

Security Incident Management Workflow – Malware

Detection

Analysis

Containment

Eradication

Recovery

Post-Incident Activities

End User

Help Desk

MSSP/IT Ops

Cybersecurity

IT Operations

CISO

Legal, PR, HR

Sr. Mgmt.

External

