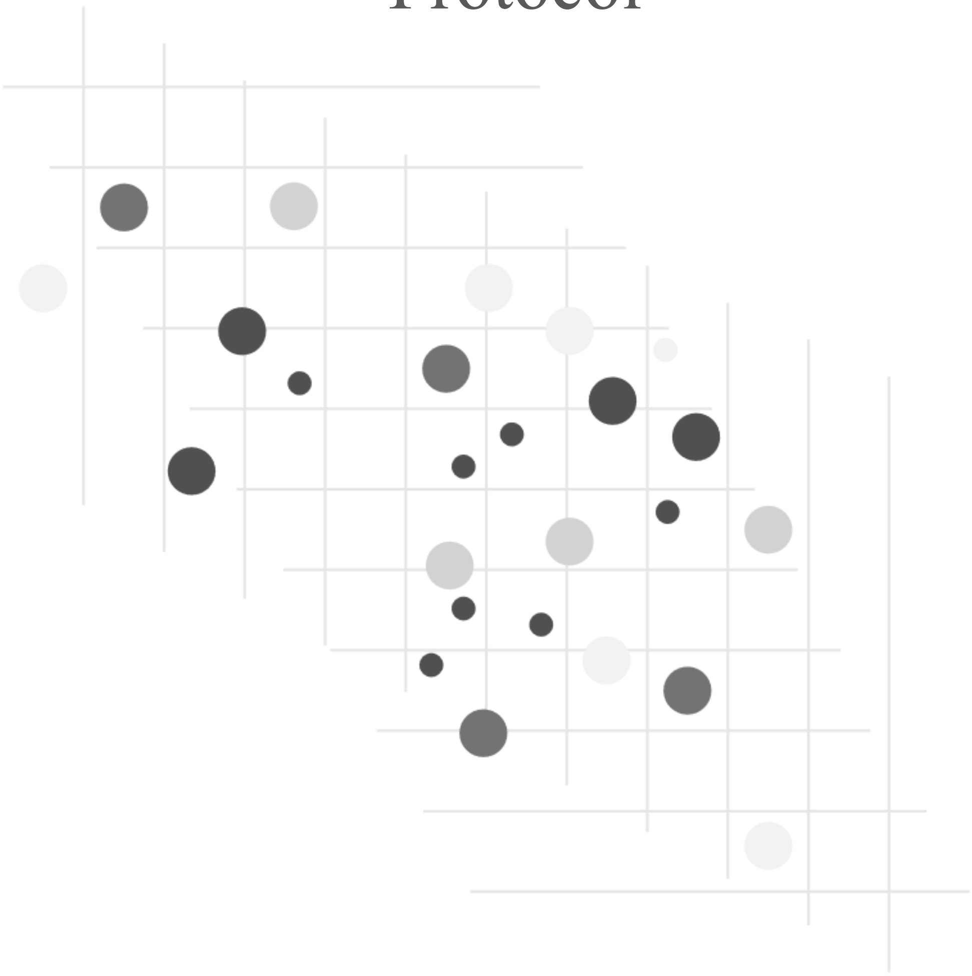
Incident Response Work Protocol



1. General

Correct handling of information security incident can help considerably through information security events such as: malicious codes software, denial of service attacks etc. on the other hand a poor reaction to information security incident may cause even more damage to Adoric than the result of the incident itself due to incorrect assessment and unnecessary speculations and deterioration into an end of which a impropriate actions are taken.

1.1 What Is an Event:

Event is every occurrence in Adoric network, such as: a user uses his given privileges to read a file, a server processes a request that was sent to him, a user receives an E-mail; the firewall blocks an inbound traffic.

1.2 What is an information security incident?

Information security incident is an event that has negative consequences to Adoric network, and which damage the availability, reliability, or the integrity of information. Example of incidents: system crashes, network packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, execution of malicious code that destroys data etc.

