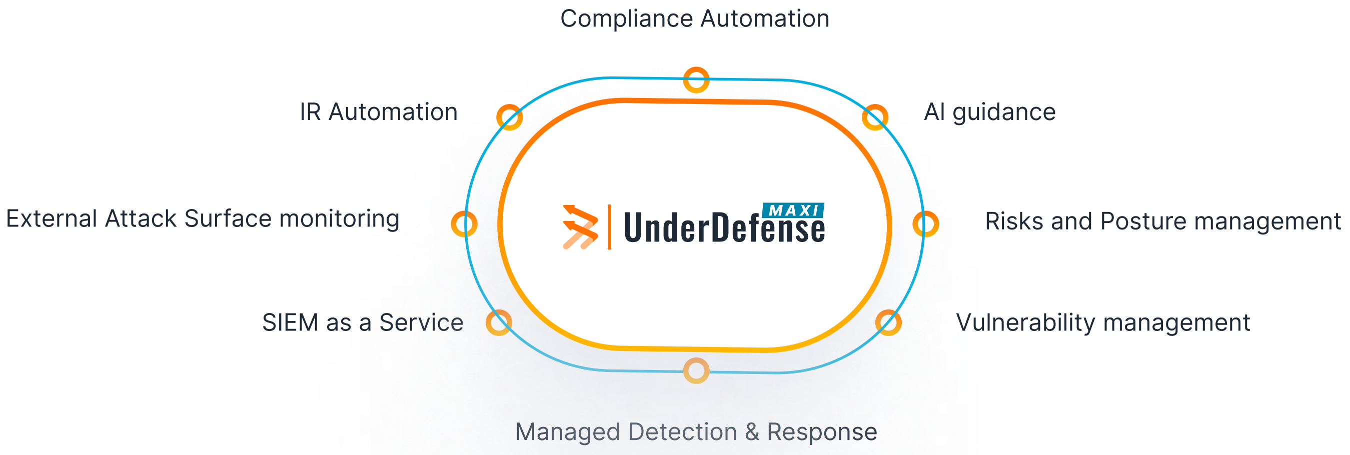
UnderDefense
CYBERSECURITY

Incident Response Plan Template

UnderDefense prevent breaches

On top of the world's most powerful and scalable security products



Compliance Automation

IR Automation

AI guidance

External Attack Surface monitoring

Risks and Posture management

SIEM as a Service

Vulnerability management

Managed Detection & Response

Full-Stack Services | Real-Time | Analytics-Powered | Enterprise-Grade | OpenTelemetry-Native

On-Prem | Hybrid Cloud | Multi-Cloud | Cloud-Native

Starting your compliance journey? UnderDefense policy templates offer comprehensive and compliance-ready documents with placeholders for easy customization with your company-specific details.

Starting your compliance journey? UnderDefense policy templates offer comprehensive and compliance-ready documents with placeholders for easy customization with your company-specific details.

How to Use This Template

This guide outlines the process for adapting these UnderDefense policy templates to align with your organization's specific requirements.

I. Policy Review and Evaluation

- Comprehensive Review: Conduct a thorough examination of each policy document, analyzing each section for its relevance to your organization's operations and risk profile.
- Risk Assessment: Evaluate the applicability of subsequent sections and associated risks to your organization. Remove any sections deemed inapplicable.

II. Policy Customization

- Company-Specific Information Integration: Substitute all highlighted text enclosed in brackets [example] with pertinent information specific to your organization. Utilize the "Find" function to ensure comprehensive replacement of bracketed text.

III. Branding and Formatting

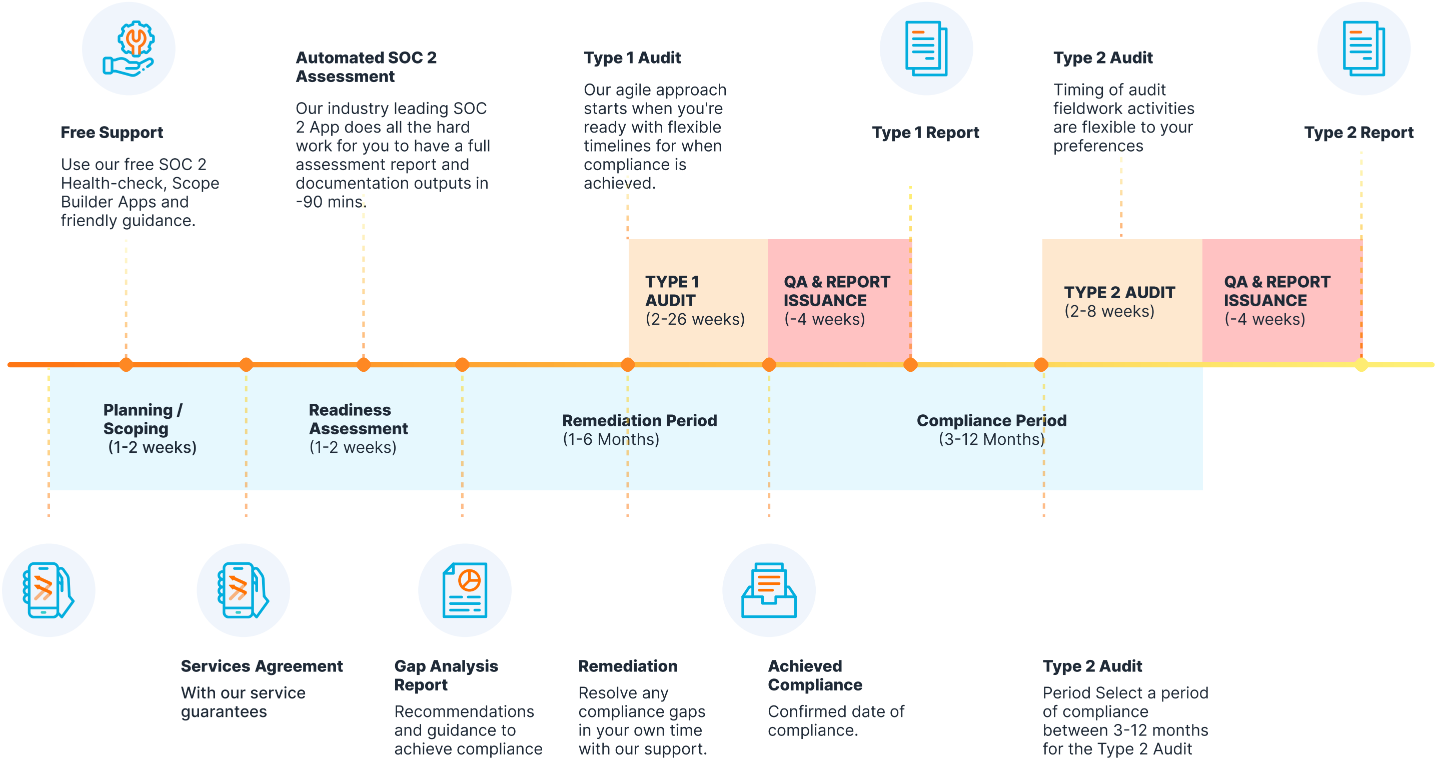
- Incorporation of Corporate Identity: Integrate your organization's letterhead, branding elements, and desired formatting style.

