



# INCIDENT RESPONSE, LESSONS LEARNED AND CASE STUDIES

N2N SECURITY CONSULTANTS


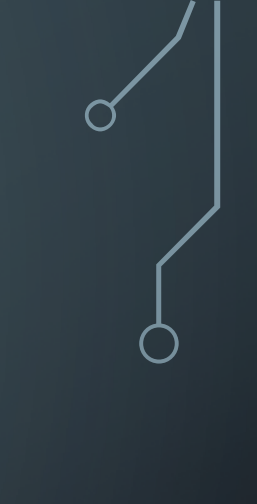

**TLP GREEN**

# ABOUT...

- 18+ years in the IT industry; 10+ in security
- My own boss now 😊 with N2N Security Pacific Consultants
- Security awareness, VAPT; ISO 27001 implementation and audit, mobile and web security, etc
- Partnered with [jimtora@thatsitconsultants.com](mailto:jimtora@thatsitconsultants.com) , That'sIT Consultants on a few projects [www.thatsitconsultants.com](http://www.thatsitconsultants.com)
- [watsoni@n2npacific.com](mailto:watsoni@n2npacific.com) +6797212220



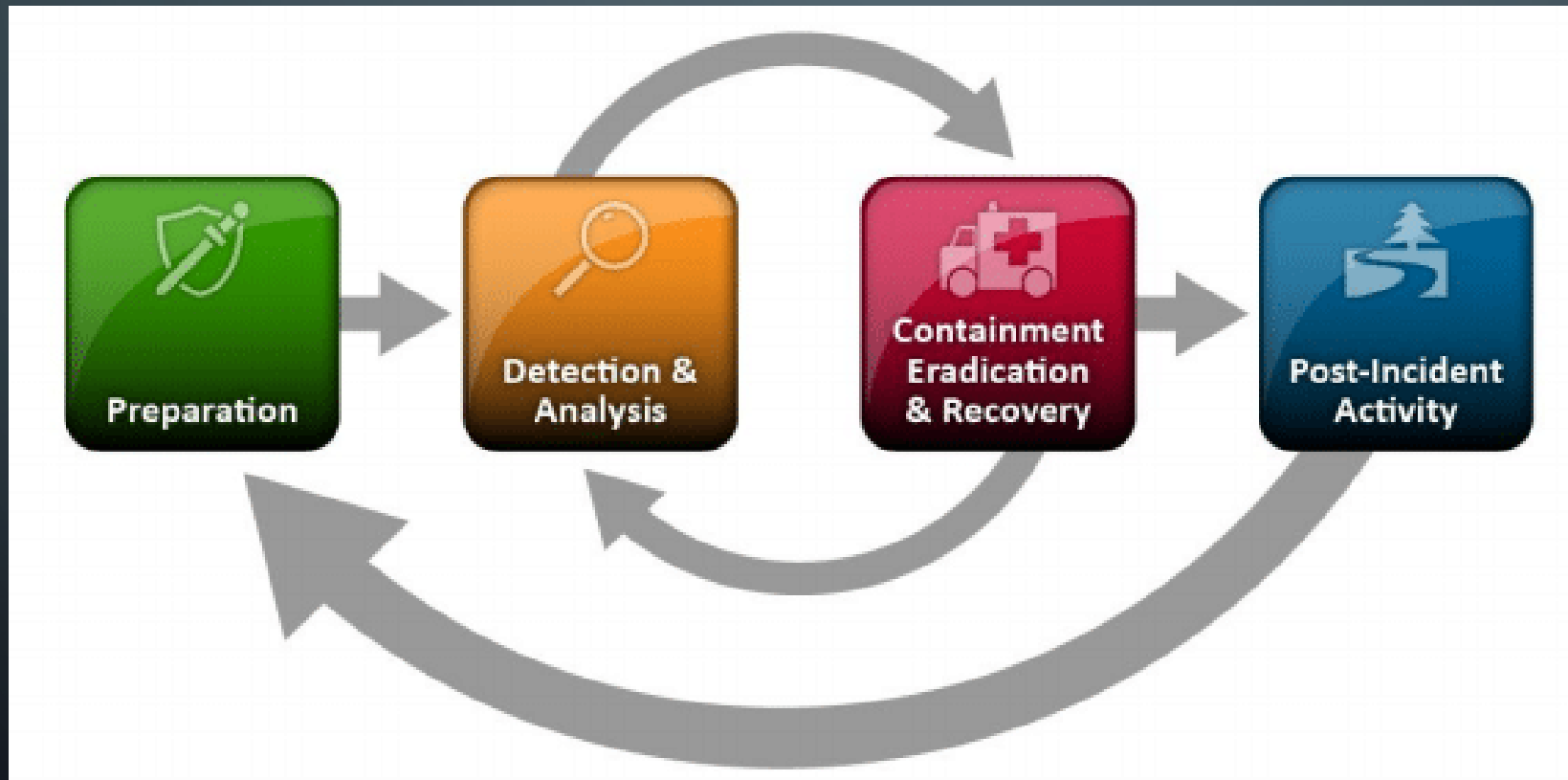
# CONTENT

- Brief overview
  - 2 case studies
  - Lessons learned
  - Recommendations
  - Key trends in IR
- 
- 
- 

# WHAT CONSTITUTES AN INFORMATION SECURITY INCIDENT?

- **any event that threatens the confidentiality, integrity, or availability of information systems and sensitive data, without authorization.**

# INCIDENT RESPONSE PLAN



# 3 PILLARS OF SECURITY

- People - are the most important part of any security program. Users of Technology and follow Processes. Most vulnerable to SE attacks.
- Process – policies and procedures that govern how technology is used and how security incidents are handled. Must be well defined to be effective.
- Technology - are the tools and systems that are used to implement security controls. Eg. Firewalls, IDS, encryption. Etc. Must be correctly placed to be effective.
- The 3 Pillars of Security are interdependent to be effective.
- Orgs need to invest in all 3 pillars of security.



