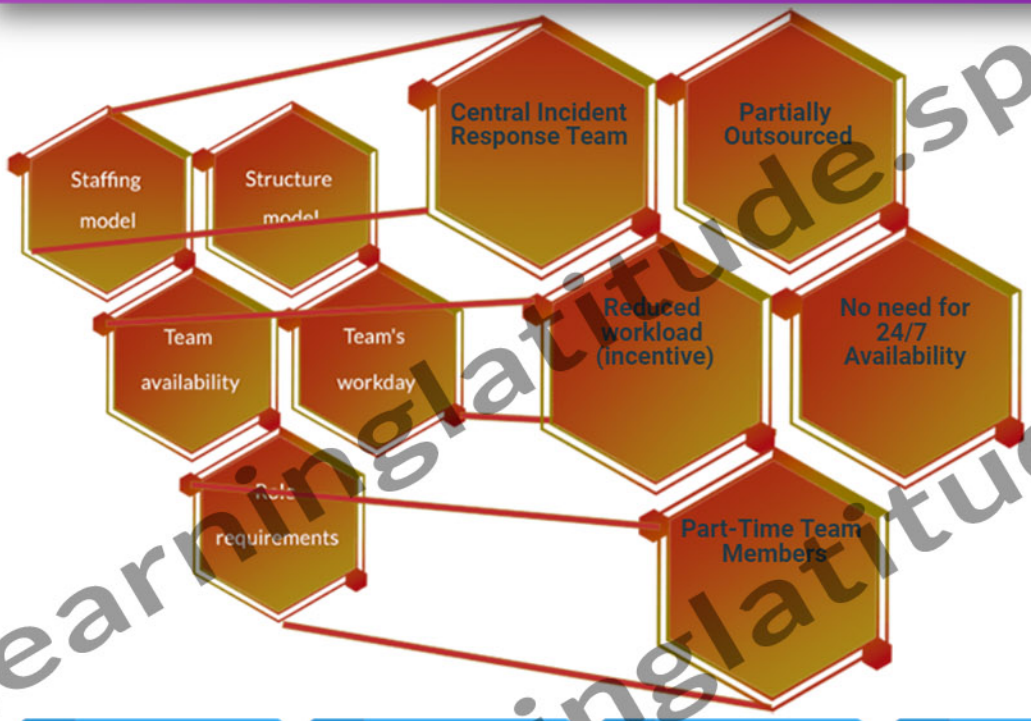
Complete

Incident Response Team



Print/Save Analysis

Continue

Once you click on the "Continue" button you will not be able to change the team's choice.

If you need to make a change use the buttons at the bottom.

Update Staffing Model | Update Structure Model | Update Team availability | Update Team's workday | Update Role requirements

Decision-making

email

Attack Vectors & Impact

Productivity	Less than 1% of systems; less than 1% of workforce	More than 1% workforce, but less than 10% of systems	More than 1% systems but less than 10% of workforce	More than 10% of systems; more than 10% of workforce	N/A
Widespread	Minimal	Moderate	High	None	N/A
Commonality	Commonly Seen	Occasionally happens	Rare	Never	N/A
Damage	Minimal	Moderate	High		N/A
Affected Parties	Less than 1% of systems; less than 1% of workforce	More than 1% workforce, but less than 10% of systems	More than 1% systems but less than 10% of workforce	More than 10% of systems; more than 10% of workforce	N/A
Business Impact	Minimal	Moderate	High		N/A

After you complete your selection of choices for this table, please click "continue" to advance to the next section. All decisions are final and you can Not go back to modify them, after advancing

Continue

Complete

Attack Vectors & Impact

Attrition	Severety	0
External/Removable Media	Severety	0
Web	Severety	0
Email	Severety	12
Impersonation	Severety	0
Improper usage	Severety	0
Loss or theft of equipment	Severety	0
Other	Severety	0

Priority Guideline	Score
Severity High: Loss of a major service	12

Initial action	Containment Goal
Immediately	<24 Hours

Print/Save Analysis

Continue

Decision-making

Checklist

Attack Vectors & Impact

	Choose Y/N	Write your comments
First person to observe incident at LOCATION follows local emergency procedures and notifies the IRT and/or building security of incident.	No	No, the user comments to a colleague with more technical expertise
The IRT assembles, investigates the incident and severety using the "Impact table".	Yes	Yes, in the email analysis
The IRT determines the SOP to be activated.	No	Not yet

Continue

Decision-making

Checklist

Attack Vectors & Impact

	Choose Y/N	Write your comments
The POC launches a notification process to all functional department heads.	No	No
The POC launches a notification process to third-party if it's needed.	No	No. Is needed a notification to: 1. email provider's SMTP server 2. firewall provider firewall.firm.in/software-firewall/
The POC launches a notification process to Law enforcement agency if it's needed.	No	Not needed

Continue

Print/Save Analysis

Analysis 1/4

SOP

Standard Operating Procedure

Open the file "**Company policy**" and answer the next questions

Company policy

	Choose Y/N	Write your comments
The users incur in any violation of the company's policy?	No	No
The policy was enough or complete to prevent the incidents described in the scenario?	No	No, is incomplete. It's not enough to prevent threats in this scenario neither to guide the user's behavior.

Continue

Analysis 3/4

SOP

Standard Operating Procedure

The IT department has developed some standard operation procedures (Playbooks) that your team has adopted.

Read the SOP's

Assign the SOP adequate to respond to the incident

Remote Access Trojan (RAT)

Phising

Denial-of-Service (DoS)

Denial-of-Service DoS — No Assign

Phishing — Assign

RAT — No Assign

Print/Save Analysis

Continue