EVIDEN

Public

RFC 2350

Author(s)	**:**	**Bartosz Misiuro, Magdalena Krajnik Jaworska**
Document Reference	**:**	**B000010**
Version	**:**	**1.0**
Status	**:**	**Final**
Source	**:**	**Eviden**
Document date	**:**	**17 April 2024**
Number of pages	**:**	**18**
Owner	**:**	**Marcin Lipinski**

Signed by /
Podpisano przez:

Marcin Lipiński

Date / Data:
2024-04-24
13:36

Role	Names
Reviewers	Magdalena Krajnik Jaworska
Approvers	Przemyslaw Bukowski
Document Controller	Patrycja Kryske
Document Owner	Marcin Lipinski
Senior Manager	Marcin Lipinski

Contents

List of changes

Version	Date	Description	Author(s)
0.1	11/04/2024	Document Template Creation	Magdalena Krajnik Jaworska
0.2	12/04/2024	First Draft	Bartosz Misiuro
1.0	17/04/2024	Final Version	Bartosz Misiuro

Target readers, communication method

Target group	Distribution/publication method
All Organizations which are interested in the Eviden CERT	*Published in Eviden Public Storage*
All Eviden Group employees	*Published in Eviden Public Storage*

Terms and Abbreviations

Terms/ Abbreviations	Description
BDS	Big Data Security
GDC	Global Delivery Center
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
VMS	Vulnerability Management Service
RES	Remediation Service
CTI	Cyber Threat Intelligence
TTX	Tabletop Exercise
ATH	Advanced Threat Hunting
PSIRT	Product Security Incident Response Team
DFIR	Digital Forensics and Incident Response
SOC	Security Operations Center
CISO	Chief information Security Officer
IoC	Indicator of Compromise
IoT	Internet of Things
SANS	SysAdmin, Audit, Network, and Security
CET	Central Eastern Time
TLP	Traffic Light Protocol
PGP	Pretty Good Privacy
S/MIME	Secure/Multipurpose Internet Mail Extensions

1 Document information

This document describes Eviden BDS GDC PL CERT based on the RFC 2350.

The main golas is to present basic information about Eviden BDS GDC PL CERT, including :

- Contact information
- Channel of communciation
- Mission
- Policies
- Scope of the service/s delivered by CERT
- Roles and responsibilities
- Etc.

1.1 Data of the last update

Please take a look on the chapter “List of changes”.

1.2 Distribution list for notifications

Please take a look on the chapter “Target readers, communication method”.

1.3 Locations where this document may be found

The current version of this document can be found at Eviden Public Storage

1.4 Authenticating this document

This document has been digitally signed by Marcin Lipinski, Head of Big Data & Security Global Delivery Center Poland

2 Contact Information

2.1 Name of the team

Type	Name
Full name	Eviden Computer Emergency Response Team
Short Name	Eviden CERT

2.2 Address

Eviden Poland R&D Sp. z o.o.

Kraszewskiego 1

85-240 Bydgoszcz

2.3 Time zone

CET

2.4 Telephone number

General phone number: +48 22 444 6500

Phone number for Incident support: +48 525 866 415

2.5 Fax number

N/A

2.6 Electronic e-mail address

For incident reporting, contact us at: breachresponse@eviden.com

For notification and support, contact us at: cert@eviden.com

In case of an emergency, please contact us by phone at +48 525 866 415

2.7 Other telecommunication

N/A

2.8 Public keys and encryption information

Type	Name
PGP Key	-----BEGIN PGP PUBLIC KEY BLOCK----- Comment: User-ID: Eviden CERT <cert@eviden.com> Comment: Created: 4/18/2024 10:50 AM Comment: Expires: 1/18/2027 12:00 PM

