automate repetitive incident response tasks.
- Playbooks guide analyst actions following SIEM or SOAR alerts.
- Clear roles and steps reduce incident impact and organizational risk.

Connect and Protect
Networks and Network Security

19 Network Components, Devices, and Diagrams

A foundational understanding of network architecture, also referred to as network design, is essential for cybersecurity analysts. Understanding how networks are structured helps analysts identify vulnerabilities and recognize how malicious actors may attempt to exploit them.

19.1 Network Devices

Network devices maintain information and services for users of a network. These devices connect through wired or wireless connections and transmit data in the form of packets. Each packet contains information about its source and destination, enabling data to be sent and received across a network.

The network itself is the infrastructure that allows devices to communicate. Specialized network devices, such as routers and switches, control how data is transmitted, while end-user devices such as computers and phones connect through these network components.

19.2 End-User Devices and Desktop Computers

Common network-connected devices include desktop computers, laptops, mobile phones, and tablets. Each device has a unique Media Access Control (MAC) address and an Internet Protocol (IP) address that identify it on the network.

These devices also contain network interfaces that send and receive data packets. Connections may be established through physical cables or wireless technologies.

19.3 Firewalls

A firewall is a network security device that monitors and controls incoming and outgoing network traffic. Firewalls act as a first line of defense by enforcing security rules configured by the organization.

Firewalls are typically positioned between a trusted internal network and untrusted external networks, such as the internet. While firewalls are an important security control, they represent only one layer of defense within a broader security strategy.

19.4 Servers

Servers provide services and information to devices on a network. Devices that request services from a server are known as clients. This interaction is referred to as the client–server model.

In this model, clients send requests for resources or services, and the server processes those requests. Examples of servers include:

- Domain Name System (DNS) servers
- File servers
- Email servers

19.5 Hubs and Switches

Hubs and switches are devices that manage traffic within a local network. A hub provides a shared connection point and broadcasts all received data to every connected device. From a security standpoint, this makes hubs vulnerable to eavesdropping. As a result, hubs are rarely used in modern enterprise networks.

Switches are the preferred alternative. Switches forward data packets only to their intended destination by analyzing MAC addresses. They maintain a MAC address table that maps devices to switch ports, improving both performance and security. Switches operate at the data link layer of the TCP/IP model.

19.6 Routers

Routers connect multiple networks and forward traffic based on destination IP addresses. They enable communication between devices on different networks.

Routers operate at the network layer of the TCP/IP model. They read IP header information and forward packets along the appropriate path until they reach their destination network. Many routers also include firewall capabilities to block malicious traffic before it reaches the internal network.

19.7 Modems and Wireless Access Points

Modems connect homes or organizations to an Internet Service Provider (ISP). ISPs deliver internet connectivity through telephone lines, coaxial cables, or fiber-optic cables. Modems convert incoming signals into a digital format usable by local network devices and typically pass this data to a router.

Enterprise networks may use alternative broadband technologies instead of modems to support high-volume traffic.

Wireless access points create wireless networks by transmitting data over radio waves. Devices with wireless adapters connect using Wi-Fi, a set of standards that enable wireless communication. Access points forward data to routers and switches, which then direct traffic to its final destination.

19.8 Using Network Diagrams as a Security Analyst

Network diagrams visually represent an organization's network architecture. They illustrate network devices and the connections between them using standardized symbols and lines.

Security analysts use network diagrams to understand how systems are connected, identify potential points of failure, and develop strategies to secure the network infrastructure.

Key Takeaways

- Networks enable communication between connected devices.
- Common network devices include servers, routers, switches, and firewalls.
- Switches improve security by directing traffic to specific devices.
- Routers connect different networks using IP addresses.
- Network diagrams help analysts visualize and secure network architectures.

20 Cloud Computing and Software-Defined Networks

Modern networks can be implemented using physical infrastructure, cloud-based services, or a combination of both. Understanding cloud computing and software-defined networking helps security analysts assess risks, scalability, and security controls in contemporary network environments.

20.1 Computing Processes in the Cloud

Traditional networks are referred to as on-premise networks, where all network devices, servers, and storage are located at a company-owned physical site. In contrast, cloud computing is the use of remote servers, applications, and networking services hosted on the internet instead of at an organization's physical location.

