

Endpoint Compromise Report

Incident Identification

Date/Time of Discovery

Reporter Name/Contact

Endpoint Name/ID

Location/Department

Incident Details

Description of Compromise

Indicators Observed

Date/Time of Compromise (if known)

Initial Detection Method

Actions Taken

Containment Measures

Eradication and Recovery Steps

Further Recommendations

Additional Notes