Automated Quarantine Response System

Intro

1	2
Modern networks face fast-spreading malware and worms	Attacks can spread across networks within seconds
3	**4**
Organizations need fast and effective response systems	Automated quarantine helps stop attacks before they become uncontrollable

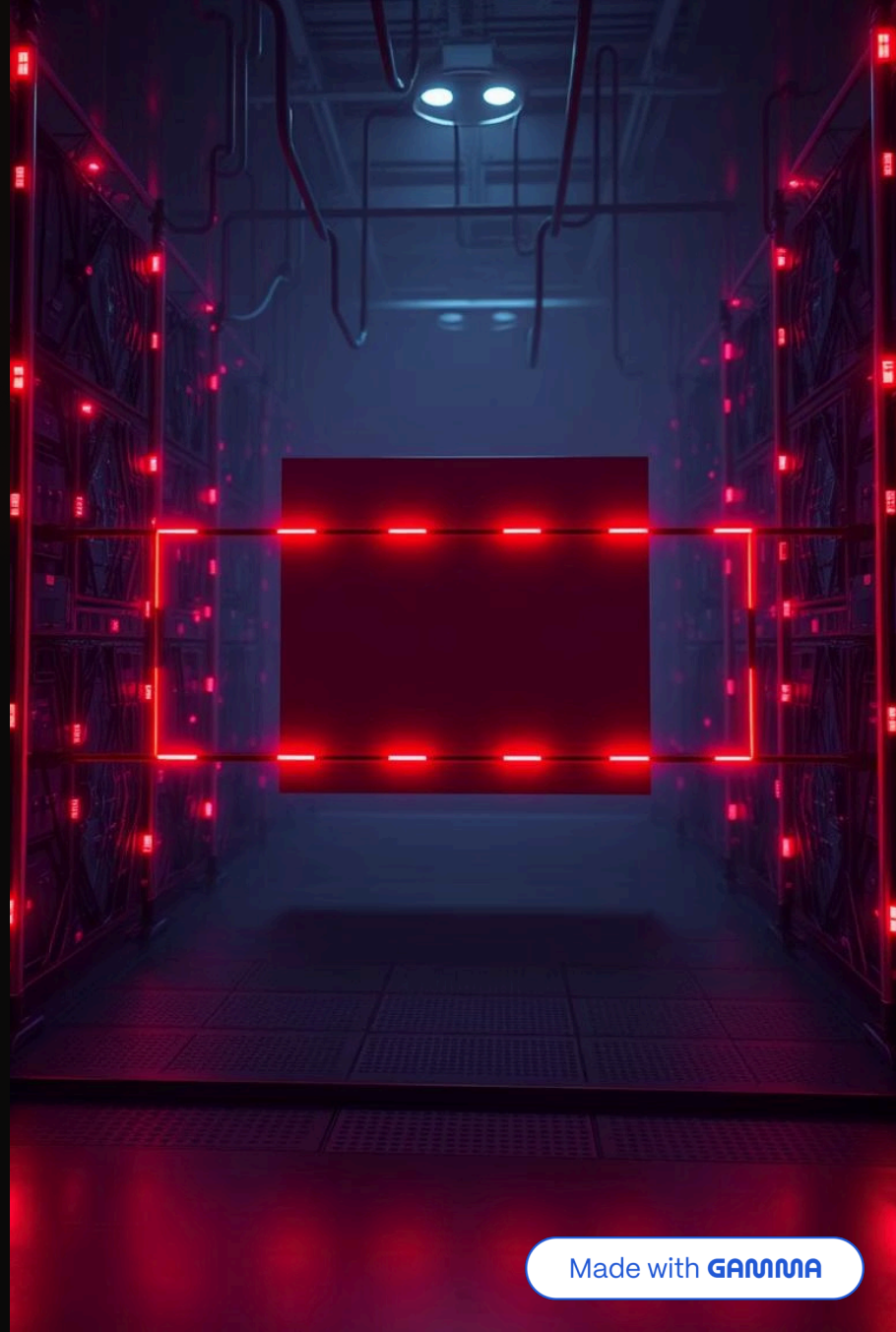
Problem Statement

When a device in a network gets infected
Malware can spread to other devices within seconds
Manual response from security teams is slow
It is impossible to isolate all devices instantly by hand

> Main PROBLEM: Network need automatic containment

What Is an Automated Quarantine System?

