



Port Scan Alert
Open Relay Alert
Hacked Account
Other Incident
Notification

IDS Alerts
Spectrum Alerts
DoS Detectors
SpamCop
Etc.

Initial
Report &
Analysis

4-HELP
Dept / Org admin
abuse@umich.edu
abuse@med.umich.edu
abuse@engin.umich.edu
CAEN/MCIT/UMnet
Other front-line folks...

Jane User
Dept of Hyperbole
College of Obfuscation

Quick Fix?

Yes

Resolve
& Close

No

Triage &
Referral

Local /
Departmental
Admins

UM Virus Busters

Org/Unit Admin
HITO, EECS, etc.

User Advocate

CAEN / MCIT /
UMnet Admin

UM DPS

ITCS Contract
Services Security
Team

Michnet/
abuse@ISP
abuse@FarEnd.org

U of M IT Security
Team

HW / SW Vendors

Local / State
Police / FBI

Others as
appropriate

Escalate
as needed

Status
Tracking
Statistics

Real-Time
Alerts

Incident status
and stats reports

Strategic
Analysis /
Response

Process Refinement & Training

User Education & Awareness

Auto-detection Rule Revision

Policy Refinement/Overhaul

Incident Prevention/Planning