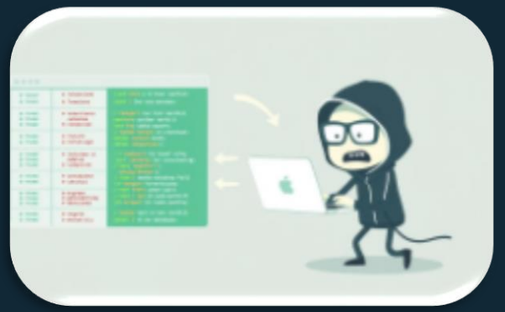
Hacking: Understanding Cyber Threats

This presentation explores today's cyber threats, giving you the knowledge to navigate the changing world of hacking and online security.

Meet the Team

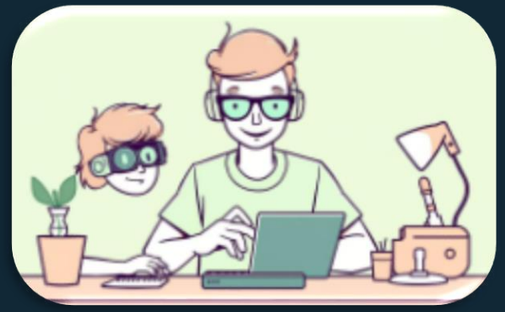
1. Aadithya S Nair
2. Aditya B Pattar
3. Anuj Jitendra Darji
4. Hithaishini S
5. Yashika Vinod Naik

Key Topics in Cybersecurity



SQL Injection

Cryptography



Hacking Devices

Phishing Attacks

DDoS Attacks

SQL Injection

What is SQL Injection? Understanding the Vulnerability

1 Exploiting Input Fields

SQL injection takes advantage of unprotected user input fields to inject malicious SQL code and gain unauthorized access to databases.

2 Bypassing Authentication

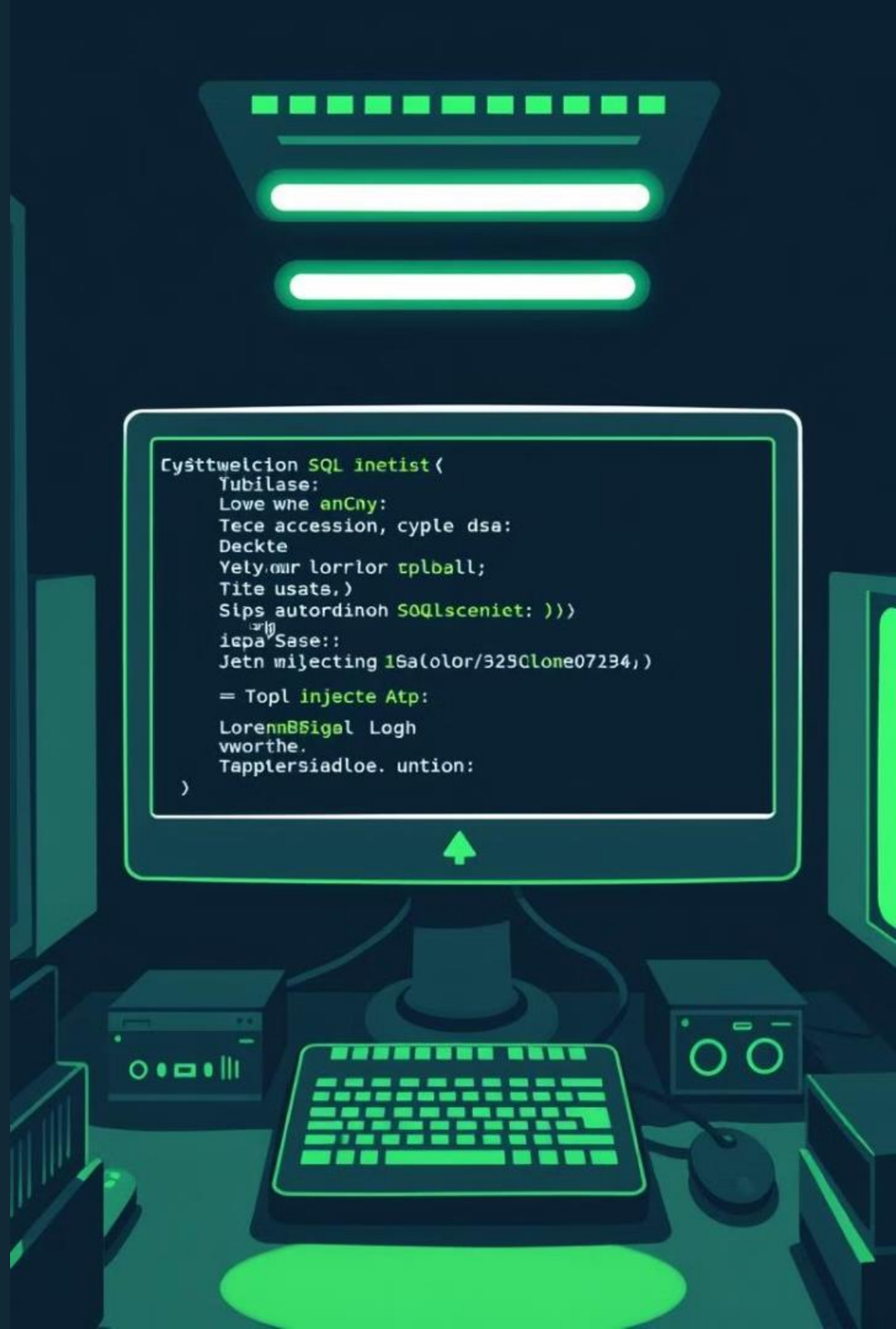
Attackers can use SQL injection to bypass login screens and gain administrative privileges, compromising sensitive data.