IV. Finalization and Submission

- Document Conversion: After completion, convert the customized document into a PDF file.
- UnderDefenseMAXI Upload: Upload the finalized PDF document to the UnderDefenseMAXI platform https://app.underdefense.com/compliance/ISO27001/approved-policies

The Path to Compliance

We'll guide you through, ensuring a smooth path to compliance:



Free Support
Use our free SOC 2 Health-check, Scope Builder Apps and friendly guidance.

Automated SOC 2 Assessment
Our industry leading SOC 2 App does all the hard work for you to have a full assessment report and documentation outputs in -90 mins.

Type 1 Audit
Our agile approach starts when you're ready with flexible timelines for when compliance is achieved.

Type 1 Report

Type 2 Audit
Timing of audit fieldwork activities are flexible to your preferences

Type 2 Report

TYPE 1 AUDIT (2-26 weeks)

QA & REPORT ISSUANCE (-4 weeks)

TYPE 2 AUDIT (2-8 weeks)

QA & REPORT ISSUANCE (-4 weeks)

Planning / Scoping (1-2 weeks)

Readiness Assessment (1-2 weeks)

Remediation Period (1-6 Months)

Compliance Period (3-12 Months)

Services Agreement
With our service guarantees

Gap Analysis Report
Recommendations and guidance to achieve compliance

Remediation
Resolve any compliance gaps in your own time with our support.

Achieved Compliance
Confirmed date of compliance.

Type 2 Audit
Period Select a period of compliance between 3-12 months for the Type 2 Audit

Need Expert Assistance?

Limited internal resources shouldn't impede your organization's ability to achieve compliance. Our experienced team offers a comprehensive solution:

☑ We navigate the complexities of regulatory requirements, streamlining the process for your team.

☑ Ensure confidence in your compliance posture with all necessary documents meticulously prepared.

☑ Our team offers specialized guidance to address any technology-related challenges you may encounter while achieving compliance.

Book a call with our expert

[Your Company Logo]

Incident Response Plan [#version]

Approved by [who and when]

This document and the information contained herein are the property of [name of your company] and are intended for internal use only by [name of your company] and its personnel. This document and any part of its contents may not be discussed, distributed, lent, disseminated, modified, or copied (in part or whole) without the written permission of [name of your company].

DOCUMENT SPECIFICATION

DOCUMENT TITLE	Incident Response Plan
DOCUMENT STATUS	□ Incident Response Plan ☑ Draft
ABSTRACT	Sets out the formal process to respond to and manage any security incidents
DOCUMENT STATUS	□ Checklist □ Policy ☑ Procedure □ Proposal □ Training (Manual / Guide) □ Report
DOCUMENT CLASSIFICATION	□ Confidential □ Public Domain ☑ Internal Use Only
DOCUMENT OWNER	[NAME] [POSITION / TITLE] [DEPARTMENT] [EMAIL] [DEPARTMENT]
ELECTRONIC COPY LOCATION	
DISTRIBUTION LIST	
NUMBER OF PAGES (INCLUDING COVER)	

VERSION CONTROL

VERSION	AUTHOR	DATE	COMMENT
[1.0]	[Name]	[date]	[Initial Version]
[1.0]	[Name]	[date]	[Review]

Table of contents

1. Purpose 7

7

2. Scope

7

3. Plan Activation

7

4. Incident Response Team 10

10

5. Incident Response Procedure

12

5.1 Preparation

5.2 Identification/Detection 12

5.3 Containment 14

5.4 Eradication 15

5.5 Recovery 16

5.6 Lessons Learning 17

6. Incident Communications 17

6.1 Internal Communication 17

Internal communication between employees and their managers

6.2 External Communication 18

7. Incident-Specific Runbooks 20

8. Annual Review and Approval of this Policy 21

9. Appendices 21

Appendix I - Alert initiation and Incident proceeding with [MDR Vendor] 22

Appendix II - Incident Response Team Contact List 22

Appendix III - Chain of Custody Form 23

Appendix IV - Security Incident Response Report 24

Appendix V - Incident Report Template to [your investors' company] 26

Appendix VI - Incident Report Template to Media & Public Relations for Incident Announcement 27

Appendix VII - Incident Report Template to Media & Public Relations for Post-Incident Report 28

1. Purpose

The purpose of this Incident Response Plan (IRP) is to define the formal process that will be followed by [name of your company] (furthermore, “company”) to respond to and manage any security incidents. This includes the identification, classification, response, and recovery from incidents to minimize impact and support the continuous operation of the organization's critical functions.

2. Scope

This plan applies to all incidents affecting the confidentiality, integrity, or availability of [name of your company] information systems, data, personnel, and other assets. It includes all organizational units, departments, employees, contractors, vendors, and other stakeholders involved in or affected by an incident.

3. Plan Activation

This section outlines the conditions and steps to activate the Incident Response Plan for [name of your company]. The plan's activation is crucial in managing and containing an incident and should be executed promptly and efficiently.

The Incident Response Plan must be activated under the following conditions:

- **Incident Detection Confirmation** of anomalous activity as a security incident by either the Incident Response Team or a third-party SOC/MDR vendor.
- **Employee and Contractor Reporting Incidents** trigger activation by emailing [email address].
- **Phone number:** [Name and Phone Number].
- **Executive Management Directive:** activation upon direct instruction or request from senior or executive leadership within the organization.
- **Compliance Concerns:** activation when an incident might result in non-compliance with applicable legal or regulatory standards and requirements.
- **Impact on Business Operations:** activation in response to an incident that may inflict substantial financial, reputational, or operational harm on [name of your company].