# 2 CASE STUDIES



# CASE STUDY 1

## Case Study Overview

- User accidentally clicked on a phishing email link, which resulted in the installation of malware on their computer.
- The malware then spread to other computers on the network, causing a significant disruption to business operations.



# INCIDENT DISCOVERY

- The incident was discovered when the user reported that their computer was running slowly and crashing frequently.
- The IT department investigated the issue and discovered that the user's computer was infected with malware.
- The IT department also discovered that the malware had spread to other computers on the network.

# INCIDENT CONTAINMENT

- IT department immediately took steps to contain the incident.
- isolated the infected computers from the network and began to investigate the extent of the damage.
- IT department also notified the affected users of the incident and advised them to change their passwords.

# INCIDENT ERADICATION

- IT department began to eradicate the malware from the infected computers.
- used antivirus and anti-malware software to scan the computers and remove the malware.
- IT department also reset the passwords for all user accounts on the infected computers.

# INCIDENT RECOVERY

- Once the malware had been eradicated, the IT department began to recover the affected systems.
- restored the systems from backups and verified that the malware was no longer present.
- also implemented additional security measures to prevent similar incidents from happening in the future.

# LESSONS LEARNED

- Users need to be educated about phishing emails. Phishing emails are one of the most common ways that malware is spread. Users need to be trained on how to identify phishing emails and what to do if they receive one.
- Organizations need to have a security plan in place. A security plan should outline the steps that the organization will take in the event of a security incident. The plan should include procedures for incident detection, containment, eradication, and recovery.
- Organizations need to implement security controls. Security controls, such as antivirus and anti-malware software, firewalls, and intrusion detection systems, can help to prevent and detect security incidents.

# RECOMMENDATIONS

- Provide security awareness training to employees. Employees should be trained on how to identify and avoid security threats, such as phishing emails and malicious websites.
- Implement multi-factor authentication (MFA). MFA adds an extra layer of security to user accounts by requiring users to enter a code from their phone in addition to their password when logging in.
- Use a security information and event management (SIEM) system. A SIEM system can collect and analyze security logs from across the network to identify suspicious activity and potential security incidents.
- Have a security incident response plan in place. The plan should outline the steps that the organization will take in the event of a security incident, including how to communicate with affected users and stakeholders.

By implementing these measures, organizations can reduce the risk of user-caused security incidents and protect their data and systems more effectively.

# CASE STUDY 2

## Case Study Overview

- a SysAdmin accidentally misconfigured a firewall rule, which allowed unauthorized access to the organization's network.
- An attacker was able to exploit this vulnerability and install malware on the network, which resulted in a data breach.

# INCIDENT DISCOVERY

- The incident was discovered when the organization detected suspicious activity on its network.
- The security team investigated the activity and discovered that an attacker had gained unauthorized access to the network.
- The security team also discovered that the attacker had installed malware on the network and had stolen sensitive data.



# INCIDENT CONTAINMENT

- incident was discovered when the organization detected suspicious activity on its network.
- security team investigated the activity and discovered that an attacker had gained unauthorized access to the network.
- security team also discovered that the attacker had installed malware on the network and had stolen sensitive data.

# INCIDENT ERADICATION

- security team began to eradicate the malware from the infected systems.
- used antivirus and anti-malware software to scan the computers and remove the malware.
- Security team also reset the passwords for all user accounts on the infected computers.

# INCIDENT RECOVERY

- Once the malware had been eradicated, the security team began to recover the affected systems.
- restored the systems from backups and verified that the malware was no longer present.
- security team also implemented additional security measures to prevent similar incidents from happening in the future.

# LESSONS LEARNED

- Sysadmins to be trained on security best practices
- Organizations need to have a security plan in place.
- Organisation needs to implement adequate security controls.

## IR PLAN TRENDS:

- Increased focus on prevention – proactive controls eg. Security awareness for employees and automated threat hunting
- Use of AI and ML to automate many tasks involved in incident response such as detecting suspicious activity and triaging incidents.
- Collaboration and communication – Industry CERTS, National CERTs, PACSON, CyberPacific
- Emphasis on recovery – Backup, develop and test IRP, BCP, communication plan for comms with customers and stakeholders etc

# CONCLUSION

- Understand the MITRE ATT&CK Framework
- Implement Security Standards; ISO 27001, NIST 53-800, OWASP
- Conduct table top exercises; ransomware, BCP, etc
- Conduct vulnerability assessments and pentest
- Training and Security Awareness

THANK YOU.