3 Malicious Code Execution

Injected SQL code can execute arbitrary commands on the server, leading to complete system takeover and data breaches.

Lets Look at a Demo of SQL Injection

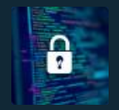
We'll walk through a step-by-step demonstration of how SQL injection attacks work, highlighting the vulnerabilities and the potential consequences for your organization.



Preventing SQL Injection Attacks

Input Validation

Properly validate and sanitize all user inputs before using them in SQL queries to prevent malicious code injection.



Parameterized Queries

Use parameterized queries or prepared statements instead of concatenating user input directly into SQL queries.

Least Privilege

Grant your application the minimum necessary database permissions to reduce the potential impact of a successful SQL injection attack.

Regular Audits

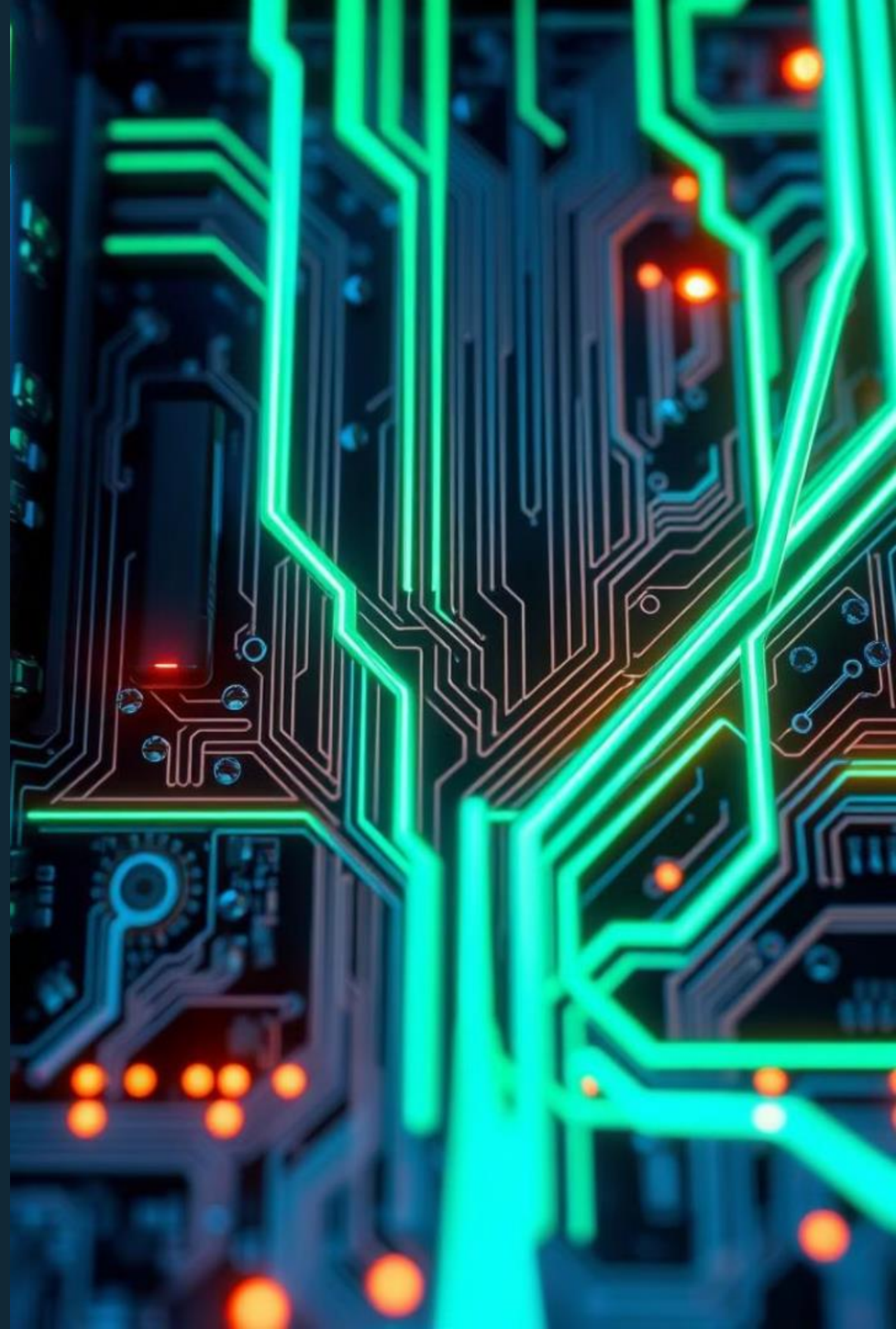
Conduct regular security audits to identify and patch any SQL injection vulnerabilities in your web applications.

