e-fense
The Global Security Professionals

Suspicious Incident Report©

Summary of Information:

Today's Date: Current Time: Date of Incident: Time of Incident:

Client Information:

Company Name: Address:

Name of Individual Filing Report with e-fense™: Position:

Telephone: Fax: Email:

e-fense™ Response Service: Bronze Silver Gold

Victim System Information:

IP Address: Hostname:

Logon Banner Installed? Impact: Significant Minimal Insignificant

Suspect: Insider External Accessible by Dialup? Dialup Numbers:

Physical Location of System:

Hardware Configuration:

Operating System: Version:

e-fense™ Host Base Monitoring Installed (HBM)?

e-fense™ Internal Intrusion Detection Monitoring System (IDMS™) Installed?

e-fense™ External Intrusion Detection Monitoring System (IDMS™) Installed?

Application(s) of System:

WWW Server: Telnet: Database: Firewall:

Anonymous FTP: News Server: Exchange Server: Gateway:

FTP: Primary PDC: Secondary PDC: Dialup Server:

Sysadmin Name: Sysadmin Tel: Sysadmin Email:

Known Intruder Information

Init IP #1: Init IP #2: Init IP #3:

Hostname #1: Hostname #2: Hostname #3:

Suspected Exploit Used:

e-fense
The Global Security Professionals

Suspicious Incident Report© (continued)

(Details of the Incident)