

Client: ABC Retail Corp

Report Type: SOC Incident Summary

Date: 2025-11-18

Threats:

- Malware execution detected from temporary directories.
- Command-and-control communication attempts observed.

Vulnerabilities:

- Endpoint protection signatures outdated.
- Lack of network segmentation.

Security Incidents:

- Two endpoints infected with trojan malware.
- Lateral movement attempts blocked by EDR.

Recommendations:

- Update endpoint security tools.
- Isolate infected systems.
- Conduct employee phishing awareness training.