Employee Training

Educate your developers and IT staff on secure coding practices to help prevent SQL injection vulnerabilities from being introduced in the first place.

Cryptography

Cryptography is a way to protect information by making it unreadable to anyone without the correct key.



Cryptography: Safeguarding Information in the Digital Age

Why Cryptography?

Secure communication, authentication, integrity, and confidentiality.

How it works?

A message is converted to ciphertext using an encryption key, sent across the network, and decrypted at the receiving end. Any tampering during transmission will result in an error, ensuring data integrity.

Types of Cryptography

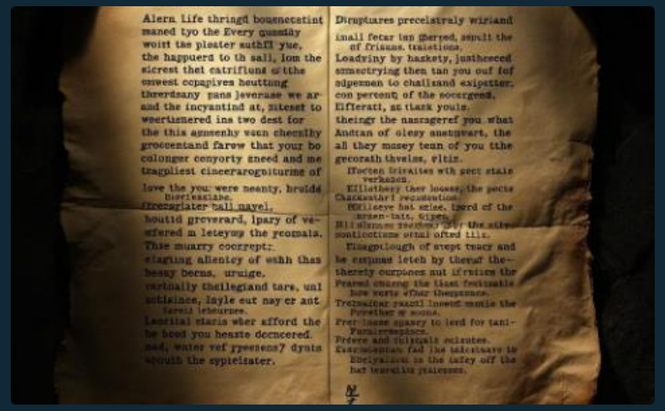
Symmetric Key Cryptography

Uses one key for both encryption and decryption.

Asymmetric Key Cryptography

A key pair - one public, one private - is used for secure communication.

Symmetric Key Cryptography



Classical Cryptography

Traditional methods like transposition ciphers (shuffling letters) and substitution ciphers (replacing letters with others).

Modern Cryptography

Contemporary methods like stream ciphers (encrypting data bit by bit) and block ciphers.

Classical Cryptography

Transposition Cipher

Rearranges the order of characters in a message. For example, "HelloWorld" could become "lroWolleHd".

Substitution Cipher

Substitutes characters with other characters or symbols. For example, "HelloWorld" might become "Mjqqt%twqi".

Block Cipher

Encrypts fixed-size blocks of text using a secret key.

Hacking Devices

Let's Explore the specialized hardware and tools that enable modern cyber threats, from software-defined radios to hardware hacking platforms.

Flipper Zero: A Swiss Army Knife for Hackers

Versatile Tool

Flipper Zero is a multi-functional device that can emulate various protocols, perform wireless attacks, and automate hacking tasks.