*note that some information security incidents are treated automatically by security solutions that are implemented in Adoric _network and without any actions needed to be taken by_ Adoric _personal, an example for that: the implemented Anti-Virus detect a virus and deletes it, but in another case the virus succeed to penetrate to_ Adoric _network, then actions are required to solve the event._

2. Scope

This work protocol includes instructions and actions that need to be taken in case of an information security incident. This work protocol will explain the response actions that must be taken from the identification of an incident through response actions to the closure of the incident.

These work protocols are related to any incident that might occur at Adoric.

3. Responsibilities

Responsibility for reporting on an information security incident that requires a response from the response team and\or suspicion of such an event applies to all employees at Adoric, one must report to his superior and\or to the head of information security or someone on his behalf.

Reporting an Information Security Incident:

It is the response team's responsibility to inform and report to the relevant personnel for decision making and operational functions as well, also the personnel responsible to the affected resources.

4. Incident Response Work Order

4.1 Principals:

This work protocol will define the work order and actions to be taken in an information security event occurring and the responsible personnel.

4.2 Preparation:

To minimize the information security incident that occur on Adoric network, it is important to implement automatic security solutions which monitor and generates alerts to relevant parties in Adoric on new vulnerabilities, new security patches, various event that occur on the network etc. it is important to implement a risk assessment process which rank the level of the vulnerability and according to that the required actions. To avoid information security events Adoric should implement and execute automated system update solution/process, endpoints hardening procedure, correct logical network components management and maintain an awareness program regarding information security for Adoric employees.

4.3 Detection and Identification of Security Information Event:

Information security events can occur through many ways and by a large number of attack vectors, so it is very important to identify the event that we are dealing with no less than to detect that an event is occurring. Event detection can be performed by security solutions which are implemented on Adoric network as well as symptoms that appear and are recognized or felt by Adoric employees. Security solutions might alert on events that happen at the moment happened in the past or might happen in the future. Some examples for symptoms:

- Security solutions alert on an event.
- Unreachable resources (unplanned).
- Drastic slow network connection.
- Multiple failed login attempts.

4.4 Information Security Incident Response:

After an information security incident was detected and identified it is very important to isolate the problem and to prevent its spread to other networks and\or network components (can be done in several ways: turn off the affected machine, disconnect the affected machine from the network, disable or stop certain services). It is very important that before any action taken as in response to the information security incident to perform a thinking session and to bring in consideration all factors that might change the chosen response action:

- What is the damage that might be caused by the incident?
- What is the damage that might be caused due to the action taken?
- What organizational processes may be affected by the incident?

- What organizational processes may be affected due to the action taken?
- How long can the incident and its consequences take?
- How long will it take to react to the incident?

*Actions will be performed only after approval by authorized parties such as: information security manager or someone on his behalf.

4.5 Event Documentation and Response:

An information security incident must be documented from the moment it was identified and until the decision of closing the event. Documentation of an information security event will be done using Form No. 35 – "Documentation of an information security event".

Every decision in the way needs to be documented and list all the decision making personal and time of events. It is very important to document events for two major reasons:

- Update all relevant personnel in the current situation and activities that were taken.
- For learning reasons.
- All evidence (in accordance with the event) will be collected by the CISO, (dates, logs, pictures, testimonies, etc.) in order to preserve all the information of the event. All evidence will be kept for a period of 7 years.

4.6 Lessons Learned:

A lesson learned process is an important process that should be done in case of an information security incident that happened in Adoric network. It may help to get a better understanding of threats to Adoric network and on how to improve security features implemented on Adoric network and procedures. The process should include all Adoric personnel that were involved in the response process to the incident; this should be done as close as possible to the closure of the incident. The lesson learned will be documented using Form 25 - "Corrective Action Form".

5. Events and Response

5.1 Denial Of Service (DOS):

Is an attack that by exhausting resources such as CPU, memory, bandwidth and disk space prevent the use of networks, systems or applications by authorized users.