A cloud service provider (CSP) is a company that offers cloud computing services. CSPs operate large data centers worldwide that house millions of servers and provide services such as compute, storage, and networking at scale. Organizations consume these services through application programming interfaces (APIs) or web-based consoles and pay only for the resources they use.

20.2 Cloud Service Models

CSPs generally offer three primary service models:

20.2.1 Software as a Service (SaaS)

Software as a Service refers to software applications that are hosted and managed by the CSP. Organizations use these applications remotely without installing or maintaining the software themselves.

20.2.2 Infrastructure as a Service (IaaS)

Infrastructure as a Service provides virtualized computing resources, including virtual machines, containers, and storage. These resources are configured remotely and can support existing applications with minimal modification while benefiting from cloud availability and security features.

20.2.3 Platform as a Service (PaaS)

Platform as a Service offers tools and environments that developers use to design, build, and deploy custom applications. These applications are

created and accessed entirely within the cloud to support specific business needs.

20.3 Hybrid and Multi-Cloud Environments

When organizations use both on-premise infrastructure and cloud services, the environment is known as a hybrid cloud. When multiple CSPs are used simultaneously, the environment is referred to as a multi-cloud environment.

Most organizations adopt hybrid cloud architectures to balance cost, flexibility, and control over sensitive network resources.

20.4 Software-Defined Networks

Cloud service providers offer networking capabilities similar to traditional physical devices through software-defined networks (SDNs). SDNs consist of virtual network components such as switches, routers, and firewalls that are implemented through software rather than dedicated hardware.

In cloud environments, SDN components are hosted on CSP-managed servers. Many modern physical networking devices also support virtualization, allowing routing and switching functions to be controlled by software. SDNs enable centralized management, automation, and rapid configuration changes.

20.5 Benefits of Cloud Computing and SDNs

Cloud computing and software-defined networking provide several key advantages to organizations.

20.5.1 Reliability

Cloud reliability depends on service availability, secure connections, and consistent performance. CSPs design their infrastructure to minimize downtime and ensure users can access resources with minimal interruption.

20.5.2 Cost

Maintaining on-premise infrastructure requires significant upfront investment in hardware, software, and maintenance. CSPs reduce these costs by offering shared infrastructure at scale, allowing organizations to avoid purchasing, upgrading, and managing their own equipment.

20.5.3 Scalability

Cloud services support elastic scaling, allowing organizations to quickly increase or decrease resource usage as business needs change. This utility-based model reduces financial risk and enables rapid deployment of security controls such as firewalls, intrusion detection and prevention systems, and web application firewalls.

Key Takeaways

- Cloud computing uses remotely hosted servers and services.
- CSPs provide SaaS, IaaS, and PaaS service models.
- Hybrid and multi-cloud environments improve flexibility.
- SDNs use software to manage virtualized network devices.
- Cloud networking improves reliability, reduces cost, and supports scalability.

21 Learn More About the TCP/IP Model

Understanding the Transmission Control Protocol/Internet Protocol (TCP/IP) model is essential for cybersecurity professionals. The TCP/IP model explains how data is transmitted across networks and how different network protocols function together. It also helps security analysts identify which layers may be affected during a network disruption or security incident.

Two widely used conceptual networking models are the TCP/IP model and the Open Systems Interconnection (OSI) model. While both models describe how data travels across a network, the examples used throughout this course are based on the TCP/IP model.

21.1 The TCP/IP Model

The TCP/IP model is a framework used to visualize how data is organized, transmitted, and received across a network. Network engineers and security analysts rely on this model to understand network behavior and communicate where security threats or failures occur.

The TCP/IP model consists of four layers:

- Network access layer
- Internet layer
- Transport layer
- Application layer

21.2 Network Access Layer

The network access layer, sometimes referred to as the data link layer, handles the creation and transmission of data packets across the physical network. This layer corresponds to physical network components such as hubs, modems, cables, and wiring.

The Address Resolution Protocol (ARP) operates at this layer. ARP maps Internet Protocol (IP) addresses to Media Access Control (MAC) addresses, enabling communication between devices on the same local network.

21.3 Internet Layer

The internet layer, also known as the network layer, is responsible for delivering data packets to their destination across different networks. It assigns IP addresses to packets to identify the source and destination hosts.

Common protocols operating at this layer include:

- Internet Protocol (IP): Routes packets between networks and relies on TCP or UDP for delivery to destination services.
- Internet Control Message Protocol (ICMP): Communicates error messages and network status information, such as packet loss or connectivity issues.

