ActZero

Incident Response Guide

This guide provides a list of basic detection and response actions that IT teams can follow as they respond to and remediate incidents.

Incident Response Guide

How to Use This Guide

The aftermath of a breach or other incident can be chaotic, and the last thing you want is to be making up an incident response plan on the fly. This guide provides a list of basic detection and response actions that IT teams can follow as they respond to and remediate incidents.

You will find basic response actions for the following severity incidents:

- Critical: Initiate response immediately
- High: Initiate response within 2 hours
- Medium: Initiate response within 4 hours
- Low: Initiate response within 24 hours

Critical Incidents

Malware

Category	Description	Examples of How to Detect
Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.	File extension changes. File associations with programs changes. Applications not working Ransom note or README present.
Exploit Kit Detection	A tool used for malicious exploitation of systems is installed and running in the environment.	System Performance is occupied by a scripting language such as python. Anti-Malware agents will inform of exploit kit activity.
Command and Control	A command and control server (C&C server) is a computer that issues directives to digital devices that have been infected with rootkits or other types of malware, such as ransomware.	Firewall Logs or Alerts inform of Malicious IP Connectivity. IPS logs or alerts show command and control signatures.

Response and Remediation

1. Assess the scope of the incident begin documenting on a separate workstation
   a. The time of detection
   b. A brief description of the detection
   c. Usernames of affected accounts (if any)
   d. Host Names of the systems
   e. Local IP Address of the systems
   f. File extension names including full file paths
2. Investigate alerts from active security tools and acknowledge any new detections.
3. Isolate affected endpoint(s) from the network to prevent malware from moving laterally throughout the environment.
4. Escalate to ActZero and provide information from Step 1.
   a. Additional Actions:
      i. Kill running process(es) associated with malware.
      ii. Delete malicious binaries.
      iii. Block command and control IP addresses at network perimeter.
      iv. Ban malicious MD5 or SHA2 hashes with whitelisting tools or other relevant products.
      v. Remove persistence mechanisms (Scheduled Tasks, Autorun Keys, etc.).
      vi. Minimize risk of a future attack by assessing administrative controls. Review account usage and reset passwords, limit administrative access where possible, and disable unnecessary file sharing access.
      vii. Patch vulnerable systems.
      viii. Determine if sensitive data is present.
         1. If so, fill out breach response form (See Appendix)

Escalation Procedure

1. Contact ActZero by one of the following and provide assessment info above:
    a. Phone Call: +1 855 917 4981 (preferred)
    b. Email: threathunting@actzero.ai
2. Incident response specialists initiate pre-defined response plans specific to the severity and type of the incident.
3. Complete initial scoping assessment to determine systems and data affected by the incident.
4. Notify appropriate personnel if scoping assessment determines that the sensitive data was affected by the incident.
5. Notify relevant stakeholders when the incident has been successfully remediated.
6. Optional debrief meeting to look at improvements to incident response process with VCISO.

Testing Procedure

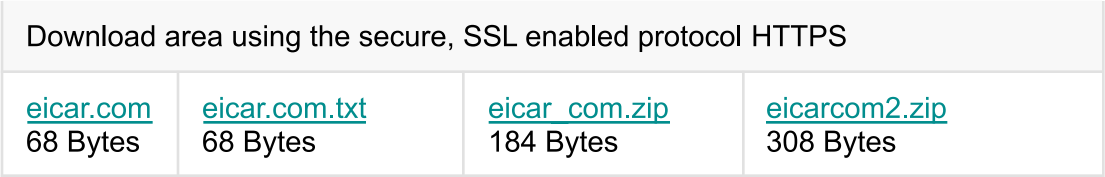
Ransomware:

To test for the procedure use the following test files and procedure on a workstation to evaluate readiness. With a corporate operating system from one of the below, open a browser and download the associated test file.