4. Incident Response Team

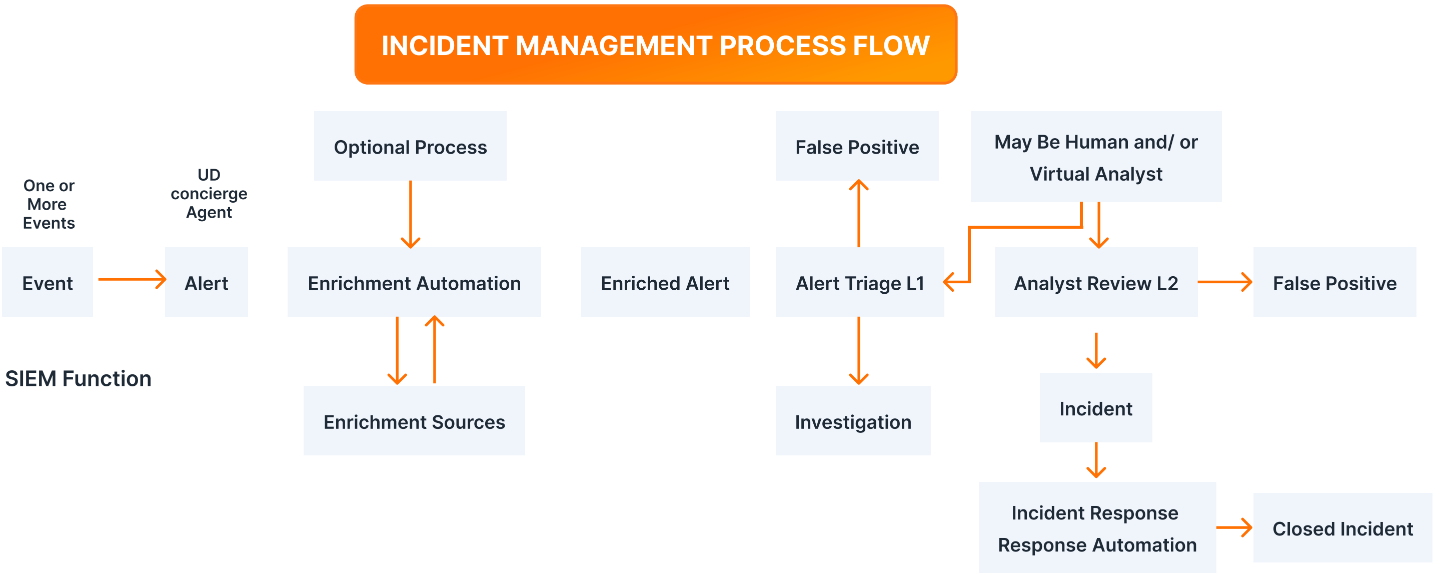
The Incident Response Team (IRT) at [name of your company] is a dedicated group responsible for effectively managing and mitigating security incidents. The team's structure, roles, and responsibilities are outlined below.

Role	Company	Responsibilities
Incident Response Officer	[name of your company]	Incident Response specialist who has ultimate accountability for the actions of the IR Team and IR function. This person should be an executive-level employee. The Incident Response Officer is responsible for: • Reporting to the CEO and is a peer of other C-level executives. • An annual summary of the incidents for the calendar year. • Review any recommendations in the post-incident report and determine additional follow-up actions. • Prevention and resolution of security incidents relating to personal data. • Procedures of storage, processing, and auditing personal data.
Incident Response Lead	[name of your company]	The employee who leads the IR team's efforts and coordinates activities between all its respective groups. This individual reports to the Incident Response Officer. The Incident Response Lead is responsible for: • Process-related training material preparation. • Activating the IR team and managing all parts of the IR process, from discovery, assessment, remediation, and resolution. • Prevention and resolution of security incidents relating to information systems. • Leading investigations into how breaches happen.
IT Operations	[name of your company]	• Restore affected systems to normal functioning. • Implement security patches or updates as required. • Monitor system stability after recovery.
Communications/PR Team	[name of your company]	• Develop and execute communication plans with internal and external stakeholders. • Manage media relations if applicable.
Human Resources	[name of your company]	• Address any personnel matters, including training or disciplinary actions if required.

Role	Company	Responsibilities
MDR Vendor	[your MDR provider]	• 24/7 managed monitoring and alerting to detect potential threats, ensuring continuous protection. • Provides ongoing dark web monitoring for signs of data exposure, including checks for compromised credentials that may affect the organization. • Proactive Threat-hunting sessions to uncover and neutralize potential risks. • Guarantees prioritized and swift response in the event of an incident to contain and mitigate potential damage based on permission access. • Involves in-depth incident investigation, including malware and forensic analysis, to understand the underlying cause. • Aids in liaising with law enforcement agencies when criminal activities are detected. • Delivers comprehensive reports after an incident, detailing findings, lessons learned, and recommendations for future preparedness. • Offers expert advice and support in planning and executing recovery actions and improving security controls. • Assists in navigating the legal and regulatory landscape related to cybersecurity incidents.

5. Incident Response Procedure

Context is critical in Incident Management Process Flow



INCIDENT MANAGEMENT PROCESS FLOW

One or More Events

Event

UD concierge Agent

Alert

SIEM Function

Optional Process

Enrichment Automation

Enrichment Sources

Enriched Alert

False Positive

Alert Triage L1

Investigation

May Be Human and/ or Virtual Analyst

Analyst Review L2

False Positive

Incident

Incident Response Response Automation

Closed Incident

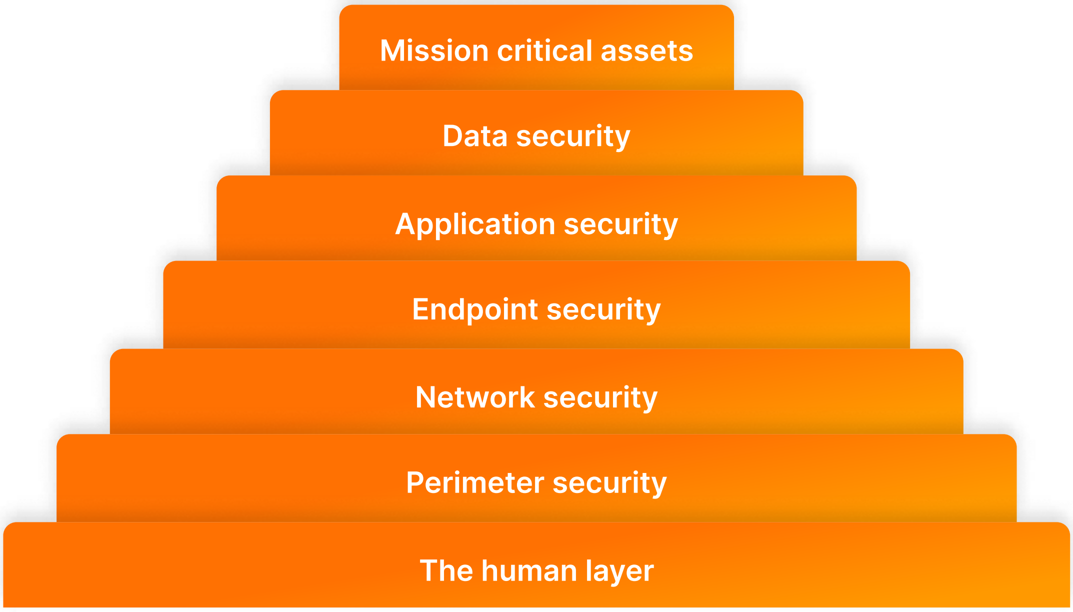
Active Directory Office 365 GSuite Drive okta AWS IAM Jira

GitHub slack CROWDSTRIKE elastic aws Nessus sysdig Amazon CloudTrail AWS Security Hub

5.1 Preparation

Ensure the organization possesses the requisite tools, processes, and personnel to detect, respond to, and recover from security incidents effectively.