- Detects infected or suspicious devices.
- Automatically isolates them from the network.
- Blocks access until issues are resolved.
- Reduces human effort and large scale attacks.



Objectives of the System

Identify abnormal or malicious devices.

Automatically cut communication.

Stop malware propagation.

Protect critical systems and reduce downtime.

How Worms Spread in Networks

- Scan for vulnerable devices.
- Send malicious payloads.
- Exploit open ports and weak security.
- Fast spread requires immediate isolation.

Detection Mechanisms

Traffic monitoring

(sudden spikes)

Port scanning detection

Behavioral analysis

Signature-based detection

Quarantine Techniques

Firewall rules to block IPs.

Move device to quarantine VLAN.

Shut down switch ports.

Apply ACLs.

System Architecture

Monitoring Module

Detection Engine

Quarantine Engine

Logging & Alerts

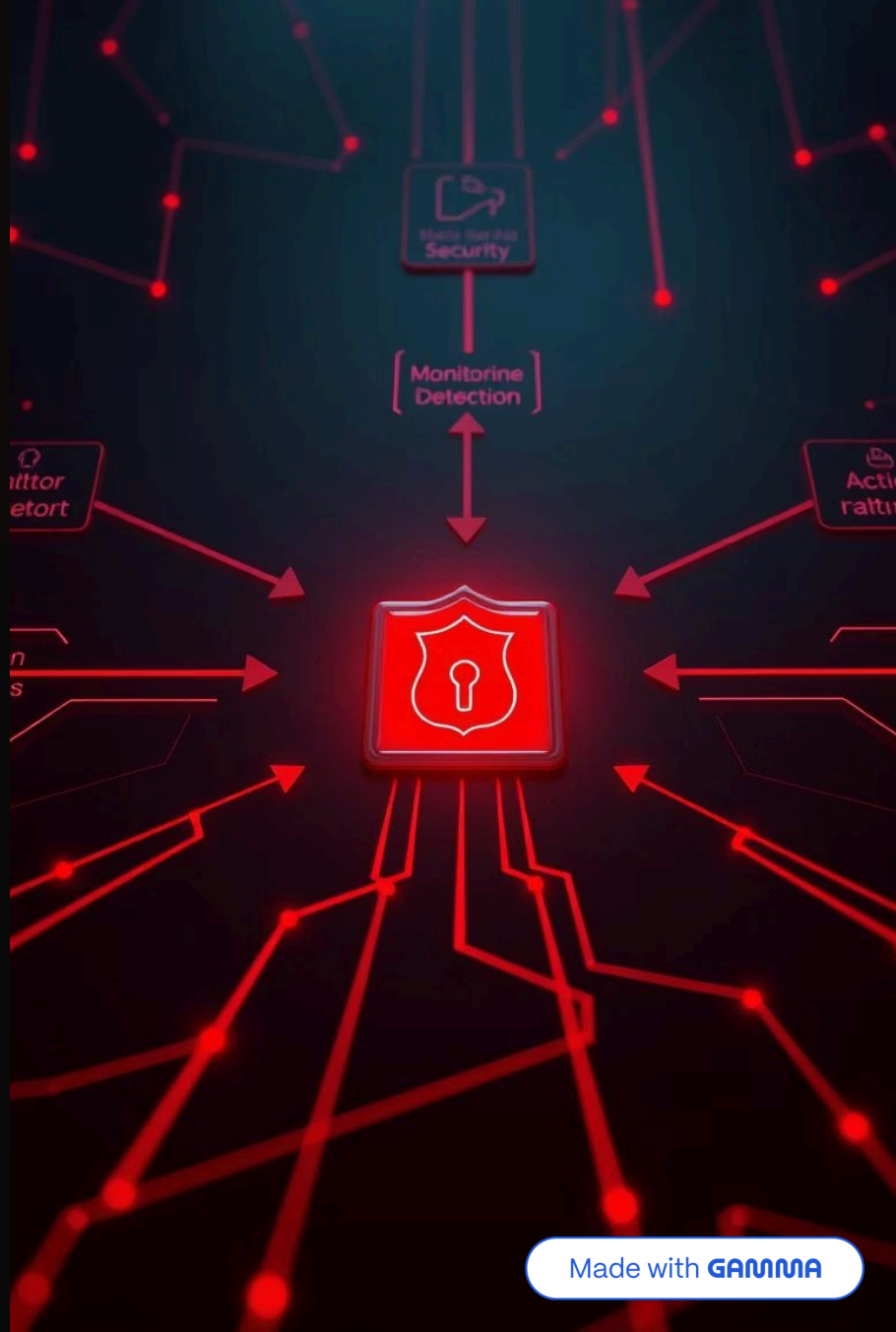
Workflow

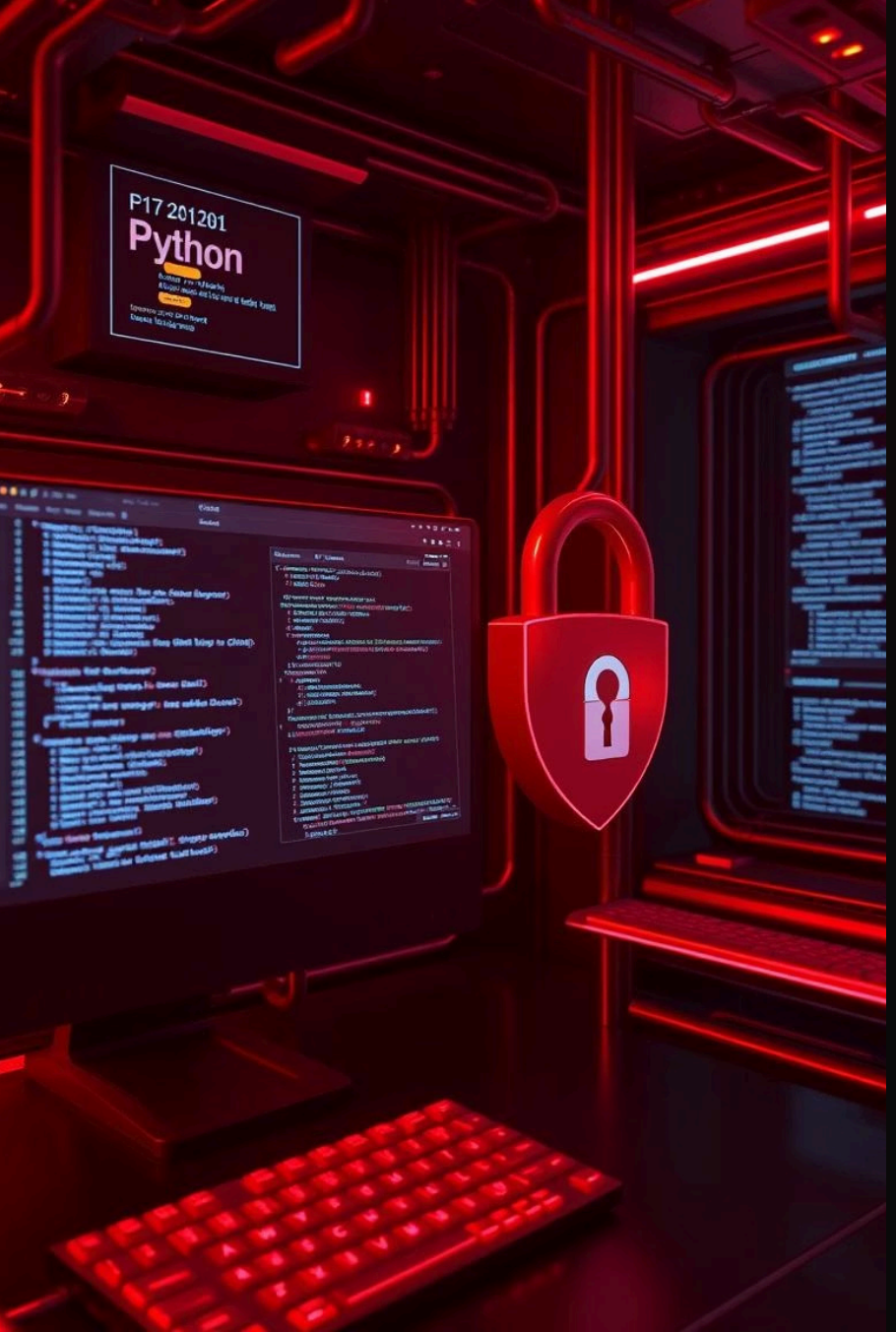