Customizable Functionality

With its open-source firmware and community-driven development, Flipper Zero can be tailored to suit diverse hacking needs.

Portable Security

The compact design and battery-powered operation make Flipper Zero a versatile tool for ethical hacking and security assessments.

Hackrf One: Software-Defined Radio for Security Professionals

Wireless Exploration

Hackrf One enables the analysis and reverse-engineering of various wireless protocols, from Bluetooth to WiFi and beyond.

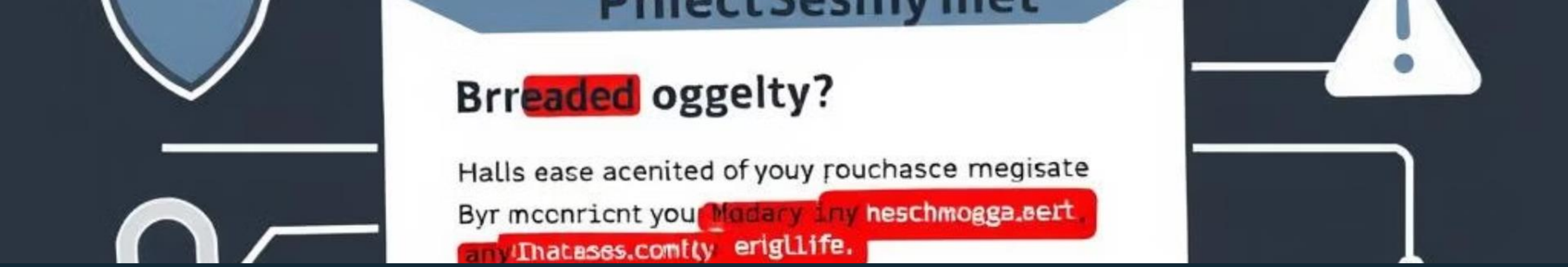
Signal Manipulation

The software-defined radio capabilities of Hackrf One allow for the creation of custom wireless attacks and signal jamming.

Security Assessments

Hackrf One is a valuable tool for penetration testing, vulnerability assessments, and identifying security weaknesses in wireless systems.

Phishing Attacks



Phishing Attacks: Baiting the Hook

Deceptive Emails

Phishing attacks leverage fake emails that appear to be from legitimate sources to lure victims into revealing sensitive information.

1

Social Engineering

Phishing exploits human psychology, using fear, urgency, and a sense of authority to manipulate victims into taking the desired actions.

3

2

Malicious Links

Clicking on links in phishing emails can lead to malware infection or redirect victims to spoofed websites designed to steal credentials.

Preventing Phishing Attacks

Educate Employees

Train staff to spot phishing attempts.

Implement Technical Safeguards

Use filters and security tools to block phishing emails.

Enforce Strong Authentication

Require multi-factor authentication for added security.

Promote Reporting

Encourage employees to report suspicious emails promptly.

Regularly Test and Improve

Conduct phishing simulations to strengthen your defenses.

DDOS Attacks

DDoS attacks, short for Distributed Denial of Service attacks, are a type of cyberattack aimed at overwhelming a target server or network with an excessive amount of traffic, making it inaccessible to legitimate users. These attacks can be launched from multiple sources simultaneously, flooding the target with requests and causing it to crash or become unresponsive. The impact of a DDoS attack can be significant, disrupting business operations, causing financial losses, and potentially damaging reputation.

DDOS Attacks: Overwhelming the Target

1

Amplification

DDoS attacks leverage botnets and other techniques to generate massive amounts of traffic, overwhelming the targeted system or network.

2

Exhaustion

The sheer volume of traffic consumes the target's resources, causing service disruptions, slow performance, or even complete system crashes.

3

Distraction

DDoS attacks can be used as a smokescreen to divert attention from other malicious activities, such as data breaches or system infiltration.

Preventing DDoS Attacks

Implement Network Monitoring

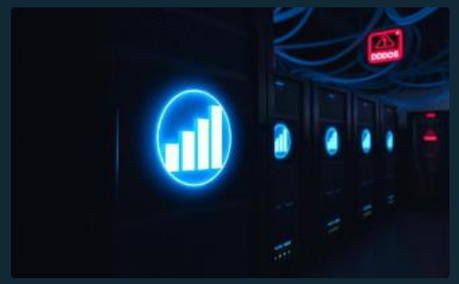
Use tools to detect and mitigate DDoS traffic in real-time, identifying and blocking malicious sources.