7 layers of cybersecurity



Mission critical assets

Data security

Application security

Endpoint security

Network security

Perimeter security

The human layer

1. Establishing the Incident Response Team (Section “4. Incident Response Team”).

2. Tools and Resources.

- Incident Management Platform: Implement a platform or system that can log, track, and manage incidents.
- Forensics Toolkit: Equip the IRT with digital forensic tools for evidence collection, analysis, and preservation.
- Communication Tools: Secure and reliable communication tools, including encrypted messaging applications [Teams, Slack, or another messaging platform] (as a backup communication channel), are essential for safe communication during incidents.

1. [management-only channel dedicated to cyber incidents] for a limited number of members;
2. [channel dedicated to cyber incidents for all personnel] for all company staff;

3. Training and Awareness.

- Training Sessions (tabletop exercises): Organize training sessions for the IRT to keep them abreast of the latest threats, tactics, and response strategies.
- Employee Awareness: Host regular security awareness sessions for all employees, emphasizing the importance of incident reporting and their roles during an incident.

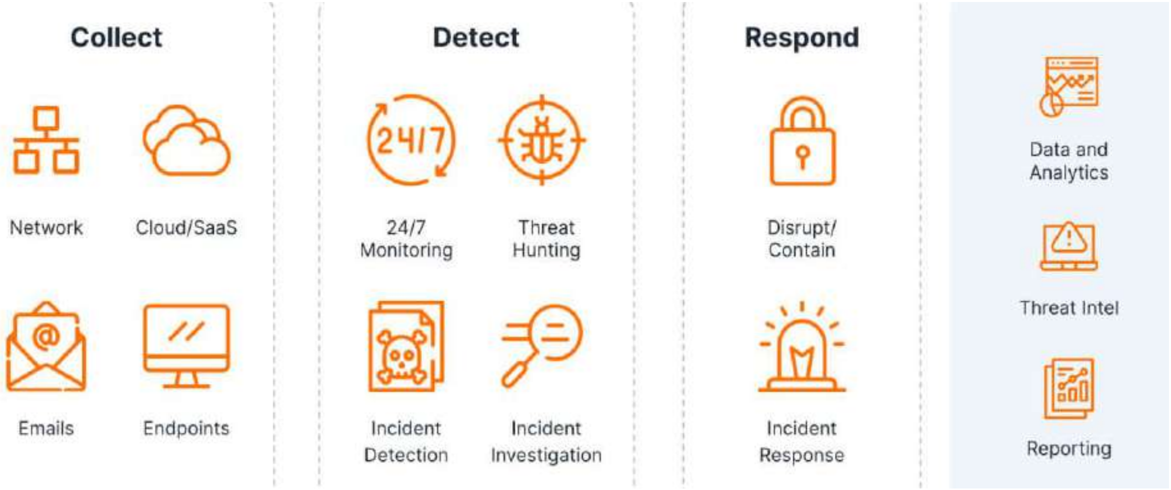
4. Documentation.

- Incident Response Runbooks: Develop detailed runbooks for common incident scenarios [e.g., ransomware, data breach. Please refer to Section “7. Incident-Specific Runbooks”]. These runbooks should offer step-by-step guidelines on how to respond.

5. Collaboration with External Entities.

1. Managed Detection and Response (MDR) Vendor: As detailed in Section **"4. Incident Response Team"**, the MDR vendor plays a critical role in our incident response strategy. Their responsibilities include:
   - **a. Continuous Monitoring and Alerting:** 24/7 managed monitoring and alerting to detect potential cyber threats swiftly.
   - **b. Dark Web Surveillance:** Conducting ongoing dark web scans to identify signs of data exposure, including compromised credentials tied to our organization.
   - **c.** Proactive Threat Hunting: Organizing threat-hunting sessions to uncover and neutralize potential risks proactively.
   - **d. Incident Response:** Ensuring a prioritized and rapid response during incidents, based on their permission access, to contain and minimize damage.
   - **e. In-depth Investigation:** Undertaking comprehensive incident investigations, encompassing malware and forensic analysis, to decipher the root cause.
   - **f. Law Enforcement Liaison:** Coordinate with law enforcement agencies if criminal activities are detected.
   - **g. Post-Incident Reporting:** Providing detailed reports post-incident, outlining findings, lessons captured, and recommendations for bolstering future preparedness.
   - **h. Recovery and Improvement Guidance:** Supplying expert insights and support in planning and implementing recovery strategies and enhancing security protocols.

2. Threat Intelligence Sharing: We collaborate with [name of your MDR vendor] to share Indicators of Compromise (IoC) and other relevant threat intelligence, ensuring that both parties benefit from the combined knowledge and stay ahead of emerging threats.



5.2 Identification/Detection

Monitoring for unusual activities, alerts, or signs of potential incidents using various tools and systems is essential to promptly detect, acknowledge, and initiate the appropriate response to potential security incidents.

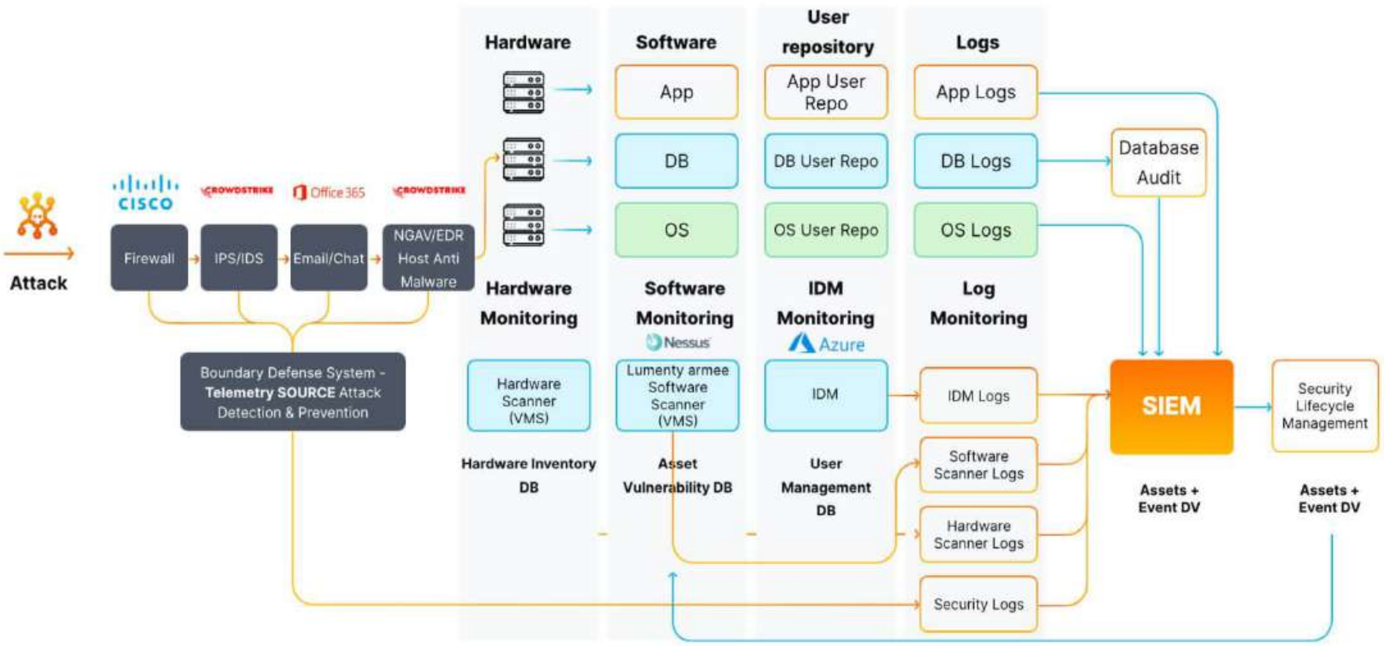
All intelligence gathered, including logs, events, and tool alerts, must be systematically directed to a central Manage Detection and Response (MDR) system.

