Security Incident Response Plan

Contents

Introductions

Objective

The objective of this document is to describe the overall plan for Innovize to prepare and respond to information security incidents. It provides an organizational structure that enables the Incident Response Team (IRT) to evaluate the severity and risk of an incident, respond appropriately to it, inform all relevant parties of the results and related risks, and reduce the likelihood the incident will occur again.

Scope

The scope of this document is the information systems and networks of Innovize and any person or device that gains access to these systems or data.

Definitions

Event

An event is an exception to the normal operation of infrastructure, systems, or services. Not all events become a security incident.

Security Incident

A security incident is an occurrence that breaches Innovize's information security policies and jeopardizes the confidentiality, integrity, or availability of information systems.

Common security incidents can include:

- Malware/viruses
- Ransomware
- Phishing
- Unauthorized electronic access

Incident Response

The incident response will be based off of the Incident Response Life Cycle as defined by the National Institute of Standards and Technology (NIST).

Preparation and Planning

This section of the document will list tools, policies, and procedures used by Innovize to prepare for and prevent a security incident.

Prevention

As listed above under common security incidents, there are common attacks a company can expect to be a target of. There are known preventative methods used to mitigate these possible threats and should be implemented as early as possible. Preventing security incidents is the first line of defense and should be a primary focus during a period of no security incidents.

Preventative tools and procedures include but are not limited to:

- Network security
- Malware/spyware protection
- Risk assessment
- Host security
- Patching systems
- Training

Training and Testing

As policies and procedures are established, the IRT should conduct testing to ensure the validity and accuracy of said documentation. All policies and procedures should be tested based on a schedule defined by Innovize to ensure continuous improvement.

Training can include:

- Simulation drills - A simulated real life scenario that allows the team to practice technical skills and evaluate all tools and software provided.
- Tabletop exercise - A scenario discussion for team members to walk through the incident response plan and identify any gaps in communication.
- Red team / penetration testing - Either the IRT or a third party team will simulate an attack and/or look for vulnerabilities in the organization's network.

Training and testing does not solely focus on the IRT, rather, it should be all encompassing of the personnel within Innovize. As the IRT will need to focus on response and planning, outside personnel should be kept on a training schedule, defined by Innovize, regarding safety procedures and incident response regarding their position.

Training for all personnel can include:

- Cybersecurity training - A course focusing on common cybersecurity threats such as phishing, malware, social engineering, and ransomware. All personnel should have a fundamental understanding of possible threats they face as well as the potential risk and consequences to follow.
- Phishing simulation - A simulated email sent to personnel to test their ability to recognize phishing emails and/or other social engineering tactics. Additional training should be provided to those who do not respond to the simulation in accordance with Innovizes' security policies and procedures.
- Password and device security - A course focusing on strong passwords, using multi-factor authentication, securing all devices (laptops, phones, tablets), installing regular updates, and being cautious of public Wi-Fi networks.
- Incident response training and simulation - A course focusing on reporting any suspicious activities or suspected security incidents. A simulated event should follow the training, giving all personnel practice with identifying suspicious activities and reporting to the IRT.

Current advised methods of mitigations:

- After a certain number of account login attempts lockout the account.
- Prevent login attempts from non-compliant devices or IP address zones.
- Multi-factor authentication.
- Refer to NIST guidelines when creating password policies.
- Proactively reset accounts that are known to be breached.
- Ensure proper file and user permissions are set.
- Have low trust systems that have limited permissions to what only is necessary.
- Remove users from the local administrator group on systems.

Detection and Analysis

This section of the documentation will list methods used by Innovize to detect a security incident and judge the level of severity of said incident.

Detection

A security incident can occur in many ways, as stated in the definition section, meaning the IRT cannot detect all possible scenarios using a single method. This section will focus on common attack vectors and should be updated by the IRT as more specific scenarios arise for Innovize.

Common attack vectors:

- External or removable media - Removable media can have malicious code uploaded, giving an attacker a doorway to execute one or more of the following attacks:
    - Malware distribution
    - Keyloggers
    - Data theft or interception
    - Ransomware
- Attrition - An attacker can try compromising, degrading, or destroying systems or services
- Web - An attacker can exploit vulnerabilities in a website such as the following:
    - Redirecting to another site
    - SQL injections or Cross-Site Scripting (XSS)
    - Cross-Site Request Forgery (CSRF)
    - Distributed Denial of Service (DDoS)
    - Session hijacking
    - DNS spoofing
- Email - An attacker can execute an attack through an email or email attachment, such as the following:
    - Email bombing - Similar to a DoS attack
    - Email spoofing
    - Credential harvesting
    - Phishing
- Impersonation
- Improper usage - An incident where personnel violate acceptable use policies.
- Loss or theft of equipment - Should an attacker gain access to a device, they will gain access to sensitive information stored on the device along with access to the company network.

Current advised methods of detection:

- Monitor for many failed login attempts across users.
- Monitor user access patterns to multiple systems over a relatively short period of time.
- Monitor network activity and traffic for abnormalities.

Analysis

It is important to note many reports of suspicious activity will be false positives. It will be the responsibility of the IRT to investigate and identify the severity, root cause, and impact of any suspected security incidents using tools and methods defined by Innovize.

Incident Reporting

Once a detection of a security incident has been made, the reporting phase should begin. When documenting the security incidents, the IRT should consist of each step taken in response as well as archiving all electronic data related to the incident. Appropriate internal and external parties should be notified of the security incident detection as well as any developments made.

Containment, Eradication, and Recovery

Containment

Containment focuses on stopping the security incident before it can spread and lowering the impact within the network. The primary method to accomplish this step is to isolate affected systems and network segments. In the instance that any critical data is missing or encrypted, legal advisors need to be consulted immediately. There are regulatory steps to take if loss or exfiltration has occurred to sensitive personal or company data.

Eradication

Eradication focuses on identifying and removing the root cause of a security incident. The primary goal is to remove threats, threat actors, and any malicious code within the company network. Examples of eradication include but are not limited to:

- What does the attacker have access to and how did they gain access? If it’s an account, lock down the account immediately.
- Are there malicious scripts running? Stop and remove the scripts immediately.
- Are there anomalous scheduled tasks? Stop these immediately.

Recovery

Recovery focuses on restoring systems and returning systems to their original state in a timely manner. Depending on the security incident, the IRT may focus on updating passwords, replacing files, or restoring the system from backup files. It is important to note there may be third parties who need to be informed (law enforcements, stakeholders, or customers).

Post-Incident Activity

This section of the documentation will focus on reviewing events and identifying areas for improvement. Innovize will need to discuss lessons learned, improve security measures, and prepare for future incidents. After every incident, Innovize should be prepared to schedule meetings to discuss the incident.

- What was learned:
    - What, when, and how?
    - How did the staff perform?
    - Was the transportation and retrieval of information efficient and effective?
    - What else does Innovize need to combat threats effectively?
    - What can Innovize do better next time?
- Security measures:
    - Where did Innovize's security fall short?
    - How can Innovize improve security measures?
    - What mitigations and detection methods can be added?
- Incident response plan:
    - What parts of the incident response plan fell short?
    - How should Innovize update and improve the incident response plan?

Resources:

MITRE n.d. "MITRE ATT&CK" Accessed February 5, 2024. https://attack.mitre.org/

Cybersecurity Incident Response Plans, 12 Oct. 2023, https://www.hhs.gov/sites/default/files/cybersecurity-incident-response-plans.pdf