

# OPERATIONS MANUAL: IPC - Stage One

Hal Flynn 2000-05-11

## Operations Manual Information Protection Centre Stage 1 - Active: Assessment Phase

---

### Stage 1 - Active: Assessment Phase

**Auto-Response IDS:** Many ID systems can be set up to automatically respond with some predefined set of activities upon detection of specified events. In this case some reasonable assessment process must be carried out ahead of the incident. The business impact of highly malicious events is pre-assessed and it is decided that the cost of a false positive is outweighed by the impact of a successful occurrence of the specified event. For example it may be better to block the source IP address(es) when an obvious denial of service is coming at you. Some ID systems can change the access control lists in a filtering router to block or shun addresses. Then again some of those source addresses could be faked, spoofing some business partners. In this case you would be then be creating your own denial of service.

- You would want to be notified of this auto-response, assess business impact and whether some other longer term response is necessary (e.g. track back to real source and work with ISPs to close attack down).

**Correlation of Incident Detection:** The IPC's sources of event logs, historical incident results and network mapping information need to be correlated to assess the validity of an incident, its source(es) and its potential impact on business operations. It may also be necessary to analyse whether it is a single large scale attack or a set of unrelated attacks at the same time.

- correlation of widespread activities:
  - all monitoring engines of a particular type of vendor alarm to the same console so widespread activities are depicted in the display
  - as alternative ID systems are deployed then effort will have to be made to observe the events on all systems to determine the scope and characteristics of detected activities
  - new products are emerging that can bring together a variety of event sources (e.g., SYSLOG, IDS logs, firewall logs, etc.).

**Triage activities and assessment activities:** Detected incidents act as indicators and warnings to the IPC. They are reviewed collectively in order to assess the events and apply an order of importance, then determine the appropriate response. In extreme cases the incident and its response must be escalated beyond that of the IPC's normal jurisdiction. Such cases would be handled by a triage group composed of local and national law and order organisations such as Intelligence Communities (DND , CSE and CSIS), Police and RCMP, as well as members of the legal community, are required to collaborate in ensuring that there is formulation of an appropriate response to major events.

- the procedures for containment and eradication should be kept up to date and a paper copy retained
- there needs to be a decision point where other IPCs/CIRTs are notified
- there needs to be a decision point at which the CIO and/or police are informed

**Escalation Levels:** Winn Schwartz has proposed a cyber defense model similar to the "DefCon" levels of escalation used by the U.S. Military. His "CyCon" model for organisations is as follows:

- noise level, no detected attacks
- unauthorized scans, sporadic attacks detected
- coordinated hacking attempts or DoS detected
- successful attack(s) detected, containment, eradication and recovery necessary
- under heavy assault, facility shutdown required

---

[Admin](#)   [Passive](#)   [Protective](#)   [Detective](#)   [Responsive](#)   [Integrative](#)

Original development of these pages was supported by  
the Province of Manitoba

The content is maintained by [Andrew Mackie](#)

*Last modified: April 29, 2000*

[Privacy Statement](#)

Copyright 2006, SecurityFocus