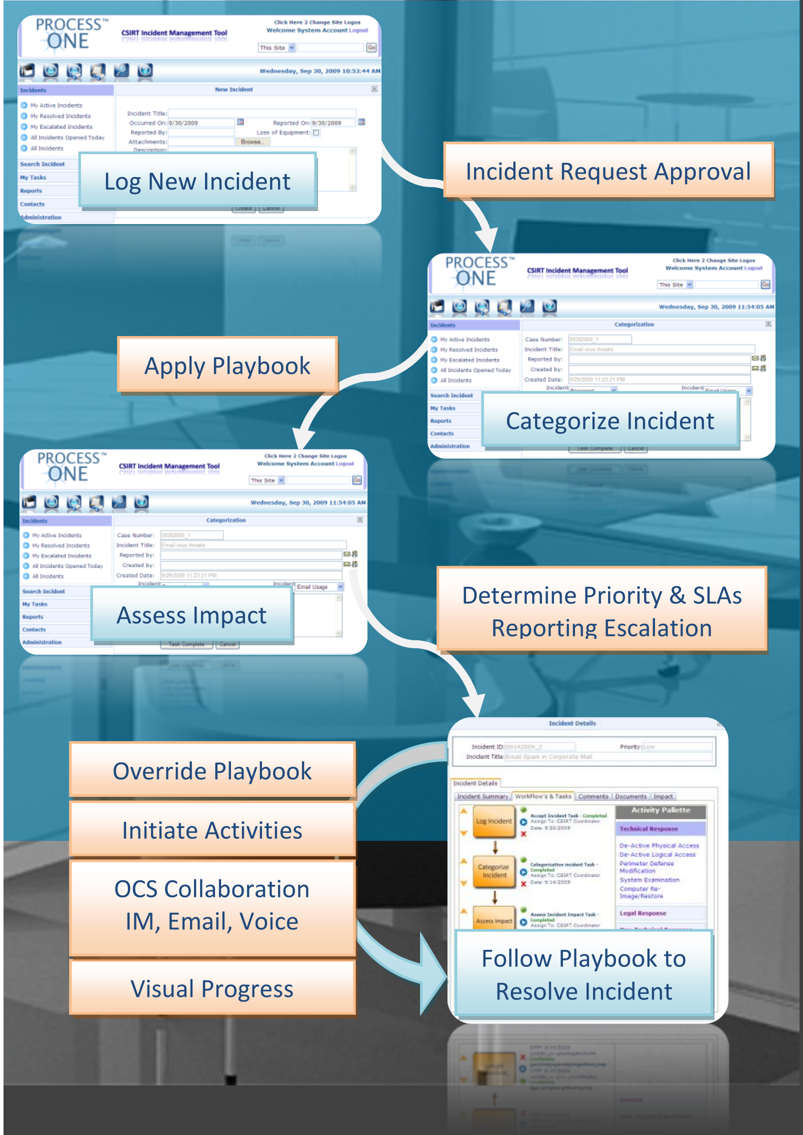
ACM
BUSINESS SOLUTIONS

THE SMART WAY TO MANAGE YOUR COMPUTER SECURITY INCIDENTS



The ProcessOne Enterprise Incident Management Tool (EIMT) is an invaluable asset that facilitates your CSIRT with advanced capabilities and enforces adherence to processes and policies laid out by your *CSIRT Program*

PROCESS™
ONE

Enterprise Incident Management Tool for CSIRTs

Philosophy

Deliver a business solution rather than a software tool.

1. Establish a CSIRT Program
2. Derive CSIRT process guide and playbooks
3. Customize tool for enterprise

Guiding Principles

- Playbook automation
- Enhanced collaboration
- Highly secure
- Extendable workflow paradigm
- Customizable to suit enterprise processes

The Knowledge Advantage

ProcessOne EIMT is the brain-child of 'Security Industry Experts' with decades of experience in the enterprise security incident management domain. Their knowledge has gone into defining best practices and suggesting resolution workflows, also known as Playbooks, for most frequently occurring security incident types. Playbooks are a culmination of CSIRT processes, enterprise departments, employees and incident response team members. Imagine all this knowledge embedded in a tool!

ProcessOne Incident Life Cycle

- ***Incident Request Logging***
  ...configurable data design
- ***Incident Classification***
  ...customized per enterprise
- ***Incident Impact and Triage***
  ...impact analysis parameters
- ***Incident Response***
  ...playbook workflows
- ***Incident Analysis***
  ...reports and BI

Salient Features

- User-role based application dashboards
- Highly configurable yet enforces CSIRT Program policies and processes
- Configurable incident types, impact parameters, playbooks, teams and roles
- Installed with a standard set of incident categories and associated playbooks
- Extendable playbook activities
- Enterprise security and collaboration integration
- Visual incident progress viewer

Technical Architecture

- MOSS* based application
- Web based client access
- MOSS workflow paradigm
- OCS collaboration integration
- Integrated MOSS security
- Audit and reporting features of MOSS
- Flexible process and data architecture

*MOSS: Microsoft Office SharePoint Server
EIMT: Enterprise Incident Management Tool
CSIRT: Computer Security Incident Response Team

