Example Co.

Managed Threat Complete – IR Plan & MDR Runbook Workshop

Prepared for:

John Customer

Prepared by:

Jane Consultant

The following document is a demonstration deliverable from Rapid7. This report provides a limited overview of what will be included in a final Rapid7 IR Planning and MDR Runbook Workshop.

Criticality Methodology:

Criticality	Indicators	Scope	Action
1 – Critical	Data breach/loss, Critical Malware, Unauthorized access, Denial of Service, Constituent/PR impact	Widespread and/or with critical servers or data exfiltration	Implement Core IRT, Incident Response Plan, create Security Incident, Organization-wide
Incidents involving the potential breach or exposure of customer or employee data. Incidents classified as Critical command immediate attention and action to perform containment including taking down any potentially compromised systems and affected applications.			
2 – High	Network failure, Loss or device theft, Websites or services compromise	Widespread and/or with critical servers or data exfiltration	Implement Core IRT, Incident Response Plan, create Security Incident, Organization-wide
Serious attempt or actual interruption in availability, or negative impact to confidentiality or integrity (e.g., denial of service attempt, simultaneous malware infections of systems, multi-stage attack, malware infection on a single critical system, successful unauthorized access to systems hosting or transmitting customer or employee data) or a repeated or persistent Medium Incident.			
3 – Medium	Phishing campaigns, malware campaigns, multiple hosts or accounts compromised	>1 impacted host or person	Notify Core IRT, Incident Response Plan, create Security Incident, Organization-wide
A single instance of a clear attempt to gain unauthorized access or information (e.g., attempt to access restricted resources, unauthorized vulnerability scan, single malware infection on a non-critical system, etc.) or repeated or persistent Low Incidents. Incidents classified as Medium may also include the incidental internal exposure of a small number of records of customer or employee data.			
4 - Low	Activated malware or phishing	Individual host or person	create Security Incident
A single instance of potential attacker activity (e.g., malware infections, port scans, unexpected performance spikes, observation of potentially malicious user activity, etc.)			

Table 1: Incident Confidence and Impact

Severity	Level	Description of Impact
S1	**Catastrophic**	Significant impact to business reputation, loss of sensitive customer data, and/or system outage beyond SLA. Damage Estimate: ● Downtime > 24 hours. ● Or financial loss of > $1 Million ● Or grave loss of reputation (e.g. event in the news, customer notification, etc.)
S2	**Critical**	Loss of non-sensitive client data, event exposed to client eroding confidence in [CLIENTNAME] products, and/or temporary disruption of SLA defined services. Damage Estimate: ● Downtime between 12 and 24 hours. ● Or financial loss between $250 thousand and $1 million. ● Or serious loss of reputation (e.g. compromises that should be reported to customers.)
S3	**Major**	Disruption to non-critical services with client exposure and/or degrades customers control of their network. Damage Estimate: ● Downtime between 6 and 12 hours. ● Or financial loss between $100 thousand and $250 thousand. ● Or major loss of reputation (e.g. compromises that should be reported to e-staff and/or compromises that triggers the use of a retainer such as Rapid7)
S4	**Moderate**	Degrades capabilities temporarily. Damage Estimate:

		• Downtime between 1 and 6 hours. • Or Financial loss of between $10 thousand and $100 thousand. • Or potential loss of reputation (e.g. compromises that do not require escalation to management or third-parties)
S5	**Minor**	An event that, if it occurred would cause only a small cost, schedule increase, and/or no observable disruption to services. Damage Estimate: • Downtime between < 1 hour. • Or financial loss of between < $10 Thousand. • Or no loss of reputation.

Critical:

Description	Highest severity level. Impact is extraordinary and potentially catastrophic to the normal operation of business, loss of public trust, and/or impact on employees. Incidents classified as 'Critical' command immediate attention and action to perform containment, including taking down any potentially compromised systems and affected applications.
Indicators	● Threat to life or physical safety of the public, customer, or employees. ● Significant destruction of IT systems/applications ● Significant destruction of corporate capabilities ● Significant disruption of business operations over a sustained period of time ● Massive loss of Personally Identifiable Information (PII), financial, customer, employee, legal, and other confidential information ● Significant loss of public confidence ● Dramatic corporate embarrassment ● Risk of large financial loss
Response Time Goals	● Notify Incident Response Coordinator within 15 minutes ● Identification of impact within 2 hours
Characteristics	● Requires immediate and continual response actions from the core IR team as well as extended resources ● Has the most significant impact on operations and involves an extensive, persistent, and usually very sophisticated attack that is difficult to contain, control, or counteract ● Executive leadership will have an immediate and ongoing interest of the incident, the investigation, and the eventual recovery from the incident ● Major external support from multiple organizations would be engaged ● Would likely involve law enforcement ● Would likely involve multiple levels of regulatory or compliance reporting ● Would likely involve media outlets

High:

