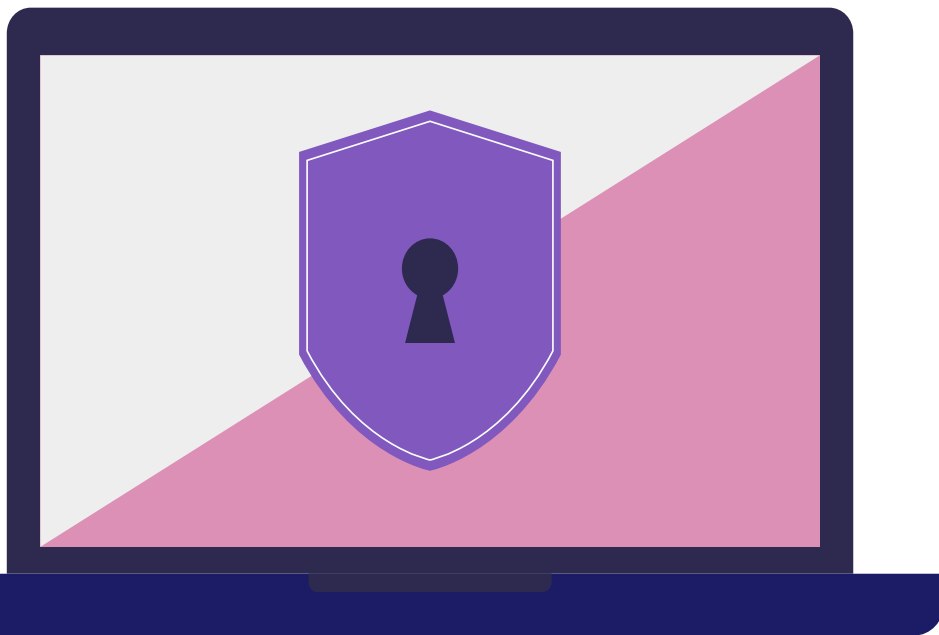


# Incident Response Plan For Ransomware

## Pure Secure Solutions



**Presented By:**

**Presented To:**

Mahtabul Bari

Hendra

Hendrawan

Deepshikha

Kajal Sodhi

Arshjeet Kaur

Aparna Pavitra Palem

Rahul Vaniya

# Table of contents

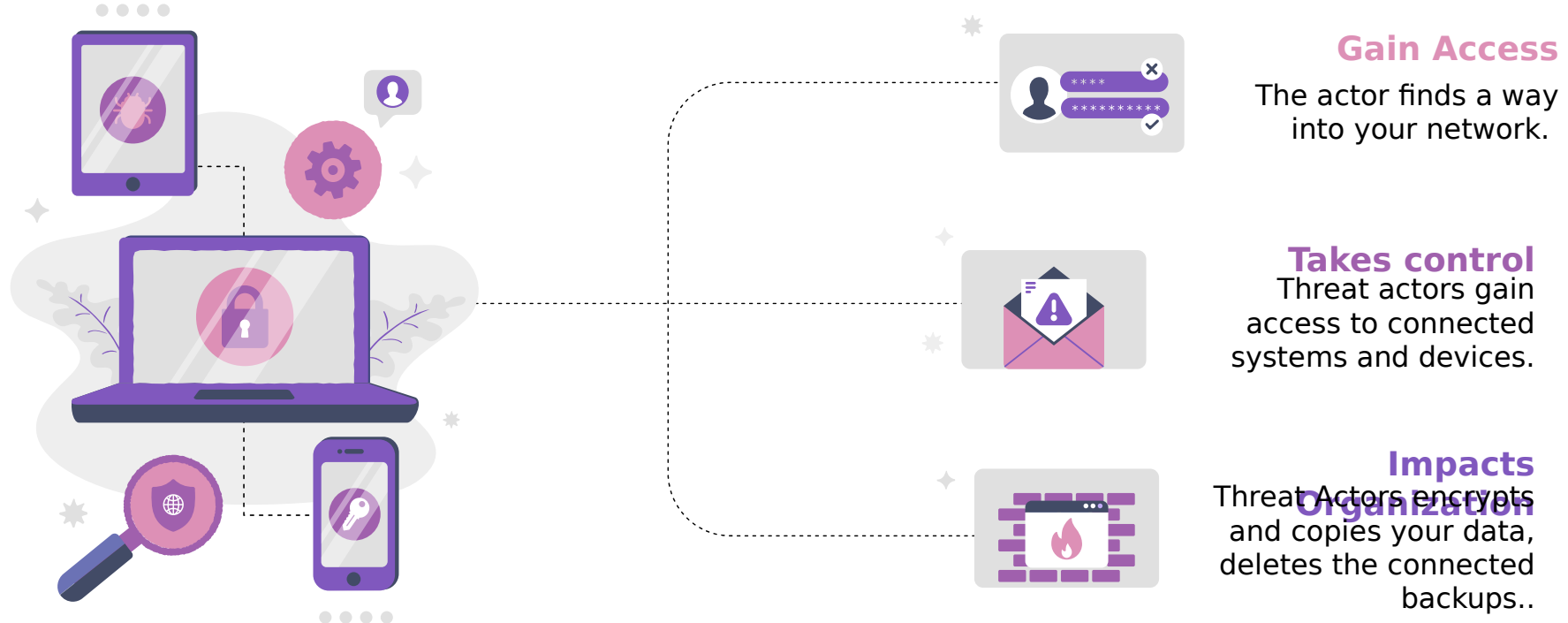
Introduction	3
How does it occur	4
Incident Response plan phases	5
IRP Checklist for Ransomware	6
Preparation for IRP of Ransomware	7
Monitor and Inspect	8
Understanding the IRP for Ransomware	9
Detection and Analysis	10
Containment and Eradication	11
Recovery plan	12
References	13