1. **Monitoring, Collection, and/or MDR Integration.**
   a. **Monitoring Tools:** Deploy various monitoring solutions, including Endpoint Detection and Response (EDR) and [other type of security tools if applicable]. These tools continuously monitor the environment for signs of malicious or anomalous activities.
   b. **Integration with MDR:** All logs, events, and alerts generated by these monitoring tools are aggregated and forwarded to the MDR system.
   c. **MDR Vendor's Role: T**he third-party Managed Security Service Provider (MSSP) is tasked with configuring, managing, and refining the detection scope within the
2. **Indicators of Compromise (IoC) and Tactics, Techniques, and Procedures (TTPs).**
   a. **Definition:**
      i. IoC: Define what constitutes an IoC within the organizational context. IoCs are specific information that indicates a potential security breach, such as known malicious IP addresses, URLs, or malware hashes.
      ii. TTPs: Outline the concept of TTPs as patterns of activities or methods associated with specific threat actors or groups. TTPs provide context, allowing the organization to understand adversaries' intent, capability, and actions.
   b. **Sources:**
      i. Threat Hunting by MDR Vendor: IoCs and insights into current TTPs can emerge from threat-hunting sessions conducted by the MSSP.
      ii. Investors/Partners Input: Investors or partners can provide IoCs and TTP information to enhance detection capabilities.
   c. **Integration by MDR Vendor:** The MDR Vendor incorporates IoCs and TTP-related insights into the

SIEM/EDR system to enhance detection mechanisms and better understand the potential threat landscape.

24/7/365 MDR Data flows & service components

MDR service includes: Cloud deployed & managed SIEM, 24/7 Threat monitoring by Tier 1-3 analysts with 20 min SLO for critical alerts, regular reporting & IR guidance



d. **Importance of TTPs:** TTPs help anticipate threat actor moves, allowing the SOC team to be proactive in defense by understanding the typical behavior of adversaries. Early recognition of a pattern or tactic can lead to quicker incident identification and response.

3. **Detection**
   a. **Role of the SOC Team:** The Security Operations Center (SOC) team (as part of MDR) is primarily responsible for identifying and reporting suspected or known security incidents from MDR.
   b. **Communication Mechanisms:** Incidents are communicated via phone, email, chats, or in-person meetings. This broad notification aims to gather potential evidence or additional information from employees who have observed or encountered aspects of the incident.
   c. **Reporting Criteria (please see section "Appendices" Appendices V-VII"):**
      i. Name of the Reporting Analyst
      ii. Response Time
      iii. Date of Incident
      iv. Host IP (and other criteria based on the specific nature of the incident)
      v. Description
      vi. Impact
4. **Incident Validation and Triage**
   a. **Alert Triage by MDR Vendor:** Performs an initial assessment of alerts generated by the MDR to distinguish between potential security incidents and benign activities. Their role is vital in prioritizing alerts that require immediate attention.
   b. **False Positives Management:** The MDR Vendor filters out false positives to ensure that the organization focuses on genuine threats.
   c. **Confirmation of Incident:** If an alert evolves into a potential security incident, the MDR Vendor conducts a deeper investigation to confirm its nature and implications.

5. **Documentation and Reporting**
   a. **Incident Logging by MDR Vendor:** Records all relevant incident details, including time of detection, systems involved, nature of the incident, and actions taken thus far.
   b. **Reporting Channels:** Established protocols dictate who gets notified upon incident identification, which could encompass the internal Incident Response Team, upper management, legal department, or external entities.
   c. **Preservation of Evidence:** Crucial evidence like logs, system images, or compromised data is preserved appropriately, ensuring it's available for subsequent investigations or legal actions.

5.3 Containment

1. Short-Term Containment/Initial: Implement immediate actions to contain the incident and prevent further damage or propagation.

   a. **System Isolation:** Disconnect the affected systems from the network to prevent further spread of malicious activity. This could involve physically unplugging or logically segmenting the machine from the network.

   b. **User Communication:** Inform relevant users not to access or use the compromised system or application. This helps prevent unintentional interference with the ongoing investigation.

   c. **Data Backup:** Securely backup all data and logs from the affected system for analysis, ensuring evidence remains intact for future investigations.

   d. **Assessment:** Evaluate the initial scope and scale of the incident. This involves understanding how many systems are compromised and estimating the data volume impacted.

2. Long-Term Containment: Apply more permanent solutions to ensure the incident is fully contained, considering future risks and compliance requirements.

   a. **Environment Stabilization:** Ensure that the broader environment is secure and stable. This might involve deploying patches, updating security configurations, or enhancing monitoring mechanisms.

   b. **Controlled Restoration:** Start the process of safely restoring services and data. This might involve cleaning systems, re-installing software, or migrating to clean backups.

   c. **Monitor for Persistence:** Adversaries often deploy multiple methods to maintain access. Monitor systems to ensure that all malicious footholds are identified and removed.

   d. **Coordination with Business Units:** Engage with relevant business units to understand the impact of containment actions on operations and coordinate alternative workflows or solutions as needed.

3. Communication During Containment

   a. **Incident Response Team Updates:** Regularly inform the Incident Response Team about the status and findings during the containment phase.

   b. **Stakeholder Communication:** Ensure stakeholders, such as business unit heads, senior management, and legal teams, are apprised of major containment actions and potential business impacts.

   c. **External Communication Control:** Ensure a coordinated and approved messaging strategy for external communications, avoiding releasing premature or sensitive information.

