

OPERATIONS MANUAL: Stage 1 - Active: Protection Phase

Hal Flynn 2000-05-11

OPERATIONS MANUAL Information Protection Center

Stage 1 - Active: Protection Phase

The IPC's goal is to continuously improve the organisation's security posture. The most important step in this is to establish strong protection. This protection comes from knowing the threats and countermeasures, being aware of the organisation's vulnerable assets and implementation of controls to protect these.

Environmental scanning: The members of the center must remain vigilant and aware of the rapidly evolving security environment. The Centre must carry out environmental scanning for both new threats and new vulnerabilities. The IPC must be aware of new products, tools or software patches that become available to counter many of these threats or vulnerabilities. This is done via review of newsgroups, Internet news feeds, peer networking and paper media. Membership in FIRST will provide access to news of security incidents from other Incident Response organisations.

- at least 1 person should read CERT, CIAC, Security Focus, Bugtraq, SANS, ISS, etc. for latest vulnerabilities and distribute them to those affected (this role could move to a central agency which disseminates info daily)
 - threat briefings by co-ops draw from www.cert.org, www.ciac.org, www.microsoft.com/security, bugtraq, www.securityfocus.com, www.sans.org and [ISS X-force mailing lists](http://ISS-X-force mailing lists) as well as www.msnbc.com and www.cnn.com

Vulnerability Analysis (VA): Continuous Vulnerability Analysis is to be applied to the organisation's dedicated segments and special highly critical resources in order to maintain a good understanding of the overall security posture of the organisation. The VA finds network vulnerabilities that are the result of misconfiguration of the operating system and network protocols; ranging from improper configurations of hosts, faulty applications, malicious code, all the way to deliberate denial of service attacks and data tampering. A VA capability is a separate and unique network service, available to system administrators to raise the security level of the whole network. VA is a specific activity that is performed at the network level. VA is a distinct

and vital activity within the IPC.

- The generic process that the IPC's VA Team will follow in conducting vulnerability analyses is based upon the following operating model. This model is defined as the "5A"s: Access, Assess, Analyze, Act and Automate.
- This process is technology independent. Various software VA tools and toolkits will be used to probe the network and check the presence of vulnerabilities.
- A VA activity will always be planned in conjunction with the concerned system administrator. Discussions on timing, schedule, bandwidth impact, and storage of results will be resolved before initiating a VA.
- The IPC will perform security audits, both at the user and network level, when requested by an organisation. This could involve policy formulation, examine procedures, and suggesting improvements. The IPC will not perform "tiger team" attacks unless so directed by the CIO.

Rules of Engagement (RoE): The rules of engagement are reflected in the automated implementation of policies in code or filters applied to control mechanisms within the architecture. The rules of engagement are derived from a synthesis of the IPC's awareness of the security environment, the architectural configuration and the VA results. These rules of engagement are programmed or configured into the security mechanisms of Intrusion Detection Systems and Firewalls.

- policies and activity logs should be reviewed regularly and policies updated as necessary
- changes to policies (e.g., router ACLs, Firewall configurations, IDS policies) must be documented in the daily log of IPC activities, signed by initiator and co-signed by IPC Director
- the RoE and IPC's role must be advertised to Sys Admins., Support Organisations and users
 - services will be denied to minimize the risk so the value of the IPC and its security enforcement must be sold

Firewalls: The IPC acts as a Point of Contact for providing firewall policy guidance or specifications and auditing firewall services. In cases where firewall management has been outsourced you will need to seek contractual agreements that allow the IPC to determine policy, audit compliance, review logs in a timely manner and be notified whenever there may be any security issue that could impact performance.

Requests: The IPC acts as a Point of Contact for security reporting and assistance. Those that would like ad hoc vulnerability probing and help with securing their systems can request these services of the IPC. These services will be provided in as timely a manner as possible, depending on current workload.

- new installation audit checks
- Security Posture Analyses (SPAs) to set baselines
- establish departmental security Point of Contacts to act as intermediary between departmental users and IPC

[Admin](#) [Passive](#) [Detective](#) [Assessive](#) [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