21.4 Transport Layer

The transport layer controls how data is delivered between systems and manages traffic flow. Two primary protocols operate at this layer.

21.4.1 Transmission Control Protocol (TCP)

TCP is a connection-oriented protocol that establishes a reliable connection between devices. It ensures data is delivered accurately and in order. TCP includes destination port numbers within the packet header to identify the receiving service and retransmits lost or corrupted data.

21.4.2 User Datagram Protocol (UDP)

UDP is a connectionless protocol that does not establish a session before data transmission. It prioritizes speed over reliability and is commonly used for real-time applications such as video streaming and online gaming.

21.5 Application Layer

The application layer defines how network services and applications interact with users. This layer is responsible for initiating network requests and responding to them.

Common application layer protocols include:

- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Secure Shell (SSH)
- File Transfer Protocol (FTP)
- Domain Name System (DNS)

Application layer protocols rely on the lower layers of the TCP/IP model to transport data across the network.

21.6 TCP/IP Model Versus OSI Model

The OSI model organizes network communication into seven layers, while the TCP/IP model combines these functions into four layers. Both models define networking standards and help professionals communicate about network processes and security issues.

The TCP/IP model is considered a simplified version of the OSI model and is more closely aligned with real-world internet communication.

Key Takeaways

- The TCP/IP model explains how data is transmitted across networks.
- It consists of four layers: network access, internet, transport, and application.
- TCP provides reliable data delivery, while UDP prioritizes speed.
- Application layer protocols define user-facing network services.
- The TCP/IP model simplifies the seven-layer OSI model.

22 The OSI Model

Network communication is organized through standardized protocols that operate at different layers. Earlier, you learned about the TCP/IP model and how protocols such as Transmission Control Protocol (TCP) and Internet Protocol (IP) support data transmission across networks. The four-layer TCP/IP model is a simplified version of the Open Systems Interconnection (OSI) model, which consists of seven layers.

The OSI model provides a more detailed view of how data moves across a network. Security professionals often use it to analyze where problems, failures, or security threats occur. This section reviews each OSI layer, working from Layer 7 (user interaction) down to Layer 1 (physical transmission).

22.1 TCP/IP Model vs. OSI Model

The TCP/IP model organizes network communication into four layers and is commonly used to describe real-world internet communication. Security analysts rely on this model to identify which part of the network stack was affected during an incident.

The OSI model is a standardized conceptual framework that divides network communication into seven layers. Network and security professionals use the OSI model to communicate clearly about technical issues and security threats.

While organizations may favor one model over the other, familiarity with both models is essential for cybersecurity analysts.

22.2 Layer 7: Application Layer

The application layer includes processes that directly interact with the user. It consists of network protocols used by applications to request and deliver information over the internet.

Examples of application layer activity include:

- Web browsing using HTTP or HTTPS
- Email communication using Simple Mail Transfer Protocol (SMTP)
- Domain name resolution using Domain Name System (DNS)

This layer enables users to access network services through software applications.

22.3 Layer 6: Presentation Layer

The presentation layer is responsible for data translation, formatting, and encryption. It ensures that data sent by the application layer can be interpreted correctly by the receiving system.

Common functions at this layer include:

- Data encryption and decryption
- Data compression
- Character encoding translation

An example of presentation layer security is Secure Sockets Layer (SSL), which encrypts communication between web servers and browsers for HTTPS connections.

22.4 Layer 5: Session Layer

The session layer manages the establishment, maintenance, and termination of connections between devices. A session allows two systems to exchange data over a defined period.

This layer is responsible for:

- Authentication
- Session management
- Reconnection and checkpointing during data transfers

If a connection is interrupted, checkpoints allow data transfer to resume from the last successful point.

22.5 Layer 4: Transport Layer

The transport layer controls the delivery of data between devices. It manages segmentation, flow control, and transmission speed to ensure data arrives correctly.

Protocols operating at this layer include:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

Segmentation divides large data transmissions into smaller segments, which are reassembled at the destination.

22.6 Layer 3: Network Layer

The network layer determines how data packets are routed between networks. It identifies destination addresses and ensures packets reach the correct network.

Internet Protocol (IP) operates at this layer and uses IP addresses to guide routers in forwarding packets from the source network to the destination network.

22.7 Layer 2: Data Link Layer

The data link layer manages data transmission within a single local network. It organizes frames and controls access to the physical network medium.