4. Evidence Preservation and Collection
    a. **Chain of Custody:** Ensure all collected evidence is logged and a proper chain of custody is maintained. This includes noting when evidence was obtained, who handled it, and how it was secured. See the "**Chain of Custody Form**" in the appendices.
    b. **Digital Forensics:** Engage digital forensic experts from IRT to create an image of affected systems. This ensures a comprehensive capture of the state of the system post-incident.
    c. **Log Collection:** Retrieve and secure all relevant logs from the SIEM system, if they exist, Cloud services, network devices, and affected endpoints.

5.4 Eradication

1. **Root Cause Analysis:** Identify the underlying cause of the incident.
    - **Incident Analysis:** Revisit the data and findings from the identification and containment phases. Utilize collected logs, forensic images, and other evidence to trace the origin and evolution of the incident.
    - **Vulnerability Identification:** Identify the vulnerabilities or weaknesses that allowed the incident to occur. This could be software vulnerabilities, misconfigurations, or process weaknesses.
    - **Threat Actor Profiling:** Based on the TTPs observed, attempt to profile the threat actor or group. Understanding their motivations and methods can offer insights into the eradication process.
2. **System Cleanup:** Eliminate the root cause and remove all affected components, ensuring complete threat eradication.
    - **Malware Removal:** Use trusted anti-malware tools to scan and clean infected systems. A full system rebuild may be necessary for particularly aggressive or sophisticated malware.
    - **Configuration Reassessment:** Ensure that configurations across systems align with recommendations from the MDR Vendor to prevent future exploitation of the same vector.
    - **Patching:** Update software, firmware, and operating systems to their latest, secure versions. Ensure all identified vulnerabilities are patched.
    - **System Rebuilds:** In cases where the integrity of systems is deeply compromised, a complete system rebuild from a known good backup might be required.
3. **Validation.**
    - **Environment Scans:** After cleanup actions, scan the environment to ensure no remnants of the malicious activities remain.
    - **Test Restored Systems:** Before fully reintegrating restored systems into the network, test them in isolated environments to ensure they are clean and functional.
    - **Continuous Monitoring:** Increase monitoring sensitivity for a stipulated period post-eradication to catch any signs of recurring malicious activity (it includes communication with the SOC team to ask them to "keep an eye" for the malicious activity).

4. **Updates and Reinforcements.**
    - **Defense Mechanisms:** Strengthen defense mechanisms based on incident insights. This could involve updating firewall rules, enhancing intrusion detection systems, or deploying new security tools.
    - **Security Policies and Protocols:** Revise and update organizational security policies, procedures, and protocols based on lessons learned from the incident.
5. **Documentation.**
    - **Eradication Report:** Document all actions taken during the eradication phase, including time of implemented actions, tools used, systems cleaned or rebuilt, patches applied, and other relevant details

5.5 Recovery

This section focuses on restoring operations, ensuring long-term safety, learning from the incident, and preparing for potential threats. It emphasizes the technical aspects and the organizational and communicative aspects of post-incident recovery.

1. **System Restoration.**
    - **Data Restoration:** Restore lost or corrupted data from the latest secure backups, ensuring the restored data hasn't been tampered with.
    - **Functionality Checks:** Test all systems for functionality. Ensure that all applications, services, and databases run efficiently and without errors.
    - **Integration:** Reintegrate cleaned and recovered systems into the network environment, ensuring they communicate and function as expected within the broader infrastructure.
2. **Monitoring Post-Incident.**
    - **Enhanced Vigilance:** Implement increased monitoring sensitivity to quickly detect anomalies or repeat incidents.
    - **Feedback Loop:** Any new alerts or potential vulnerabilities detected during this enhanced monitoring period should be immediately reported to the Incident Response Team for validation.
3. **Validation.**
    - **System and Network Validation:** Confirm that all systems and networks operate optimally, ensuring no latent malicious activity or undiscovered vulnerabilities.
    - **Business Process Validation:** Check that all business processes, including third-party integrations and customer-facing services, are fully functional.
4. **Communication.**

    Internal Communication: Update company personnel on the recovery status, any ongoing risks, and measures being taken.

    External Communication: Notify customers, partners, and other relevant external entities about the resolution of the incident and any potential impacts

5. **Documentation.**
   - **Recovery Report:** Document all actions taken during the recovery phase, highlighting key decisions, challenges faced, and solutions implemented.
   - **Incident Closure:** Formally close the incident in all tracking systems, ensuring that all details and documentation are archived for future reference.

5.6 Lessons Learning

- **Post-Incident Review:** Conduct a comprehensive review to understand what went right, what went wrong, and why.
- **Report:** Document the review findings, including recommendations for improvements.
- **Implementation:** Apply the lessons learned to enhance existing prevention, detection, and response strategies.

6. Incident Communications

Internal Communication: Regularly communicate with internal stakeholders, providing updates and guidance as required.

External Communication: Notify external entities such as regulators, law enforcement, or affected customers as legal or contractual obligations require.

6.1 Internal Communication

Internal communication between employees and their managers:

1. **Incident Identification:** immediate contact should be established with the employee and their respective manager.

2. **Notification Channels:**

- Email for all employees using [your corporate email address].
- Phone calls directly to the employee that figured in the current incident.
- Messaging application [Teams, Slack, or other messaging platform, if applicable] which has the title “[management] cyber-incidents.”

3. **Notification Content. The notification should:**

- Briefly describe the nature of the incident.
- Explain the potential impact.
- Outline any actions the employee should take.
- Provide contact details for further information or support.

4. **Documentation:** Record all notifications sent, including the date, time, channel used, and recipient details in the **Security Incident Response Report.**

5. **Follow-up:** Depending on the severity of the incident, a follow-up communication may be necessary to update the employee and their manager on resolution efforts or additional precautionary measures.

6.2 External Communication

Affected Customers or Clients:

1. **Incident Identification:** Once an incident is detected and its scope is understood, determine the customers or clients that may be affected WITHIN ONE BUSINESS DAY OF DISCOVERY.
2. **Notification Channels:** Depending on the contact information provided by the customer/client, use the appropriate channel(s) for notification. This could be:
   - Email.
   - Phone call.
   - SMS or other messaging platforms, if applicable.
3. **Notification Content. The notification should:**
   - Briefly describe the nature of the incident.
   - Explain the potential impact on the customer/client.
   - Outline any actions the customer/client should take.
   - Provide contact details for further information or support.
4. **Follow-up:** Depending on the severity of the incident, a follow-up communication may be necessary to update customers or clients on resolution efforts or additional precautionary measures.