Utilize Cloudflare or CDN

These services can absorb and filter DDoS traffic, shielding your servers and maintaining service availability.

Enable Strict Firewall Rules

Configure firewalls to block suspicious IP addresses, protocols, and traffic patterns associated with DDoS attacks.



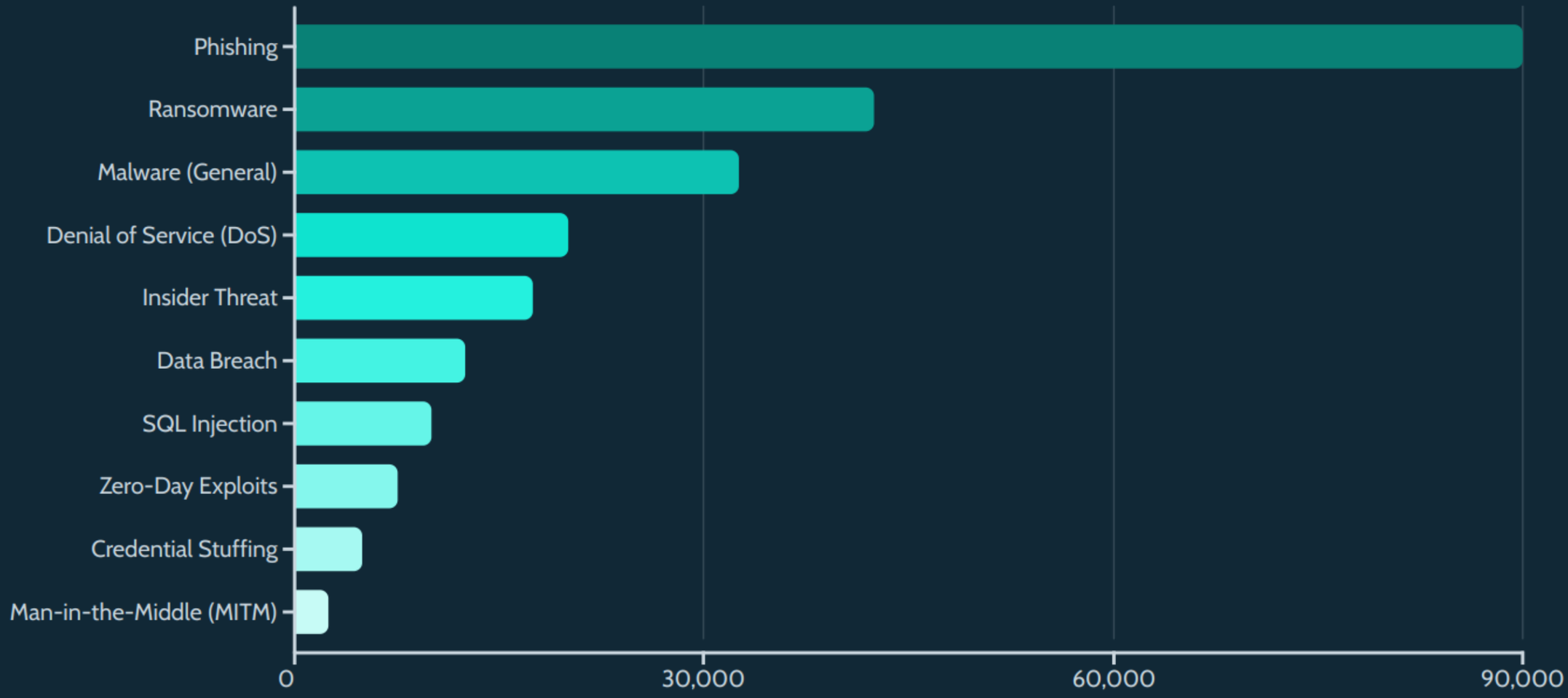
Scalable Infrastructure

Ensure your system architecture can dynamically scale to handle sudden spikes in legitimate traffic, preventing service outages.

Incident Response Plan

Develop a comprehensive plan to detect, respond, and recover from DDoS attacks, minimizing the impact on your operations.