Devices and protocols at this layer include:

- Network interface cards (NICs)
- Switches
- Network Control Protocol (NCP)
- High-Level Data Link Control (HDLC)
- Synchronous Data Link Control (SDLC)

22.8 Layer 1: Physical Layer

The physical layer represents the hardware components used for network communication. This includes cables, connectors, hubs, and modems.

At this layer, data is transmitted as electrical signals, light pulses, or radio waves. Binary data is converted into physical signals for transmission and then converted back into digital data by receiving devices.

Key Takeaways

- The OSI model consists of seven communication layers.
- It provides a detailed view of network communication processes.
- Each layer performs a specific function in data transmission.
- Security professionals use the OSI model to locate threats and failures.
- The OSI and TCP/IP models are both essential for network analysis.

23 Components of Network Layer Communication

The network layer corresponds to Layer 3 of the OSI model and is responsible for addressing and routing data packets from a source device to a destination device. At this layer, data is directed across multiple networks using Internet Protocol (IP) addresses.

Understanding network layer communication is essential for security analysts, as many attacks, misconfigurations, and routing issues can be identified by analyzing packet-level information.

23.1 Operations at the Network Layer

The network layer manages the logical addressing and delivery of data packets across networks. Routers forward packets from one network to another based on the destination IP address contained in each packet's header.

Routing decisions are made using routing tables, which store paths to destination networks. As packets travel across the internet, routers examine header information and forward packets until they reach the destination network.

All transmitted data packets contain an IP address. For TCP connections, these packets are commonly referred to as IP packets, while UDP connections use datagrams. Header information includes the source and destination IP addresses, packet size, and the protocol used for the data payload.

23.2 IPv4 Packet Structure

An IPv4 packet consists of two primary sections:

- Header
- Data

The header contains routing and control information, while the data section carries the actual message being transmitted. The total maximum size of an IPv4 packet is 65,535 bytes.

The IPv4 header ranges from 20 to 60 bytes. The first 20 bytes are fixed fields, and the remaining bytes (up to 40) are optional fields used for additional instructions or security features.

23.3 IPv4 Header Fields

The IPv4 header contains 13 fields that guide packet delivery:

- Version (VER): Indicates the IP version used (IPv4).
- Header Length (HLEN/IHL): Specifies where the header ends and the data section begins.
- Type of Service (ToS): Allows routers to prioritize packets for quality of service.
- Total Length: Indicates the size of the entire packet, including header and data.
- Identification: Identifies packet fragments for reassembly at the destination.
- Flags: Indicates fragmentation status and whether more fragments follow.
- Fragment Offset: Specifies a fragment's position within the original packet.
- Time to Live (TTL): Limits the lifespan of a packet to prevent infinite routing loops.
- Protocol: Identifies the protocol used by the data portion (e.g., TCP or UDP).
- Header Checksum: Detects corruption in the header during transmission.
- Source IP Address: IPv4 address of the sending device.
- Destination IP Address: IPv4 address of the receiving device.
- Options: Provides optional instructions or security features when enabled.

23.4 IPv4 vs. IPv6

IPv4 was originally designed with a limited address space of approximately 4.3 billion addresses. As internet usage grew, this space became insufficient, resulting in IPv4 address exhaustion.

IPv6 was developed to address this limitation and improve routing efficiency.

23.4.1 Address Format Differences

IPv4 addresses:

- 32-bit addresses
- Four decimal values (0–255)
- Example: `198.51.100.0`

IPv6 addresses:

- 128-bit addresses
- Eight hexadecimal blocks

- Example: `2002:0db8::ff21:0023:1234`

IPv6 supports approximately 340 undecillion addresses, greatly expanding available address space.

23.4.2 Header Differences

The IPv6 header is simpler than the IPv4 header. IPv6 removes fields such as Header Length, Identification, and Flags, and introduces a Flow Label field used to identify packets requiring special handling by routers.

23.5 Security Implications

Analyzing IP packet headers allows security analysts to determine:

- Where traffic originates
- Where traffic is destined
- Which protocol is being used
- Whether packets are malformed or suspicious

Understanding network layer packet structure enables informed decisions about filtering, routing, and detecting malicious activity.

Key Takeaways

- The network layer manages packet addressing and routing.
- IP headers contain critical routing and security information.
- IPv4 packets include detailed header fields for delivery control.
- IPv6 expands address space and simplifies packet headers.
- Packet analysis supports threat detection and incident response.