- Windows — https://wildfire.paloaltonetworks.com/publicapi/test/pe
- MacOSX— https://wildfire.paloaltonetworks.com/publicapi/test/macos
- Android — https://wildfire.paloaltonetworks.com/publicapi/test/apk

Exploit Kit:

To test the exploit kit the anti-virus must inform the user of the kit. Use any of the following links to test these alerts with your anti-malware product by selecting a Windows workstation in the environment and clicking on the links:



Download area using the secure, SSL enabled protocol HTTPS			
eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

High Incidents

Account Compromise

Category	Description	Examples of How to Detect
Cloud Account Takeover	An account which access email or cloud file systems has been used by someone other than the intended user	Security Alert from Providers inform of potential account takeover Dark web monitor informs of breached email addresses

Response and Remediation

1. Assess the scope of the incident begin documenting on a separate workstation
    a. The time of detection
    b. A brief description of the detection
    c. Usernames of affected accounts
    d. Source IP Addresses of Attackers
2. Contact user via phone to inform their account requires a password reset
3. Enable Multi-Factor Authentication if disabled.
4. Investigate email logs to determine any access behavior.
5. Determine if sensitive data present.
    a. If so, fill out breach response form (See Appendix)

Escalation Procedure

1. Contact ActZero and provide assessment info above to close tickets.
    a. Email: threathunting@actzero.ai
2. Optional debrief meeting to look at improvements to incident response process with VCISO.

Testing Procedure

Account Takeover

Send the following email to IT Administration to test procedures:

ActZero detected a suspected O365 Account Takeover (ATO) based on a successful login to an account from a known malicious IP address. We have the following information about the suspected attack:

ACCOUNT: username@domainname.com
TIMESTAMP: 2021-04-01 12:58:49 (UTC)
IP ADDRESS: 196.54.28.56
IP ADDRESS COUNTRY: United States

Microsoft recommends you take following actions:
https://docs.microsoft.com/en-us/archive/blogs/office365security/how-to-fix-a-compromised-hacked-microsoft-office-365-account

You might see the same event as a login failure on your logs if you have any further protection enabled on your portal (such as conditional access rules) that might block the authentication on a later phase. At a minimum, we recommend you reset the user’s credentials because they are known by the attacker.

ActZero Team.

Data Loss

Category	Description	Examples of How to Detect
Asset Loss	A user has lost a device which contains corporate data	A laptop is lost or stolen A smartphone is lost or stolen connected to the enterprise messaging system
Data Loss	A user has lost data either in hardcopy or during an attack with unauthorized access	A USB key containing sensitive data is lost A hard copy of data is lost or stolen.

Response and Remediation

1. Assess the scope of the incident begin documenting on a separate workstation:
    a. The time of detection
    b. A brief description of the detection
    c. Usernames of affected accounts (if any)
    d. Host Names of the systems
    e. Local IP Address of the systems
    f. Data Fields such as usernames, passwords, addresses
2. Fill out breach response form to record incident.
3. Use Appendix to contact required privacy offices.

Escalation Procedure

1. Schedule time with VCISO to discuss exposure and plan for communications.

Testing Procedure

Asset Loss:

Send the following email to IT Administration to test procedures:

I have lost my laptop which contains employment information for staff on the subway.

Data Loss:

Send the following email to IT Administration to test procedures:

A set of printed records from our file cabinet seems to have been lost in an office move.

Medium Incidents

Dark Web Chatter

Category	Description	Examples of How to Detect
Dark Web Chatter	A threat intelligence services has indicated a threat actor is discussion an attack against the organization	Local Law Enforcement contacts you to indicate that there are threat actors targeting members of staff or the network.

Response and Remediation

1. Assess the scope of the chatter record:
   a. Threat Actor Name or Group
   b. Target usernames, IPs or systems in question
   c. Escalate to VCISO

Escalation Procedure

1. Provide information to VCISO.
2. Debrief on Threat Actor and prepare defenses accordingly.

Testing Procedure

Send email to VCISO with the following:

Received a call from the FBI regarding activity of an attack from COZY BEAR.

Low Incidents

Malware

Category	Description
Riskware	Tools that are typically installed intentionally but are designed to circumvent security policy and controls.

Response and Remediation

1. Acknowledge detection(s)
2. Kill running process(es)
3. Contact affected end user
4. Uninstall unwanted programs
5. Mark as remediated

Escalation Procedure

1. Primary responder will remediate detection within 24 hours.
2. Document response actions and notify relevant stakeholders as needed upon remediation.

Testing Procedure

1. On a windows machine within the environment click on any of the following viruses:

Download area using the secure, SSL enabled protocol HTTPS			
eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

2. Send an email to IT Administration with a screenshot of the detection.

Vulnerabilities

Category	**Description**
Bug Bounty	A reward offered to a person who identifies an error or vulnerability in a computer program or system.