Description	Impact is substantial to the proper conduct of business, loss of public trust, and/or impact on operations or employees. This typically involves a serious attempt or actual interruption in availability, or negative impact to confidentiality or integrity (such as, denial of service attempt, malware infections on several simultaneous hosts or on one critical systems, multi-stage attack, successful unauthorized access to systems hosting or transmitting sensitive customer or employee data or a repeated or persistent 'Medium' Incident).
Indicators	● Impactful destruction of some [CLIENTNAME] IT systems/applications ● Impactful destruction of some corporate capabilities ● Substantial disruption of business operations over a sustained period of time ● Substantial loss of PII, financial, customer, employee, legal, and other confidential information ● Substantial loss of public confidence ● Substantial corporate embarrassment ● Risk of financial loss
Response Time Goals	● Notify Incident Response Coordinator within 15 minutes ● Identification of impact within 4 hours
Characteristics	● Requires immediate response from the core IR team ● May involve extended work hours, to include weekends, or could involve 24/7 response activities ● Has real and negative impacts on operations and involves a persistent or sophisticated attack that requires substantial resources to contain, control, or counteract ● Executive leadership will likely have an interest in the outcome of the incident, the investigation, and the eventual recovery from the incident ● External support from multiple organizations will likely be needed to resolve the situation ● Would likely involve law enforcement ● Would likely involve some level of regulatory or compliance reporting ● Would likely involve media outlets

Medium:

Description	Impact is moderate to the proper conduct of business, and/or impact on operations or employees. This typically involves a single instance of a clear attempt to gain unauthorized access or information (e.g., attempt to access restricted resources, unauthorized vulnerability scan, single malware infection on a non-critical system, etc.) or repeated or persistent Low Incidents. Incidents classified as Medium may also include the incidental internal exposure of a small number of sensitive customer or employee data.
Indicators	● Moderate disruption of [CLIENTNAME] business operations over a sustained period of time ● Multiple sites or multiple business units affected by the incident ● Loss of non-PII consumer information ● Limited loss of public confidence ● Limited corporate embarrassment ● Risk of financial loss
Response Time Goals	● Identification of impact within 24 hours
Characteristics	● Requires notification to the core IR team ● Several or most of the core incident response team will be engaged in some aspect of the response effort ● May involve extended work hours initially and will revert to a normal working schedule once initially contained ● Has some impact on operations and involves an attack that requires an organized response to contain, control, or counteract ● External support may be necessary and will be engaged as needed ● May involve law enforcement ● May involve some limited level of regulatory or compliance reporting ● Would likely not involve media outlets

Low:

Description	Impact is greatly limited to the proper conduct of business, and/or impact on operations or employees. This typically involves a single

	instance of potential attacker activity (e.g., malware infections, port scans, unexpected performance spikes, observation of potentially malicious user activity, etc.).
Indicators	● Limited or no disruption of [CLIENTNAME] business operations ● Multiple business units affected by the incident ● No unauthorized access to PII, Protected Health Information (PHI), and/or other confidential information ● No impact to public confidence ● No impact to corporate embarrassment ● Risk of financial loss is minimal
Response Time Goals	● Identification of impact within 48 hours
Characteristics	● This level of severity requires handling by an incident response team member ● This level of response can be conducted during normal working hours ● An incident of this severity has limited or no impact on [CLIENTNAME] operations ● External support is generally not needed ● Law enforcement is generally not engaged ● Regulatory reporting is not warranted ● Would likely not involve media outlets

RACI Diagram

To define the roles and responsibilities associated with the different phases of the process, Rapid7 recommends using the RACI Matrix method, as shown in Table 1 and Table 2:

Responsible (R)	Who is performing, or assigned to work on this phase?
Accountable (A)	Who has the authority to make a decision?
Consulted (C)	Who can provide additional information in this phase?
Informed (I)	Who has to be updated about the progress of this phase?

Table 1: RACI Matrix

Incident Response Initiation

	IR Lead	IR Coordinator	Legal Lead	Public Relations Lead	Internal Communications Lead	Human Resources Lead	IT Security Lead	IT Networking Lead	IT Desktop Lead	Desktop Support	Network	Databases	Server	Applications	Forensic Analyst	Incident Response Consultant
	IR Leadership									**IR Team**					**External**	
Determine Incident Type																
Incident Analysis																
Incident Coordination																
Incident Resolution																
Coordination with Legal Authorities																
Authorization and Execution of Comms with Int. and Ext. Parties																
Retain Outside Counsel																
Retain Public Relations																
Retain Technical Experts																
Remediation and Recovery Planning																
Incident Communications																
Employee Communications																

Incident Response Process

	IR Lead	IR Coordinator	Legal Lead	Public Relations Lead	Internal Communications Lead	Human Resources Lead	IT Security Lead	IT Networking Lead	IT Desktop Lead	Desktop Support	Network	Databases	Server	Applications	Forensic Analyst	Incident Response Consultant
	IR Leadership									**IR Team**					**External**	
Desktop/Laptop Support																
Network Monitoring																
Database Analysis																
Server Analysis																
Application Analysis																
Technical Investigation Support																
Containment																
System Recovery																
Log Review																