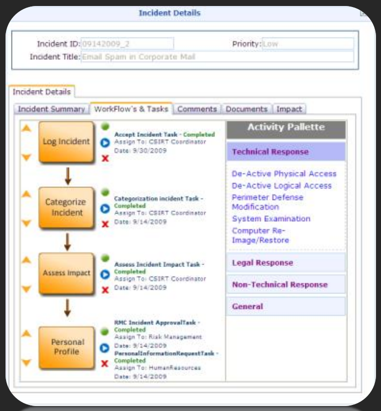
The Paradox: Flexible yet Enforcing

ProcessOne EIMT manages an interesting paradox. On one hand, the tool offers coordinators the flexibility needed to initiate appropriate actions to resolve an incident and on the other hand, the tool's business process management features enforce adherence to the policies and procedures outlined by an enterprise.

Configurable items of EIMT include:

● Incident Categories ● Impact Parameters ● SLAs ● Roles ●
● Departments ● Notification Templates ● Workflow Activities ●

Incident Management Tool: User Interface



Incident Details

Incident ID: 09142009_2 Priority: Low
Incident Title: Email Spam in Corporate Mail

Incident Details

Incident Summary | WorkFlow's & Tasks | Comments | Documents | Impact

Log Incident — Accept Incident Task - Completed; Assign To: CSIRT Coordinator; Date: 9/30/2009

Categorize Incident — Categorization incident Task - Completed; Assign To: CSIRT Coordinator; Date: 9/14/2009

Assess Impact — Assess Incident Impact Task - Completed; Assign To: CSIRT Coordinator; Date: 9/14/2009

Personal Profile — RMC Incident ApprovalTask - Completed; Assign To: Risk Management; Date: 9/14/2009; PersonalInformationRequestTask - Completed; Assign To: HumanResources; Date: 9/14/2009

Activity Pallette

Technical Response

De-Active Physical Access
De-Active Logical Access
Perimeter Defense Modification
System Examination
Computer Re-Image/Restore

Legal Response

Non-Technical Response

General

ProcessOne EIMT presents an intuitive user interface that makes managing incidents easy and efficient. OCS based collaboration features enable e-mail, instant messaging, voice and conferencing with contextual reference to an incident.

Tool Deployment and Support Services

Deployment Options:

● On Premise ● On Demand (SaaS)

Deployment & Support Services:

● CSIRT Program Consulting → CSIRT Process Guide
● ProcessOne EIMT Deployment
  ● Playbook Analysis
  ● ProcessOne EIMT Data Customization
  ● ProcessOne EIMT Process Customization
● ProcessOne EIMT Beta Run
● User Acceptance
● Maintenance & Support

Playbook

Definition:- A notebook containing descriptions and diagrams of the plays that a team has practiced

Playbook in a CSIRT Tool Context:- A set of activities recommended to be taken up in a specific sequence in order to resolve an incident.

ACM
BUSINESS SOLUTIONS

407 Wekiva Springs Rd Ste 241
Longwood Fl 32279, USA
Phone: 407-788-1505
Fax: 407-788-0316

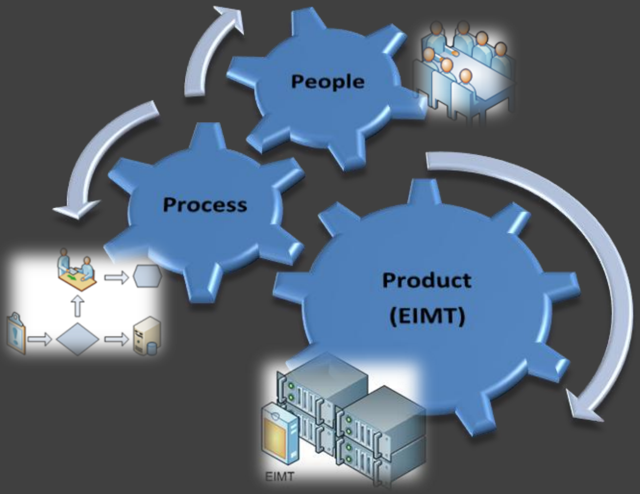
www.acmbs.com

CSIRT
PROGRAM

Malicious acts and intrusions occur despite the best of information security infrastructure. It is critical for an enterprise to have an efficient way to respond when security incidents occur.

CSIRT* is a service entity that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Our 'CSIRT Program' offering, equips an enterprise with security related incident handling capabilities; defines CSIRT and associated teams, processes and responsibilities. It is an enterprise specific implementation of security incident handling best practices delivered in the form of an actionable process guide. Once implemented, the CSIRT program will help limit the damage and lower the cost of recovery by increasing process efficiency to recognize, analyze, and respond to an incident

ProcessOne EIMT complements your enterprise CSIRT program by providing the 'IT Toolset' that is required to handle incidents efficiently. Our experienced security domain consultants can help in setting up a CSIRT program for your enterprise coupled with the advantage of EIMT, thus making the approach holistic in terms of processes, people and IT product technology.


People
Process
Product
(EIMT)
EIMT