24 Common Network Protocols

Network protocols define the rules and structure that allow devices to communicate across a network. These rules specify how data is formatted, transmitted, received, and interpreted. Protocols function as a shared language, ensuring that devices from different manufacturers and locations can communicate reliably.

Although network protocols enable global communication, they can also introduce security risks. Some protocols contain vulnerabilities that threat actors exploit to intercept traffic, redirect users, or gain unauthorized access. For this reason, understanding protocol behavior and security implications is essential for cybersecurity analysts.

24.1 Overview of Network Protocols

A network protocol is a standardized set of instructions that governs how data packets are transmitted between devices. These instructions define packet structure, transmission order, error handling, and recovery mechanisms.

Protocols operate at different layers of the TCP/IP model and may serve different purposes. From a security perspective, analysts must understand how protocols function and how they can be abused by attackers.

24.2 Categories of Network Protocols

Network protocols can be grouped into three primary categories:

- Communication protocols
- Management protocols
- Security protocols

24.3 Communication Protocols

Communication protocols control how data is exchanged across a network. They define connection establishment, data transfer methods, and error handling.

24.3.1 Transmission Control Protocol (TCP)

Transmission Control Protocol (TCP) is a connection-oriented protocol that ensures reliable data transmission. TCP establishes a connection using a three-way handshake process:

- SYN: The client initiates the connection
- SYN/ACK: The server acknowledges the request
- ACK: The client confirms the connection

TCP guarantees data delivery, ordering, and retransmission of lost packets. In the TCP/IP model, TCP operates at the transport layer.

24.3.2 User Datagram Protocol (UDP)

User Datagram Protocol (UDP) is a connectionless protocol that prioritizes speed over reliability. Unlike TCP, UDP does not establish a connection or retransmit lost packets.

UDP is commonly used for time-sensitive services such as DNS queries and streaming applications. In the TCP/IP model, UDP operates at the transport layer.

24.3.3 Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP) enables communication between web clients and servers. It operates on port 80 and transmits data in plaintext, making it vulnerable to interception and manipulation.

Due to security concerns, HTTP is increasingly replaced by HTTPS. HTTP operates at the application layer.

24.3.4 Domain Name System (DNS)

Domain Name System (DNS) translates human-readable domain names into IP addresses. DNS typically uses UDP on port 53 but may switch to TCP when responses are large.

DNS operates at the application layer and is a common target for attacks such as DNS spoofing and redirection.

24.4 Management Protocols

Management protocols monitor and manage network performance, device status, and error reporting.

24.4.1 Simple Network Management Protocol (SNMP)

SNMP is used to monitor and manage network devices such as routers, switches, and servers. It can retrieve performance metrics, modify device configurations, and reset credentials.

SNMP operates at the application layer and must be securely configured to prevent unauthorized access.

24.4.2 Internet Control Message Protocol (ICMP)

ICMP is used for error reporting and network diagnostics. It provides feedback about packet delivery failures and network reachability.

ICMP is commonly used by the `ping` command to test connectivity. In the TCP/IP model, ICMP operates at the internet layer.

24.5 Security Protocols

Security protocols protect data in transit using encryption and secure authentication mechanisms.

24.5.1 Hypertext Transfer Protocol Secure (HTTPS)

HTTPS is the secure version of HTTP and uses SSL/TLS encryption to protect data during transmission. HTTPS operates on port 443 and prevents unauthorized parties from reading transmitted content.

HTTPS operates at the application layer.

24.5.2 Secure File Transfer Protocol (SFTP)

SFTP securely transfers files using Secure Shell (SSH). It typically operates over TCP port 22 and uses strong encryption algorithms such as AES to protect data.

SFTP is commonly used for cloud storage and secure file transfers and operates at the application layer.

24.6 Security Considerations

While encryption protects data content, it does not conceal metadata such as source and destination IP addresses. Threat actors may still analyze traffic patterns even when encryption is used.

Security analysts must monitor protocol usage, enforce secure configurations, and identify abnormal protocol behavior to mitigate risk.

Key Takeaways

- Network protocols define how data is transmitted and interpreted.
- Protocols are grouped into communication, management, and security categories.
- TCP provides reliable delivery, while UDP prioritizes speed.
- HTTPS and SFTP encrypt data to protect confidentiality.
- Protocol knowledge helps analysts detect and prevent network attacks.