Escalation Procedure

1. Provide information to vCISO.
2. Debrief on bug discovered and review to determine if it is a risk.

Responsible Disclosure

You should not engage if the following events occur during a bounty:

- Attempts to modify/destroy/corrupt other users data.
- Attempts to (D)DoS any applications
- Any violations of applicable law.
- Accessing other users' account details or any other user's private information.

Testing Procedure

Send email to VCISO with the following:

Received an email regarding a bug bounty from an anonymous user asking for a reward.

Reply back with the following:

Thank you for contacting [CUSTOMER NAME]. Please note, the [CUSTOMER NAME] does not operate a public bug bounty program and does not offer rewards or compensation in exchange for submitting potential issues. We appreciate the contribution researchers and experts make to our security efforts.

Appendix A: Record Keeping Post-Incident

Use the following form post-incident to record information about the incident where sensitive information was accessed.

DPO/COMPLIANCE OFFICER/INVESTIGATOR DETAILS:			
NAME:		**POSITION:**	
DATE:		**TIME:**	
TEL:		**EMAIL:**	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION & NATURE OF BREACH:			
TYPE OF BREACH:			
CATEGORIES OF DATA SUBJECTS AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO. OF DATA SUBJECTS AFFECTED:		**NO. OF RECORDS INVOLVED:**	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
STAFF INVOLVED IN BREACH:			
PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			
BREACH NOTIFICATIONS:			
WAS THE SUPERVISORY AUTHORITY NOTIFIED?			**YES/NO**
IF YES, WAS THIS WITHIN 72 HOURS?			**YES/NO/NA**
If no to the above, provide reason(s) for delay			

WAS THE BELOW INFORMATION PROVIDED? *(if applicable)*	**YES**	**NO**
A description of the nature of the personal data breach		
The categories and approximate number of data subjects affected		
The categories and approximate number of personal data records concerned		
The name and contact details of the Data Protection Officer and/or any other relevant point of contact (for obtaining further information)		
A description of the likely consequences of the personal data breach		
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)		
WAS NOTIFICATION PROVIDED TO DATA SUBJECT?	**YES/NO**	
INVESTIGATION INFORMATION & OUTCOME ACTIONS:		
DETAILS OF INCIDENT INVESTIGATION:		
PROCEDURE(S) REVISED DUE TO BREACH:		
STAFF TRAINING PROVIDED: *(if applicable)*		
DETAILS OF ACTIONS TAKEN AND INVESTIGATION OUTCOMES:		
HAVE THE MITIGATING ACTIONS PREVENTED THE BREACH FROM OCCURRING AGAIN? *(Describe)*		
WERE APPROPRIATE TECHNICAL MEASURES IN PLACE?	**YES/NO**	
If yes to the above, describe measures		
Investigator Signature: ______________________ Date: ____________________		

Appendix B: Privacy Office Contacts NEA

Country	Province/ State	Name of Legislation or Local Regulation ID	Information URL	Breach Report Form URL
Canada	Federal	PIPEDA | Personal Information Protection and Electronic Documents Act	Click here	Click here
Canada	Alberta	PIPA | Personal Information Protection Act Regulation	Click here	Click here
Canada	British Columbia	PIPA | Personal Information Protection Act Regulation	Click here	Click here
Canada	Manitoba	PIPEDA | Personal Information Protection and Electronic Documents Act	Click here	Click here
Canada	New Brunswick	PIPEDA | Personal Information Protection and Electronic Documents Act	Click here	Click here
Canada	New Foundland	PIPEDA | Personal Information Protection and Electronic Documents Act	Click here	Click here
Canada	Nova Scotia	FOIPOP | Freedom of Information and Protection of Privacy Act PIIDPA | Personal Information Disclusore Protection Act	Click here	Click here
Canada	Ontario	PIPEDA | Personal Information Protection and Electronic Documents Act	Click here	Click here
Canada	PEI	PIPEDA | Personal Information Protection and Electronic Documents Act	Click here	Click here
Canada	Quebec	Bill 62 (PIPEDA until the bill passes)	Click here	Click here
Canada	Sask	PIPEDA | Personal Information Protection and Electronic Documents Act	Click here	n/a
EU	General	GDPR | General Data Protection Regulation	Click here	n/a
EU	Austria	GDPR | General Data Protection Regulation	Click here	Click here
EU	Belgium	GDPR | General Data Protection Regulation	Click here	Click here
EU	Croatia	GDPR | General Data Protection Regulation	Click here	n/a