Visualizing Cyber Threats: Graphs and Data Analytics



This bar chart visualizes the number of cybersecurity incidents by attack type, providing insights into the most prevalent threats facing the organization. Data sources: Verizon DBIR, Symantec Internet Security Threat Report, Mandiant Threat Intelligence, CISA Alerts, Europol IOCTA, ENISA Threat Landscape Report, SANS Institute, Cisco Cybersecurity Report.

Real-World Case Studies: Lessons Learned

EQUIFAX

Equifax Data Breach

Highlighting the importance of robust security practices and timely software updates to prevent large-scale data breaches.

WannaCry Ransomware

Demonstrating the need for comprehensive backup strategies and the prompt implementation of security patches to mitigate the impact of ransomware attacks.

TARGET

Target Payment System Hack

Underscoring the significance of secure payment processing and the vigilance required to protect customer data from sophisticated threats.

Developing a Proactive Cybersecurity Strategy

1 Risk Assessment

Identifying and prioritizing potential vulnerabilities and threats to your organization's critical assets and infrastructure.

2 Incident Response

Establishing a comprehensive plan to detect, investigate, and mitigate the impact of cyber incidents, minimizing damage and disruption.

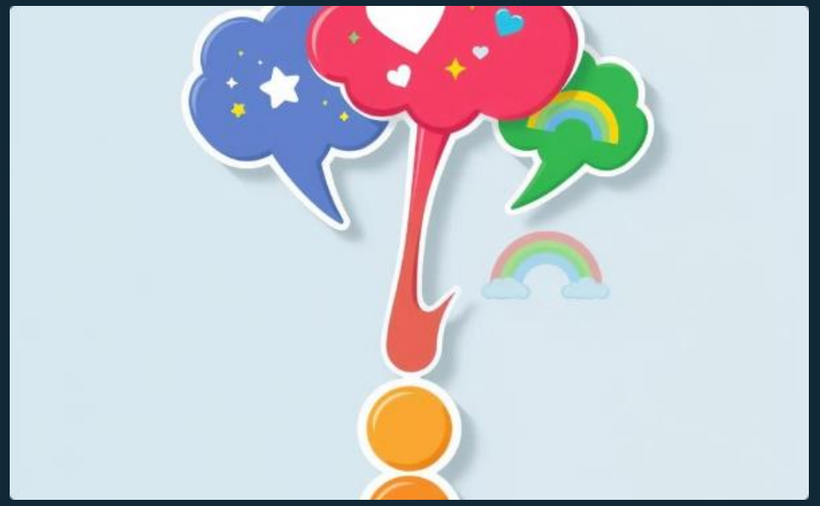
3 Continuous Monitoring

Implementing robust security monitoring and alerting systems to quickly identify and address emerging threats in real-time.

4 Employee Training

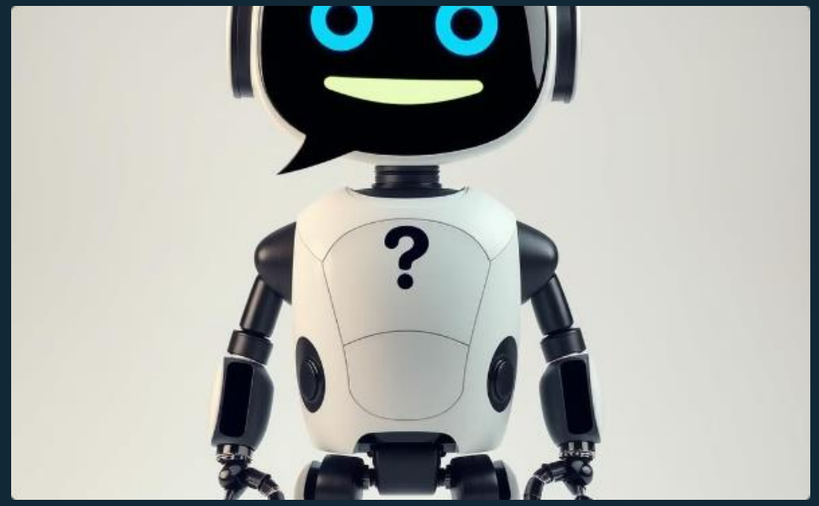
Educating and empowering employees to be the first line of defense against social engineering, phishing, and other human-based attacks.

Q & A



Questions

We encourage you to ask any questions you have about cybersecurity.



Answers

We are here to provide clear and insightful answers to your queries.

Thank You

We appreciate your time and attention.