25 Additional Network Protocols

In addition to core communication, management, and security protocols, cybersecurity analysts frequently work with supporting protocols that enable addressing, device configuration, remote access, and email communication. Understanding how these protocols function, which ports they use, and where they operate in the TCP/IP model is critical for network monitoring, firewall configuration, and incident response.

25.1 Network Address Translation (NAT)

Devices within a private network use private IP addresses to communicate locally. However, private IP addresses are not routable on the public internet. To enable internet access, routers or firewalls replace the private source IP address with a public IP address. This process is called Network Address Translation (NAT).

For outbound traffic, NAT substitutes the private IP with the public IP. For inbound responses, the router reverses the translation and forwards the traffic to the correct internal device. NAT helps conserve IPv4 addresses and provides basic network isolation.

NAT primarily operates at the internet layer of the TCP/IP model, with interaction at the transport layer when tracking ports and sessions.

25.1.1 Private vs. Public IP Addresses

Private IP address ranges:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Public IP addresses are globally unique, assigned by Internet Service Providers (ISPs), and regulated by the Internet Assigned Numbers Authority (IANA).

25.2 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a management protocol used to automatically configure network devices. DHCP assigns IP addresses, default gateways, and DNS server information to devices joining a network.

DHCP servers operate on UDP port 67, and DHCP clients operate on UDP port 68. DHCP functions at the application layer of the TCP/IP model.

25.3 Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) maps IP addresses to Media Access Control (MAC) addresses within a local network. When a device knows the destination IP address but not the MAC address, it broadcasts an ARP request to identify the correct hardware address.

Devices store IP-to-MAC mappings in an ARP cache to reduce network overhead. ARP operates at the network access layer and does not use port numbers.

25.4 Telnet

Telnet is an application layer protocol that enables remote access to systems using a command-line interface. All data transmitted using Telnet is sent in plaintext, including authentication credentials.

Telnet operates over TCP port 23. Due to its lack of encryption, Telnet is considered insecure and has largely been replaced by Secure Shell (SSH).

25.5 Secure Shell (SSH)

Secure Shell (SSH) provides encrypted remote access to systems. SSH supports secure authentication and protects data confidentiality and integrity during transmission.

SSH operates at the application layer over TCP port 22 and is the secure replacement for Telnet.

25.6 Post Office Protocol (POP3)

Post Office Protocol version 3 (POP3) is used to retrieve email from a mail server. Emails are downloaded to the client device and may be deleted from the server, limiting synchronization across multiple devices.

POP3 uses:

- TCP/UDP port 110 for unencrypted communication
- TCP/UDP port 995 for encrypted communication using SSL/TLS

POP3 operates at the application layer.

25.7 Internet Message Access Protocol (IMAP)

Internet Message Access Protocol (IMAP) allows users to access email directly from the mail server. Email content remains on the server, enabling synchronization across multiple devices.

IMAP uses:

- TCP port 143 for unencrypted communication
- TCP port 993 for encrypted communication using TLS

IMAP operates at the application layer.

25.8 Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) is used to send and route email from a sender to the recipient's mail server. SMTP works with Message Transfer Agent (MTA) software and DNS to resolve recipient domains.

SMTP uses:

- TCP/UDP port 25 for unencrypted communication
- TCP/UDP port 587 for encrypted communication using TLS

SMTP operates at the application layer. Port 25 is commonly associated with spam traffic and is often restricted by network firewalls.

25.9 Protocols and Port Numbers

Port numbers allow network devices and firewalls to identify which services should receive incoming traffic. Security teams frequently use port-based filtering to restrict access to sensitive services.

Protocol	Port
DHCP	UDP 67 (server), UDP 68 (client)
ARP	None
Telnet	TCP 23
SSH	TCP 22
POP3	TCP/UDP 110 (unencrypted), 995 (SSL/TLS)
IMAP	TCP 143 (unencrypted), 993 (TLS)
SMTP	TCP/UDP 25 (unencrypted), 587 (TLS)

Key Takeaways

- NAT enables private networks to communicate with the public internet.
- DHCP automates IP address assignment and network configuration.
- ARP maps IP addresses to MAC addresses on local networks.
- SSH provides encrypted remote access, replacing Telnet.
- POP3, IMAP, and SMTP support email retrieval and delivery.
- Knowing protocol ports is essential for firewall and SOC work.