Investors

1. [Notifying the head office of any cyber incident that impacts operations, may necessitate regulator notification, or involves the loss of PII or other confidential data must occur WITHIN 24 HOURS OF DISCOVERY if the impact is assessed as High. If the incident's impact is assessed as Medium or Low, the head office will be notified at the discretion of the Incident Response Officer.]
2. The initial notification to the head office should be made via phone, messaging application [Teams, Slack, or other messaging application, if applicable], and email.
3. The initial notification to head office should be sent to [Name of a responsible personn], who will then be responsible for informing other members of the [your company’s] executive team and, if necessary, the Board of Directors. Please see the Contacts in the section “Incident Response Team Contact List” for the role “Investors.”
4. The involvement of regulators or local/state/provincial/federal law enforcement agencies must be disclosed to the head office IMMEDIATELY.

5. The [IRO/IRL/CISO] must provide [Name of a responsible person] with subsequent updates relating to the incident at pre-determined intervals.
6. Any indicators of compromise are to be shared by the entity’s [IRO/IRL/CISO] to the members of the CISO working group either directly or through [Name of responsible person] as soon as they become readily available under the heading of “PRIVILEGED AND CONFIDENTIAL - ATTORNEY-CLIENT WORK PRODUCT SHARED UNDER COMMON INTEREST PRIVILEGE.”

Media and Public Relations:

1. Incident Verification

- Before any communication, verify the incident with the Incident Response Team (IRT) to ensure accurate understanding.
- Coordinate with legal and compliance teams to understand potential regulatory implications.

2. Establish a Communication Team

- Point of Contact (PoC): To avoid mixed messages, designate a single spokesperson, preferably from the Public Relations (PR) or Communications department.
- Support Team: Include representatives from legal, IT, IRT, and senior management to provide timely information and ensure consistent messaging.

3. Draft an Initial Statement

- Briefly describe the nature of the incident without diving into technical jargon.
- Outline what is currently known and actions being taken.
- Share, if known, the potential impact on customers, partners, or the general public.
- Ensure the statement adheres to legal and regulatory guidelines.

4. Determine Communication Channels

- Press Release: The official statement was released to all media outlets.
- Company Website: A dedicated page or banner about the incident status.
- Social Media: Use company profiles to share official statements and direct followers to the company website for detailed information.
- Direct Emails: For affected stakeholders or partners.

4. Determine Communication Channels

- Press Release: The official statement was released to all media outlets.
- Company Website: A dedicated page or banner about the incident status.
- Social Media: Use company profiles to share official statements and direct followers to the company website for detailed information.
- Direct Emails: For affected stakeholders or partners.

5. Address Inquiries

- Direct all media inquiries to the designated PoC. Avoid speculating or providing unverified information.

- Set up a dedicated helpline or email for the public. Ensure that personnel handling queries are adequately briefed.

6. **Update Regularly**

- **Periodic Updates:** Provide updates at regular intervals, even to confirm that the situation is being addressed and that more information will be provided later.
- **Changes in Situation:** Immediately communicate any significant changes or if new information becomes available.

7. **Coordinate with Affected Third Parties**

- Ensure that business partners, vendors, or other third parties that might be affected or questioned are informed and aligned on the messaging.

8. **Post-Incident Communication**

- Once the incident is resolved, release a final statement detailing the resolution, lessons learned, and any forthcoming changes in policy or procedure.
- Engage in Reputation Management: Depending on the severity and publicity of the incident, consider proactive PR campaigns or community engagement to rebuild trust.

9. **Review and Feedback**

- Review the effectiveness of the communication strategy, identify areas of improvement, and adjust the procedure accordingly.

7. Incident-Specific Runbooks

The following runbooks provide detailed procedures for handling specific types of incidents:

- **Ransomware Incidents (encryption of data): [link if available].**
- **Phishing Emails: [link if available].**
- **DRP [link if available].**
- **BCP [link if available].**

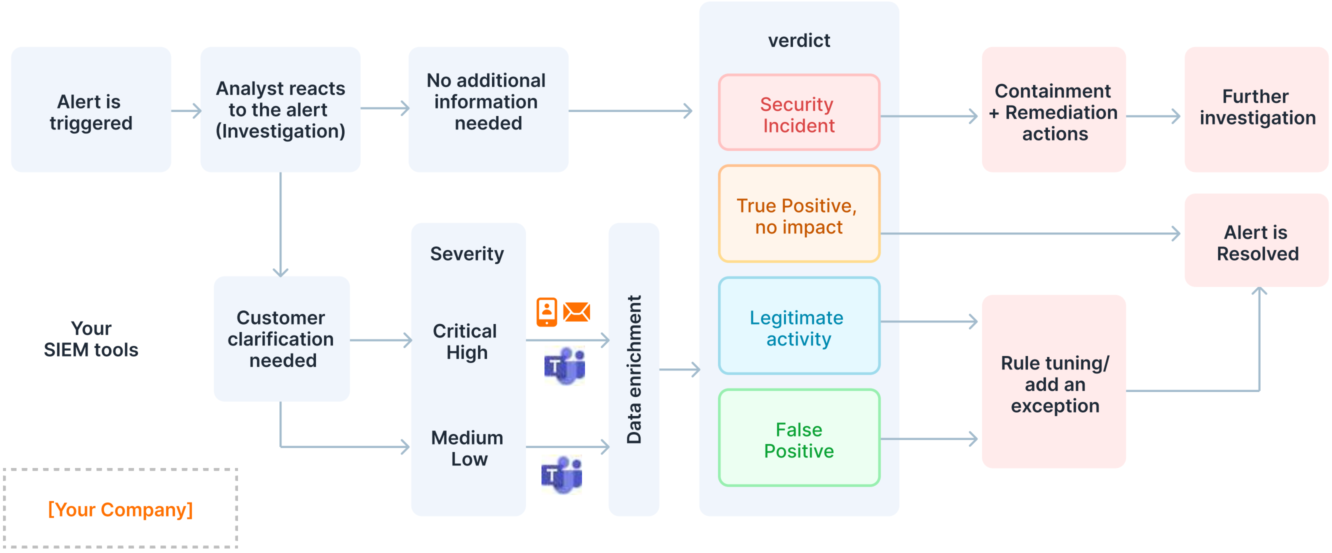
The IRT must follow these runbooks when dealing with the corresponding incidents. Additional runbooks may be developed and added as required.

8. Annual Review and Approval of this Policy

This Plan shall be subject to ongoing review by the Board of Directors. The Document owner is responsible for reviewing and updating this Plan as appropriate and presenting the amended document to the Board of Directors for their approval at least annually.
The Document owner will also be responsible for amending this Plan for any updates or changes in legislation or otherwise which may be required, such changes to be reviewed and ratified by the Board of Directors.

