Security Incident Management

ReadiNow INNOVATE

Security Incidents

Report and manage IT Security Incidents, this module has been designed specifically for these types of events.

Functionality

- ✓ Ability to record and track security events either manually or from external sources (example, SIEMs).
- ✓ Ability to configure event attributes to match the source system.
- ✓ Ability to identify key attributes such as Host Name, Source Type, Domain, Logon ID, Event Message, Event ID (unique key) and Linked Assets.
- ✓ Simplified incident recording screen and button to assist end users in reporting security incidents easily
- ✓ Ability to record Security Incidents in a centralised repository to effectively respond to threats and reduce the impact on the organisation.
- ✓ Ability to link one or more security events to a given security incident to provide required information for Security Engineers and/or analysts to perform time critical remediation actions.
- ✓ Ability to automatically link affected technology affects (Devices, Application and Information Assets) to an incident based on the information available in Security Events.
- ✓ Ability to classify security incidents to various categories such as APT, Denial of Service, etc. for better understanding the impact of attack.
- ✓ Ability to document the attack vectors if known. Such as Ad-based malware, attrition, etc.
- ✓ Ability to rate business impact and priority to easily manage the incident queue.
- ✓ Ability to flag if there is a potential data loss or chance of data loss.
- ✓ Ability to configure necessary reminders or alerts to stakeholders (owner, reporter, business unit/department lead, etc.)
- ✓ Ability to manage incident lifecycle through various stages.
- ✓ Ability to manage the above stages via built in work-flow process including notifications and alerts (emails) if necessary.
- ✓ Ability to forecast the overall time required to complete actions identified to respond to the incident - depending on the sequence of actions.
- ✓ Ability to measure individual stage times.
- ✓ Ability to measure end to end elapsed time.
- ✓ Ability to provide overall performance metrics of security incidents by summarising time to respond, time to prepare, etc.
- ✓ Ability to download incident details that can be distributed outside of the organisation. Example, a formatted Incident Report using Microsoft Mail Merge functionality.

Investigations

Conduct investigations to determine the root-cause of incidents.

Functionality

- ✓ Ability to conduct independent investigations to determine root-cause of incidents
- ✓ Ability to identify submitter and investigator for each investigation record
- ✓ Ability to specify the priority of the investigation depending on the impact of the incident and/or external requirements.
- ✓ Ability to record interview and conversations with personnel related to the incident.
- ✓ Ability to record resolution steps (initial response and others) to the incident to provide complete visibility to the investigator
- ✓ Ability to store documents (or attachments) that may be required to be presented to various parties including external/regulatory bodies.
- ✓ Ability to conduct risk assessment based on likelihood of this incident happening again and the impact it could have.
- ✓ Ability to define and allocate action plans/tasks to individuals to perform to mitigate the effects of the incident.

Security Roles

General Users - Security Incident Security Analyst	Create, view and edit access to Security Incidents - to report incidents. Access granted to General Users and create, view and edit access to Action Library, Control, Incident Action, Lessons Learned, Security Events, Security Incident and Technology Risk (all of the above only if they are assigned as an analyst for a given Security Incident).
Security Incident Managers	Access granted to Security Analysists and create, view and edit access to Action Library, Incident Action, Incident Analysis, Lessons, Security Events and Security Incidents.
Administrator	Administration access to all objects and ability to make configuration changes