EU	Cyprus	GDPR | General Data Protection Regulation	Click here	Click here
EU	Czech Republic	GDPR | General Data Protection Regulation	Click here	Click here
EU	Denmark	GDPR | General Data Protection Regulation	Click here	n/a
EU	Estonia	GDPR | General Data Protection Regulation	Click here	n/a
EU	Finland	GDPR | General Data Protection Regulation	Click here	Click here
EU	France	GDPR | General Data Protection Regulation	Click here	n/a
EU	Germany	GDPR | General Data Protection Regulation	Click here	n/a
EU	Greece	GDPR | General Data Protection Regulation	Click here	Click here
EU	Hungary	GDPR | General Data Protection Regulation	Click here	Click here
EU	Ireland	GDPR | General Data Protection Regulation	Click here	Click here
EU	Italy	GDPR | General Data Protection Regulation	Click here	n/a
EU	Latvia	GDPR | General Data Protection Regulation	Click here	Click here
EU	Lithuania	GDPR | General Data Protection Regulation	Click here	Click here
EU	Luxembourg	GDPR | General Data Protection Regulation	Click here	Click here
EU	Malta	GDPR | General Data Protection Regulation	Click here	Click here
EU	Poland	GDPR | General Data Protection Regulation	Click here	Click here
EU	Portugal	GDPR | General Data Protection Regulation	Click here	Click here
EU	Romania	GDPR | General Data Protection Regulation	Click here	Click here
EU	Slovakia	GDPR | General Data Protection Regulation	Click here	n/a
EU	Slovenia	GDPR | General Data Protection Regulation	Click here	n/a
EU	Spain	GDPR | General Data Protection Regulation	Click here	n/a
EU	Sweden	GDPR | General Data Protection Regulation	Click here	Click here
EU	The Netherlands	GDPR | General Data Protection Regulation	Click here	Click here
Germany	Bavaria	GDPR | General Data Protection Regulation	Click here	Click here
Germany	Berlin	GDPR | General Data Protection Regulation	Click here	Click here

Germany	Hamburg	GDPR | General Data Protection Regulation	Click here	n/a
Germany	Lower Saxony	GDPR | General Data Protection Regulation	Click here	n/a
Germany	Mecklenburg-Vorpommern	GDPR | General Data Protection Regulation	Click here	Click here
Germany	Rheinland-Pfalz	GDPR | General Data Protection Regulation	n/a	Click here
Germany	Saarland	GDPR | General Data Protection Regulation	Click here	n/a
Germany	Schleswig-Holstein	GDPR | General Data Protection Regulation	Click here	Click here
Germany	Thuringia	GDPR | General Data Protection Regulation	Click here	n/a
UK	All	GDPR | General Data Protection Regulation	Click here	n/a
USA	Federal	No centralized data protection legislation, see state-specific regulations	n/a	n/a
USA	Alabama	Ala. Code § 8-38-1 et seq.	Click here	n/a
USA	Alaska	Alaska Stat. § 45.48.010 et seq.	Click here	n/a
USA	Arizona	Ariz. Rev. Stat. § 18-551 to -552	Click here Click here	n/a
USA	Arkansas	Ark. Code §§ 4-110-101 et seq.	Click here	Click here
USA	California	Cal. Civ. Code §§ 1798.29, 1798.82	Click here	n/a
USA	Colorado	Colo. Rev. Stat. § 6-1-716	Click here	n/a
USA	Connecticut	Conn. Gen Stat. §§ 36a-701b, 4e-70	Click here	n/a
USA	Delaware	Del. Code tit. 6, § 12B-101 et seq.	Click here	n/a
USA	District of Columbia	D.C. Code §§ 28- 3851 et seq., 2020 B 215	Click here	n/a
USA	Florida	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)	Click here Click here	n/a
USA	Georgia	Ga. Code §§ 10-1-910 to -912; 46-5-214	Click here Click here	n/a
USA	Guam	9 GCA §§ 48-10 et seq.	Click here	n/a
USA	Hawaii	Haw. Rev. Stat. § 487N-1 et seq.	Click here	n/a
USA	Idaho	Idaho Stat. §§ 28-51-104 to -107	Click here	n/a
USA	Illinois	815 ILCS §§ 530/1 to 530/25, 815 ILCS 530/55 (2020 S.B. 1624)	Click here Click here	n/a
USA	Indiana	Ind. Code §§ 4-1-11 et seq., 24-4.9 et seq.	Click here	n/a
USA	Iowa	Iowa Code §§ 715C.1, 715C.2	Click here	n/a

