Fortifying the Frontier: Network Security & Incident Response

In today's interconnected world, safeguarding our digital infrastructure is paramount. This presentation will equip with practical knowledge to defend against evolving cyber threats and respond effectively when incidents occur.

Jhon Lloyd T. Cruz

Chapter 1

Protecting Our Perimeters

Effective network security relies on a layered defense. We'll explore foundational tools that act as your first line of defense, filtering malicious traffic and securing communications.

Firewalls

Your network's vigilant gatekeeper, meticulously filtering traffic based on predefined security rules.

IDS/IPS

Intrusion Detection Systems alert to suspicious activity; Intrusion Prevention Systems proactively block threats.

VPNs

Virtual Private Networks encrypt data and create secure tunnels for private, protected communication.

Jhon Lloyd T. Cruz

Chapter 2

Understanding the Adversary

To build robust defenses, it's crucial to understand the tactics used by attackers. These common methods can compromise network integrity and data.

⊗ DoS (Denial of Service)

Attackers flood a system with traffic, overwhelming its resources and making it unavailable to legitimate users. A distributed variant (DDoS) uses multiple sources.

⊗ Sniffing

Intercepting and reading network traffic. Unless encrypted, sensitive information like passwords can be captured, leading to data breaches.

⊗ Spoofing

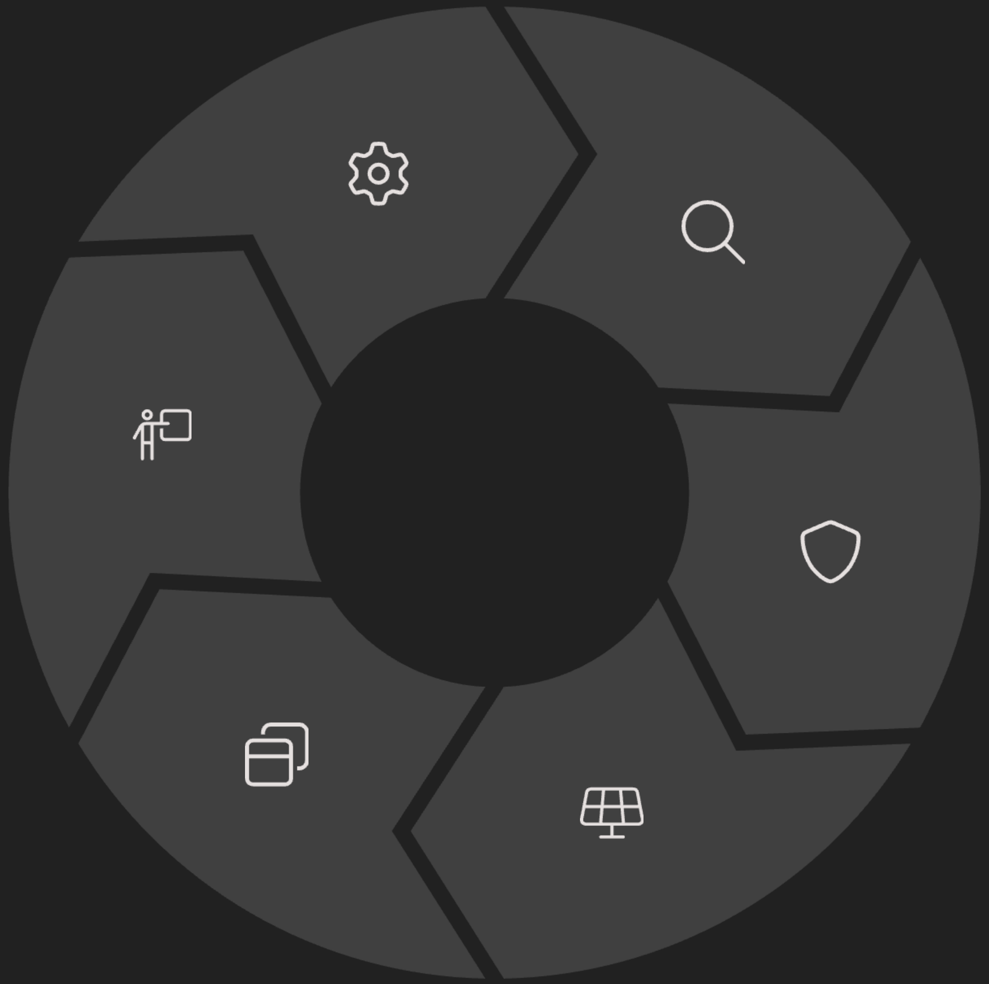
Falsifying identity to deceive systems or users. This can involve IP address spoofing, MAC address spoofing, or email spoofing to gain unauthorized access or trust.

Jaycho Carido

Chapter 3

The Incident Response Lifecycle

When a security incident occurs, a structured approach is vital to minimize damage and learn from the event. This lifecycle provides a roadmap for effective response.



Preparation

Develop policies, train staff, and implement security tools proactively.

Detection & Analysis

Identify suspicious activity and confirm the scope and nature of the threat.

Containment

Isolate affected systems to prevent the incident from spreading.

Eradication

Remove the root cause of the incident, such as malware or attacker access.

Recovery

Restore affected systems and services to full operation, verifying integrity.

Lessons Learned

Review the incident, identify gaps, and update defenses for future resilience.

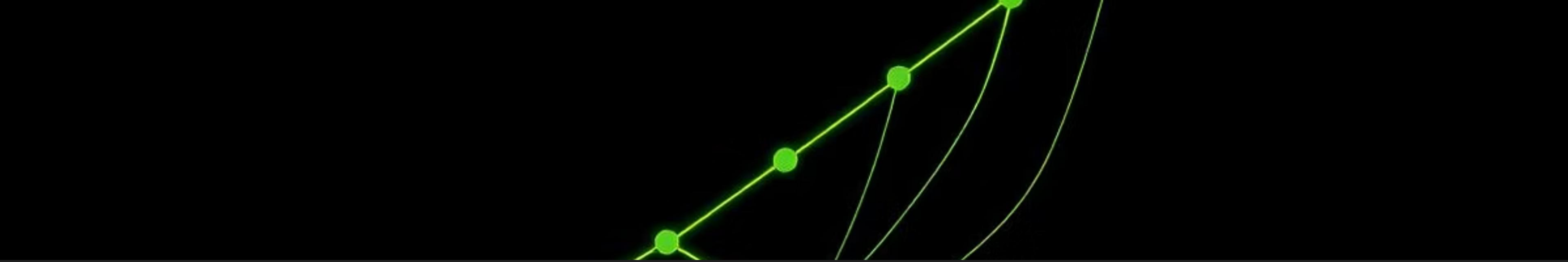
Summary: Key Takeaways

Secure Your Network: Implement a robust defense-in-depth strategy with **firewalls**, **IDS/IPS**, and **VPNs** as core components. Regularly review and update configurations to counter emerging threats.

Know the Threats: Familiarize your team with common attack vectors like **DoS**, **sniffing**, and **spoofing** to anticipate and mitigate risks effectively. Conduct regular security awareness training.

Respond Strategically: Master the **incident response lifecycle** to ensure rapid detection, effective containment, and swift recovery, minimizing business disruption and data loss.

Paul Benjie Bongaos



Continuous Improvement

Network security is not a destination, but an ongoing journey. Regularly assess your defenses, stay informed about the latest threats, and conduct drills to refine your incident response capabilities.

Thank You!

Questions?

Regine Cruda