Monitor network devices

Detect abnormal activity

Trigger quarantine actions

Log events and notify admins



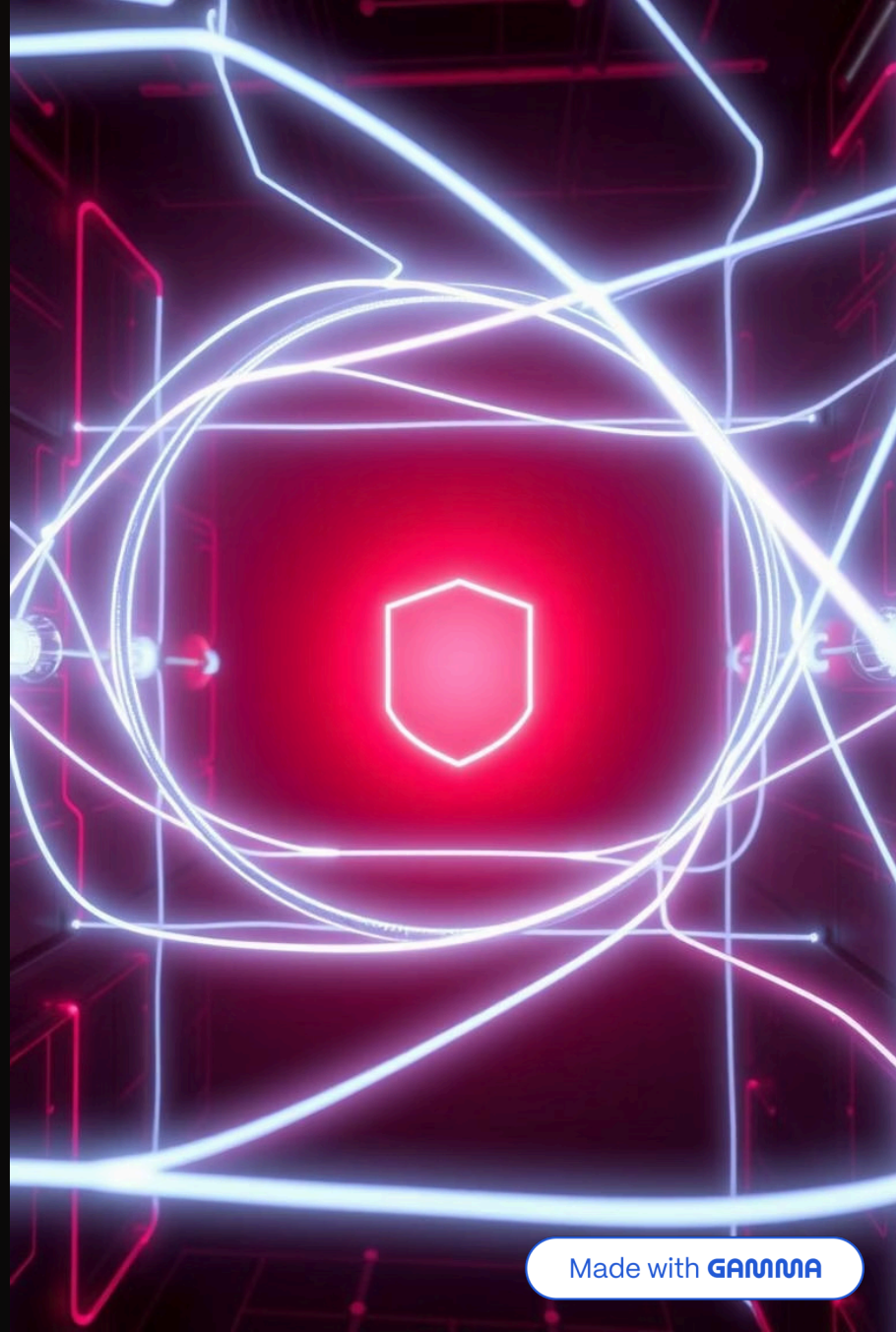


Tools Used

- Python scripting for automation
- nmap for network scanning
- Operating system firewall (Windows / Linux)
- Logging tools for event tracking

Conclusion

- Malware spreads fast.
- Manual response is slow.
- Automated quarantine is essential.
- Improves network security.



Q & A

Thank you. Questions?