# Introduction

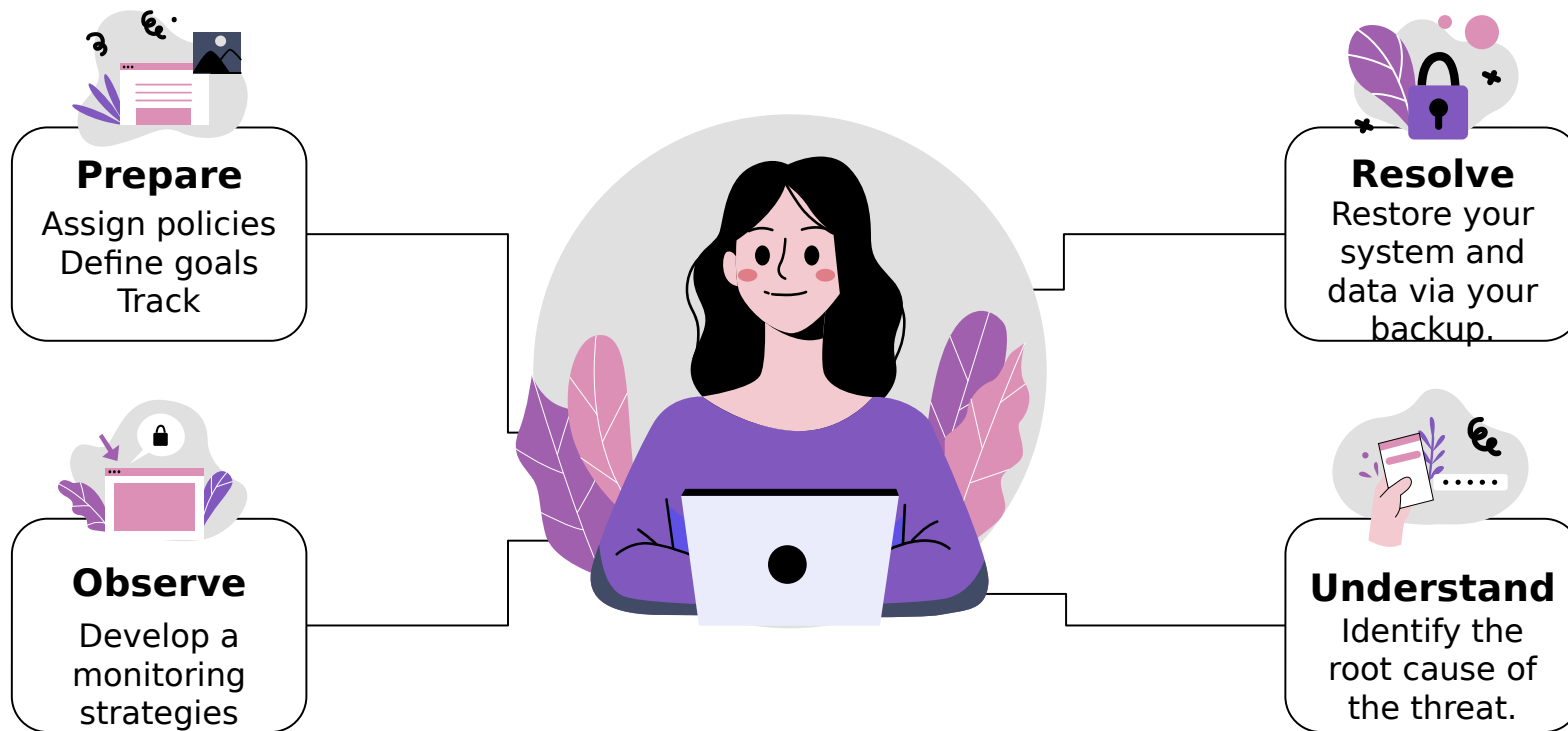


A type of malware i.e., **Ransomware** denies the access attempt by the user to a system until or unless a sum of money is paid. It is a serious cyber threat that is escalating day by day.

# How does it occurs



# Incident Response Plan Phases



# Incident Response Plan Checklist for Ransomware



## **Risk Assessment**

Risk Assessment defines the threats and vulnerabilities.

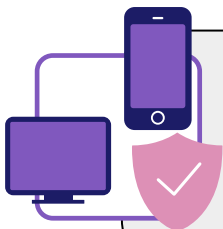


## **Policies and Procedures**

Develop IRP that defines roles and responsibilities.



**CIRT**  
CIRT for specifying and resolving threats



## **Training**

Training programs for the organizations



## **Identify Stakeholders**

Internal and external stakeholders need to be identified.







## **Communications**

Central point to report incidents.

# Preparation for IRP of Ransomware



 <b>Manage users</b>	Manage users and administration accounts for non-administrative functions
 <b>Implementing Logs and alerts</b>	Enabling the monitoring capabilities for networks for organizations.
 <b>Segment your networks</b>	Segmentation assists in isolating the organization's network and routes.
 <b>Establish defense</b>	Usage of Anti-viruses, anti-malware, and a firewall.

# Monitor and inspect



Develop a monitoring strategy (E.g Frequency included network)

1

Monitor your networks and connected devices for threats

2

Generate event and incident reports regularly.

3

Analyze the data and determine whether you need to activate your response.



# Understanding the IRP for Ransomware

8



## Root cause

Identifying the root cause of the incident

Evaluate your incident response.

## Evaluate



## Improvement

Highlights the areas that require improvements.

Improve the response plan for future initiatives.