9. Appendices

Appendix I - Alert initiation and Incident proceeding with [MDR Vendor]



Appendix II - Incident Response Team Contact List

Role	Name	Contact
Incident Response Officer	[Name]	Email: [email address] Phone: [phone number]
Incident Response Lead		Email: Phone:
Investors [the name of the entity]		Email: Phone:
		Email: Phone:
		Email: Phone:
IT Operations		Email: Phone:
		Email: Phone:
Communications/ PR Team		Email: Phone:
Human Resources		Email: Phone:
MDR Vendor		Email: Phone:

Appendix III - Chain of Custody Form

Case name/number:

Description of Evidence

Item #	Quantity	Description of item (Type, Model, Serial #, Condition, Marks, other details)

Chain of Custody

Item #	Quantity	Sent from	Sent to	Comments		Locations (Where it is stored)	
				For what reason it was sent?	How was it sent?	Before sent	Before sent

Appendix IV - Security Incident Response Report

Submitter Information	
Date Of Report:	[Insert report creation date]
Submitter Name:	[Insert name]
Title:	[Insert title]
E-mail	[Insert e-mail]
Incident Information	
Notified Individuals:	[Insert notified Individuals' names]
Status:	• Ongoing • Solved • Unknown
Date Of Incident:	[Insert incident date and time]
Type Of Incident:	• Exposure of information • Alteration/destruction of information • Network • Stolen/lost computer equipment • Other, use the field below
	[Insert additional incident type information]
Affected Systems:	[Insert names of systems affected by the incident]
Affected Records:	[Insert names of records affected by the incident]
Incident Description:	[Insert incident description]
Classification of incident:	[Insert Priority Code]

Action Recording

Name and Position:	Action Description:	Data and Time:	Comments:
[Insert name and position of a person who took/ planned the action]	[Insert taken/planned actions with date and time]	[Insert date and time when action was taken/planned]	[Insert any relevant/useful data]

Name and Position:Summary

Resolution:	[Insert resolution/mitigation steps]
Recommendation:	[Insert recommended actions that should be taken to ensure that the same incident does not happen again]

Appendix V - Incident Report Template to [your investors' company]

This section presents a streamlined **email template** for promptly updating investors about incidents.

It prioritizes clear communication and transparency and ensures investors are well-informed about any situation's nature and implications.

To: [IT Working Group / CyberSecurity Subcommittee / General Counsel Working Group]
From: [name of your company]
Date: MM-DD-YYYY
Project Name: [name]

1. What type of compromise/breach did the [name of your company] experience? Can be one or more of the following: Confidentiality loss, Integrity loss, Availability loss)
2. What was the result of the compromise/breach? It can be one or more of the following: denial of Service or Distributed Denial of Service (DoS/DDoS), Business Email Compromise (BEC), data exfiltration, data encryption (ransomware), etc.
3. What was the initial vector (if known) that the attacker used?
4. What tools and methods (if known) were used to exploit the vector and gain a foothold?
5. What tools and methods (if known) were used to move laterally or elevate within the environment?
6. What technical limitations or vulnerabilities were exploited to gain/elevate access? It can be one or more of the following: unpatched/end-of-life systems, misconfigured/lack of hardened systems, lack of a specific security solution in place, false negatives on an existing security tool, etc.
7. What asset(s) were specifically compromised? Please list specific operating systems, applications, cloud-based solutions/resources, network equipment, etc.
8. How was the compromise detected?
9. Is the dwell time of the compromise known? If so, please list it.
10. What Indicators of Compromise (IoCs) are known that would affect other [affiliate companies, projects, etc.]? Please list any and all known IP addresses, URLs, file names, file hash/checksum values, registry values, services, commands, created account names, processes, etc.
11. What steps or remediation methods were effective in containing or stopping the incident?
12. Any other pertinent information that can be passed along to other [affiliate companies, projects, etc.]?

Appendix VI - Incident Report Template to Media & Public Relations for Incident Announcement

[Organization Letterhead/Logo]
Designation: FOR IMMEDIATE RELEASE
Date: MM-DD-YYYY
Type: Incident Announcement – [name of your company]

Intro:
We are writing to inform our valued customers, partners, and the broader community that we recently identified a security incident. We are currently working diligently to address the issue and minimize any potential impact.

Key details to include:

- **Nature of Incident:** [Briefly describe the nature of the incident without technical terms, approaching it in an informal or neutral style to ensure a clear understanding].
- **Current Status:** We identified a recent security incident and promptly activated our Incident Response Team (IRT) to implement the necessary measures. We are collaborating with external cybersecurity specialists to conduct a comprehensive investigation and achieve a swift resolution.
- **Potential Impact:** Our primary focus remains the protection of our user data. We are conducting a comprehensive assessment to determine the potential scope of any data exposure. We will directly notify impacted individuals as necessary.

Expressing Commitment:
We understand this incident may cause concern and sincerely apologize for any inconvenience. The company is committed to resolving this matter with transparency and efficiency. We will review and strengthen our existing protocols to prevent similar incidents as part of our ongoing security posture improvement efforts.
To stay informed, we will provide further updates as more information becomes available. In the meantime, please contact our dedicated response team at [Phone Number] or [Email Address] for inquiries or if you believe you may be impacted.
We appreciate your understanding and patience as we navigate this situation.

[Spokesperson Signature]

Appendix VII - Incident Report Template to Media & Public Relations for Post-Incident Report

[Organization Letterhead/Logo]
Designation: FOR IMMEDIATE RELEASE
Date: MM-DD-YYYY
Type: Post-Incident Report – [name of your company]

Intro:
Following up on our earlier communication regarding the security incident [the date of the initial incident], we are pleased to provide an update on its resolution. This communication also details the lessons learned from this experience and the steps we are taking to improve our security measures and prevent similar incidents in the future.

Incident Recap:

- **Nature of Incident:** [Briefly describe the nature of the incident without technical terms, approaching it in an informal or neutral style to ensure a clear understanding].
- **The business impact:** Following a comprehensive investigation with our cybersecurity experts, we have determined the scope of the incident. We identified that [provide a specific and quantifiable impact, e.g., a limited number of user accounts were compromised]. All impacted individuals have been directly notified and offered the necessary support.

Response Efforts

- **Incident Containment and Resolution:** The Response Team, in collaboration with outside specialists, successfully stopped the incident and fixed the vulnerability, eliminating the risk of unauthorized access.
- **Remediation and Prevention:** We conducted a comprehensive review of our IT configurations and implemented corrective measures to align them with industry best practices. We've also introduced additional monitoring and security checks to prevent similar incidents in the future proactively.
- **User Support:** We understand this incident may have caused some users concern. We proactively contacted potentially impacted users and offered them [specific measures based on the incident type] to assist and support them.

Expressing Commitment:
At our company, we value your trust in us and deeply regret any inconvenience caused by this incident. We are committed to learning from this experience and continuously enhancing our security infrastructure. We will initiate [specific forward-looking measures based on the incident type] to further fortify our systems.
We recognize the importance of your trust and appreciate your understanding and patience. For further inquiries or concerns, please contact our dedicated helpline at [Phone Number] or via email at [Email Address].
[Spokesperson Signature]