5.1.1 Symptoms:

- Unusual activity that appears to be preparation for a DOS attack.
- User reports of system unavailability
- Unexplained connection losses
- Network intrusion detection alerts
- Increased network bandwidth utilization
- Large number of connections to a single host
- Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host)
- Firewall and router log entries
- Packets with unusual source addresses

5.1.2 Incident Response:

- An event is being to relevant personal, depends on the affected data, system and\or components
- Reviewing security system logs and alerts
- Considering response actions: changing the affected components address, contacting the ISP for help in filtering the attack
- Findings the vulnerabilities that were exploited
- Mitigate the vulnerabilities found
- Confirming that the affected system function in a normal manner
- Create an event report
- Lesson learned session

5.2 Malicious Code Attack:

A program with the intent to destroy data, run destructive or intrusive programs and to compromise the security or the confidentiality, integrity, and availability of data, applications, or operating system. Malicious code samples: viruses, worms, Trojan horses.

5.2.1 Symptoms:

- Antivirus software alerts of infected files
- Sudden increase in the number of emails being sent and received
- Changes to templates
- for word processing documents, spreadsheets, etc.
- Deleted, corrupted, or inaccessible files
- Unusual items on the screen, such as odd messages and graphics
- Programs start slowly, run slowly, or do not run at all
- System instability and crashes If the malicious program achieves root-level access
- Port scans and failed connection attempts targeted at the vulnerable service
- Unexpected dialog boxes, requesting permission to do something

5.2.2 Incident Response:

- An event is being to relevant personnel, depends on the effected data, system and\or components
- Reviewing security system logs and alerts
- Decision whether a response is necessary (more than 5 malicious code alert in 2 hours need response)
- Finding the effected machines, networks
- Considering response actions: deleting malicious files, turning off effected machines, disconnecting affected machines from the network.
- Findings the vulnerabilities that were exploited
- Mitigate the vulnerabilities found
- Confirming that the effected system function in a normal manner
- Create an event report
- Lesson learned session

5.3 Defacement:

This attack is intended to harm the reputation of the organization by changing the visual appearance of the organization site or webpage.

5.3.1 Symptoms:

- Unauthorized changes made to the organization site or webpage.

5.3.2 Incident Response:

- An event is being to relevant personnel, depends on the effected data, system and\or components
- Reviewing security system logs and alerts
- Considering response actions: redirecting the organization site, uploading "site is down for maintenance" page
- Findings the vulnerabilities that were exploited
- Mitigate the vulnerabilities found
- Confirming that the effected system function in a normal manner
- Create an event report
- Lesson learned session

5.4 Data Corruption:

This attack is performed in order to damage the availability of organization data, and can be executed in several ways.

5.4.1 Symptoms:

- Data is inaccessible
- Users receiving different error messages
- Operating system suggest to repair files
- Blue screen
- Security solutions alerts on unauthorized data modifications

5.4.2 Incident Response:

- An event is being to relevant personnel, depends on the effected data, system and\or components
- Reviewing security system logs and alerts
- Finding the effected tables, instances
- Considering response actions: deny all access to the database
- Findings the vulnerabilities that were exploited
- Mitigate the vulnerabilities found
- Confirming that the effected system function in a normal manner
- Restore data from back up if needed
- Create an event report
- Lesson learned session

5.5 Data leakage:

In this case organization data ``leaks" out to unauthorized personnel, that has stronger privileges then he was given or then he actually needs.

5.5.1 Symptoms:

- Administrator notice that a user has access to data that he does not need to be exposed to.
- Security solutions alert on data leak

5.5.2 Incident Response:

- An event is being to relevant personnel, depends on the effected data, system and\or components
- Reviewing security system logs and alerts
- Finding the misused privileges and account that uses them
- Considering response actions: disabling the account, edit the account privileges, identify exposed data
- Findings the vulnerabilities that were exploited or how wrong privileges were given
- Mitigate the vulnerabilities found, correction to the process that exploited
- Confirming that the effected system function in a normal manner
- Create an event report

6. Document Owner and Approval

The CISO is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff on the corporate intranet.

This procedure was approved by the Chief Information Security Officer (CISO) on 20/04/2021 and is issued on a version-controlled basis under his signature.

Signature: Barak Ben Ami Date: 20/04/2021

History Record:

Action	Date	Edited By	Approved By	Version	Change
Created	20/04/2021	Shimrit Klein	Barak Ben Ami	1	Created
