7.1. Detecting Information Security Incidents

Objective

7.1.1. Organisations have implemented tools, processes and procedures to detect information security incidents, minimise their impact and have these activities embedded as part of IT governance.

Context

Scope

7.1.2. This section covers information relating to detecting information security incidents. Detecting physical and personnel security incidents is out of scope of this section, unless there is an impact on information systems. Refer to Chapter 8 - Physical Security and Chapter 9 - Personnel Security.

7.1.3. It is important to note that in most cases, information systems are likely to be affected.

7.1.4. Additional information relating to detecting information security incidents, and topics covered in this section, can be found in the following sections of this manual:

- Section 5.9 - Vulnerability Disclosure Policy;
- Section 6.1 - Information Security Reviews;
- Section 6.2 - Vulnerability Analysis;
- Section 7.2 – Reporting Information Security Incidents;
- Section 7.3 – Managing Information Security Incidents;
- Section 9.1 - Information Security Awareness and Training;
- Section 16.6 - Event Logging and Auditing;
- Section 17.9 – Key Management; and
- Section 18.4 - Intrusion Detection and Prevention.

References

7.1.5. Standards and guidance published by Standards Bodies and industry groups include:

Reference	Title	Publisher	Source
ISO/IEC 27035-1:2023	**Information technology — Security techniques — Information security incident management — Part 1: Principles and Process**	ISO	ISO/IEC 27035-1:2023 - Information technology — Information security incident management — Part 1: Principles and process
ISO/IEC 27035-2:2023	**Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response**	ISO	ISO/IEC 27035-2:2023 - Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response
	Definitions of Computer Security Incident	NIST	https://csrc.nist.gov/glossary/term/Computer_Security_Incident
SP 800-61 rev.2	**Computer Security Incident Handling Guide**	NIST	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [PDF, 1.5 MB]
	US-CERT Federal Incident Notification Guidelines	CISA	https://us-cert.cisa.gov/incident-notification-guidelines
	NCSC Incident Management Be Resilient Be Prepared	NCSC	https://www.ncsc.govt.nz/protect-your-organisation/guides/incident-management-be-resilient-be-prepared/
	Cyber Security Incident Response Guide	CREST	Implementation & Procurement Guides - CREST
	Good Practice Guide for Incident Management	ENISA	Good Practice Guide for Incident Management | ENISA
	Vulnerability Disclosure for Security researchers	CISA	security.txt: A Simple File with Big Value | CISA

PSR references

7.1.6. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV6, GOV7, INFOSEC1 and INFOSEC4	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements

Rationale & Controls

Preventing and detecting information security incidents

7.1.7.R.01. **Rationale**

Processes and procedures for the detection of information security incidents will assist in mitigating attacks using the most common vectors in systems exploits.

7.1.7.R.02. **Rationale**

New or advanced attacks and exploits can frequently be detected through other metrics and effects, rather than direct identification. For example, unexpected spike in network traffic or network latency, unapproved changes in file permissions, unexpected high utilisation of computing resources etc.

7.1.7.R.03. **Rationale**

Potential information security incidents are detected by both personnel and automated incident detection tools.

1. Personnel should be well trained and aware of information security issues.
2. Automated incident detection tools should be utilised to assist in developing use cases and a known baseline. Management and operation of the tools should be undertaken by experienced information security personnel.

7.1.7.R.04. **Rationale**

Agencies may consider some of the tools described in the table below for detecting potential information security incidents.

Tool	Description
Next-Generation Firewall (NGFW)	NGFWs can provide dynamic network defence by combining application/cloud service level control and dynamic threat feeds with signature or other anomaly detection to help prevent malicious connections to the network, or users connecting to malicious or non-approved cloud services. NGFWs may be deployed as cloud services (i.e. cloud firewall or firewall-as-a-service) or as a hardware or software appliance.
Protective DNS	Protective DNS provides real-time secure DNS resolver checks for domains and IP addresses against known malicious entities.
Threat Intelligence Platform (TIP)	TIPs enable an automated means to collect, analyse and manage threat data received from various intelligence sources to enrich prevention and detection capabilities.
Network and host Intrusion Detection Systems (IDSs)	Monitor and analyse network and host activity, usually relying on a list of known attack signatures to recognise/detect malicious activity and potential information security incidents.
Cloud threat detection capabilities	Enable, monitor and tune the threat detection capabilities of respective cloud services to detect threats and create high-quality alerts from log data or agents for cloud workloads and identity providers.
Anomaly detection systems	Baselines normal host and network activity and identifies events that deviate from expected patterns of activity .
Endpont Detection and Response (EDR) /Extended Detection and Response (XDR	Endpoint Detection and Response (EDR) provide host based threat detection and response that provide real-time monitoring and analytics. Extended Detection and Response expands on the functions of EDR to distinct security capabilities within your organisation.
Log analysis	Involves collecting and analysing event logs using pattern recognition to detect anomalous activities.
Application Allow listing	Lists the authorised activities and applications and permits their usage.
Security Information and Event Management (SIEM)	SIEM solutions provide centralised platform for log collection, storage, alerting and detection of security threats.
Data Loss Prevention (DLP)	DLP solutions identify and prevent sharing or transfer of sensitive information.
security.txt	Internet standard RFC 9116 defines a way for organisations to disclose their vulnerability disclosure practices.

7.1.7.R.05. **Rationale**

Automated tools are only as good as their implementation and the level of analysis they perform. If tools are not configured to assess all areas of potential security risk then some vulnerabilities or attacks will not be detected. Maintenance of the tools is important to ensure that emerging threats and vulnerabilities are able to be identified. Failure to do so will reduce the effectiveness to identify vulnerabilities.

7.1.7.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:1153]

Agencies MUST develop, implement and maintain tools and procedures covering the detection of potential information security incidents, incorporating:

- user awareness and training;
- counter-measures against malicious code, known attack methods and types;
- intrusion detection strategies;
- data egress monitoring & control;
- access control anomalies;
- audit analysis;
- system integrity checking; and
- vulnerability assessments.

7.1.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1154]

Agencies SHOULD develop, implement and maintain tools and procedures covering the detection of potential information security incidents, incorporating:

- user awareness and training;
- counter-measures against malicious code, known attack methods and types;
- intrusion detection strategies;
- dynamic network defence (i.e. protective DNS and/or NGFW)

- data egress monitoring & control;
- access control anomalies;
- audit analysis;
- system integrity checking; and
- vulnerability assessments.

7.1.7.C.03. **Control System Classifications(s): All Classifications; Compliance: Should [CID:1155]**

Agencies SHOULD use the results of the security risk assessment to determine the appropriate balance of resources allocated to prevention versus resources allocated to detection of information security incidents.