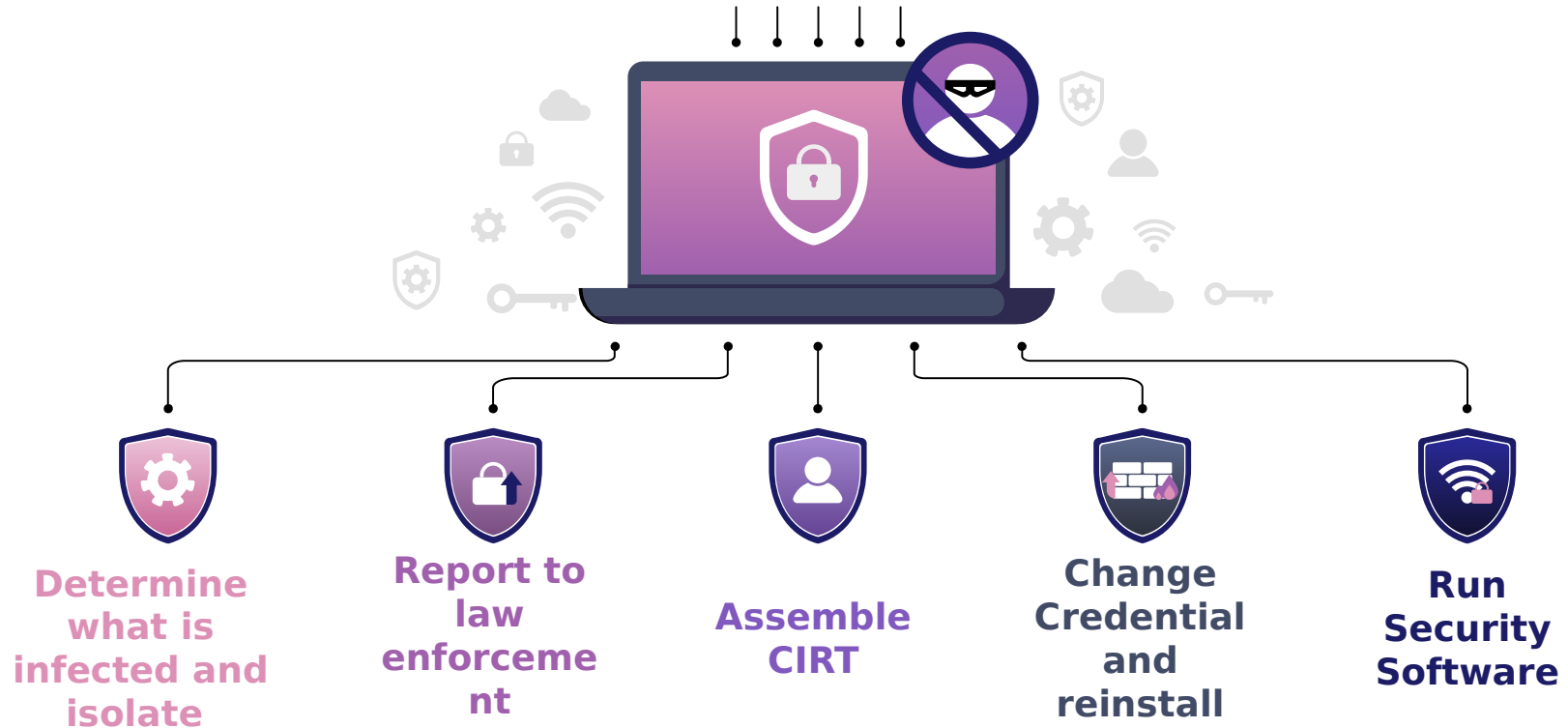
## Lesson Learned



# Detection and Analysis



# Containment and Eradication



# Recovery Plan



**Credential  
Hygiene**



**Principle of  
least privilege**



**Employee  
Training**



**Multifactor  
Authentication**

# References



<https://www.malwarebytes.com/ransomware>  
<https://www.imperva.com/learn/application-security/ransomware/>  
<https://glacistech.com/cybersecurity/incident-response-plan-ransomware-security-breach/#:~:text=An%20Incident%20Response%20Plan%20%28IRP%29%20is%20a%20documented,recovering%20from%20a%20cyber%20incident%20such%20as%20ransomware>



<https://netdiligence.com/blog/2020/06/ransomware-incident-response-plan/>  
<https://www.varonis.com/blog/incident-response-plan>  
<https://www.indeed.com/career-advice/career-development/incident-response-plan>



# Thank you