USA	Kansas	Kan. Stat. § 50-7a01 et seq.	Click here	n/a
USA	Kentucky	KRS § 365.732, KRS §§ 61.931 to 61.934	Click here Click here	Click here
USA	Louisiana	La. Rev. Stat. §§ 51:3071 et seq.	Click here	n/a
USA	Maine	Me. Rev. Stat. tit. 10 § 1346 et seq.	Click here	n/a
USA	Maryland	Md. Code Com. Law §§ 14-3501 et seq., Md. State Govt. Code §§ 10-1301 to -1308	Click here Click here	n/a
USA	Massachusetts	Mass. Gen. Laws § 93H-1 et seq.	Click here	n/a
USA	Michigan	Mich. Comp. Laws §§ 445.63, 445.72	Click here Click here	n/a
USA	Minnesota	Minn. Stat. §§ 325E.61, 325E.64	Click here Click here	n/a
USA	Mississippi	Miss. Code § 75-24-29	Click here	n/a
USA	Missouri	Mo. Rev. Stat. § 407.1500	Click here	n/a
USA	Montana	Mont. Code §§ 2-6-1501 to -1503, 30-14-1704, 33-19-321	Click here Click here	Click here
USA	Nebraska	Neb. Rev. Stat. §§ 87-801 et seq.	Click here	n/a
USA	Nevada	Nev. Rev. Stat. §§ 603A.010 et seq., 242.183	Click here Click here	n/a
USA	New Hampshire	N.H. Rev. Stat. §§ 359-C:19, 359-C:20, 359-C:21	Click here Click here	Click here
USA	New Jersey	N.J. Stat. § 56:8-161, 163	Click here	n/a
USA	New Mexico	N.M. Stat. §§ 57-12C-1	Click here	n/a
USA	New York	N.Y. Gen. Bus. Law § 899-AA	Click here	n/a
USA	North Carolina	N.C. Gen. Stat §§ 75-61, 75-65, 14-113.20	Click here Click here	Click here
USA	North Dakota	N.D. Cent. Code §§ 51-30-01 et seq.	Click here	n/a
USA	Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192	Click here Click here	Click here
USA	Oklahoma	Okla. Stat. §§ 74-3113.1, 24-161 to -166	Click here Click here	n/a
USA	Oregon	Oregon Rev. Stat. §§ 646A.600 to .628	Click here	n/a
USA	Pennsylvania	73 Pa. Stat. §§ 2301 et seq.	Click here	Click here
USA	Puerto Rico	10 Laws of Puerto Rico §§ 4051 et seq.	n/a	n/a
USA	Rhode Island	R.I. Gen. Laws §§ 11-49.3-1 et seq.	Click here	n/a

USA	South Carolina	S.C. Code § 39-1-90	Click here	n/a
USA	South Dakota	S.D. Cod. Laws §§ 20-40-19 to -26	Click here Click here	na
USA	Tennessee	Tenn. Code §§ 47-18-2107; 8-4-119	Click here Click here	n/a
USA	Texas	Tex. Bus. & Com. Code §§ 521.002, 521.053	Click here Click here	n/a
USA	Utah	Utah Code §§ 13-44-101 et seq.	Click here	n/a
USA	Vermont	Vt. Stat. tit. 9 §§ 2430, 2435	Click here	n/a
USA	Virgin Islands	V.I. Code tit. 14, §§ 2208, 2209	Click here	n/a
USA	Virginia	Va. Code §§ 18.2-186.6, 32.1-127.1:05	Click here Click here	n/a
USA	Washington	Wash. Rev. Code §§ 19.255.010, 42.56.590	Click here Click here	n/a
USA	West Virginia	W.V. Code §§ 46A-2A-101 et seq.	Click here	n/a
USA	Wisconsin	Wis. Stat. § 134.98	Click here	n/a
USA	Wyoming	Wyo. Stat. § 6-3-901(b), §§ 40-12-501 to -502	Click here	n/a

ActZero

COVER MORE GROUND

Interested in hearing what ActZero's MDR service can do to help your organization defend against cyber threats?

Request A Demo