	Comment: Type: 4,096-bit RSA (secret key available) Comment: Usage: Signing, Encryption, Certifying User-IDs, SSH Authentication Comment: Fingerprint: A16348B23815E3ED8DD90CDC2B6B75A5CB667340 mQINBGYg3usBEACseaPsaLcuGjLEXt/nutOYTPFvbHR843ozzx1kiTIkUlNd/t0l 4z65Pn/rm+5JLihCUwj3abvu7UGMvGdHDCWB2D66jweDyVlllOC3Zl5KYRnbIPQW IN0CQPmoTd5VU94vnze/4tIbdVlwO3SRb+T6MrCnxElMa0+ST4DJn3MlFvVkQf+J EBVyE4UXyIrbShKc1ylc/6XpH81zak9+H2oHKkTwrgGPtR/SVzXwfS/hzbKoQKd0 PefmnTS7vHruldWrX2hiWIDcgGhwlIFbkWmfrzjoIO0uGDavvMl6wAAELhJ3yHGc nEjsitQqrJnutv1ivaSuLikJyQaIJ9wniLZqkQ1tfaM2tQQql+bxLsZLIAbA4Zoi Cr8qSp6hZtMbG1GQjuMNeCvKphA8gY8zXOlIr6JuKNzkhaO0PVbVCfdPdcSxxE5M HOopHH+o9CLAi2It665n4PwX4uyV3W4utFLrWsg/DZ6QzKJcPE3xYWS9uOXyQx0P 7/ocTkJefcE6T+ntLfCKjmjbYDSOyAMnY0pt5grHj3NYAlKEqG2PR2lp6aDtixYx GS/ep9LJIuIZhGxKSN+mjzChh9lE9Tf2sViBqcPIkvwmrswGEy/meM8sSdMBR+fd 1u6/gO8S+alrVf6wK+59JIKZAUYMu98OI64Nv0fOCnIG87ltFUFNXX/P2wARAQAB tB1FdmlkZW4gQ0VSVCA8Y2VydEBldmlkZW4uY29tPokCVwQTAQgAQRYhBKFjSLI4 FePtjdkM3CtrdaXLZnNABQJmIN7rAhsjBQkFLRHFBQsJCAcCAiICBhUKCQgLAgQW AgMBAh4HAheAAAoJECtrdaXLZnNA3/cQAIDnJduIu5Bo78CWywDYgmf0U2ENCIna cGai5aCCWD+M600yNvd9AEfVkoLlmvhAHEFiu/LnfCM/g/LGMMGPAnhxObUKvr7Y X9v/gEv1DLqxiy/pwCs5sW6XRNVOcCw8q7ZhUzACu6uxRh/gH8cpaeySSweEAQso LK3Fm9KXMY4jZXe7usQCCDU7E/nCB+08FwG48Ay9azvkTsGv353tumkcTln4skP4 W0Cu0I8X/+XUs0n9DmqSVuytQbDSQiu1R1oCdRIgw3gYGyYaGur6jPG9zH9JOO1H vhkHgG4uhd+mN3MKuFiK2A80xg9dTkhRQoSl99HhJviGDPpRAjPK31nu3Mj2X0HU oSlebVek7S3GOwlAbIuZ1E5PbOwuJofzMngsSwx0gj7OHJQcBRb6JafGBFLvXyXJ pk10NhWe6UotuM0abWGsgZGIib6EKcoIAQdK51AUHqn2fuAChl12Yc/U/gOmTIxP 3Gf61GPQXUq3iGATmVnCj4blAyC/xkao6byHWNEfkdvjAcUu+3+p1iud44cxtxSD Z07/w19MV1oSXouDDcBzGnwgBNmLSTuummti+Yg4Q146mftFx1BObL5q+F3F6DMs y8fWxzaGD3xdpuAjtvYH29FHI5KT13KwTbbR7XJStLKsoR9owK6rVJ059zCE5Ckx YN3ieH2uJBnuuQGNBGYg3usBDAC9SybMfVRSbvWgi124Dm9oCluTUm0AUbQOKhIi d6REZw0Mje/oO2BMm64cJXXmUUTYIEyQdQkuf0V+0zx9Bl5vHBW99YSX000fhBQi n1aeSgAQG0zSu5NIDhLRB6aFm5SBReL5cxpqCUvrSnlSKzIQjjvCPy+4KsUiiUSl 3lARITA00ij5iTlg0guk7aoYkocdIMdyPzp6IZdAhmDYUaTM6DORDdJkP7FXwQtu ygeAfZpJnBC38oyxSPn+0jYP1DR+5621G5Z8C1QMcceRBLAG7y61kdxCqohe0ae4 6pXMkaXu6djF7Rj/OUnEbbRA6w1/E7iyPwCyhqnEIPtJONduZJrFySGwpNP1JPyW awHpUNCOaE3wyhGI/UFFqTf0mFODVYxogol7ZyTSDJJW3V00g2Uzo5eKF3UutklT bZeCpj0dTvXmwZN6gZMTOJJFSu10qkatJgFEbTpz1OGXPR5GpOnarSf96KlvCdcu fFIeLcNbL4bqpIrMcFewUXyORmEAEQEAAYkCPAQYAQgAJhYhBKFjSLI4FePtjdkM 3CtrdaXLZnNABQJmIN7rAhsMBQkFLRHFAAoJECtrdaXLZnNARlMP/RWHtYeOYVvG w6RV+zZTAenJ7ZaljmsiCr9qMIGG/raxZNOsZ4TQ//hqr3KmvHvYyUruFUHdQRIt 517eUOgf/IFu31UT+tzHO6TNbC+NZob5Wpnbx44fh1GSIpcVCjXxX6XKzv2suBS0 re2bj5gZZNEEqP+LDbrxpYzjvFFpe0qbIM7YgphPCNpe74npQWd9RDqqqKo4FGYy UfvxqTwse8mX88Cfs+yhtvcJYzAQj/a2uSZ0zoLbjpQwvl/FtXWpa7/obzSMjwX+ ubGJCkxq88n91PWPYpJ27thM5vZZRupfgaidwPjSAu+kxLNeDm1ozGKQ029AZCCb

	OSDt5/S/3Lc/Xc9SwsHcJa29dvn+TZ4yZs272F6/8FgBg9hrcskmml0kDRZ3oImZ Fbtvm0zX2uWbJCylJDfzIqyfSnthYzturfy/qJPCTAr49Y+7DXfEVw2M/aGLP8RO OLmp8VuDyyzCSEQK4lvfb7ytd6/vp+kI64F+7JfQ7eHZTJc1yzwZGDBnYdceE4ww ZVxVrNM0Bz42HN4rw/i7cDsOPUALEaF5Q92GB25iCljFEwb2dhbAGj/HEeFDYNUL kFEPFLJZ4VL8opcN4/QpEt0vOQK+iCGUQ2LTuW23WZIYF7wN2aw+7GQtqwMc+BZp +jh5fnggZ0Y5fsVIw8uSmWqEQedXF1/+ =Jtu8 -----END PGP PUBLIC KEY BLOCK-----
Location	Eviden CERT

2.9 Team members

The Team includes 100+ members and consists with the following department:

- Computer Security Incident Response Team (CSIRT)
- Security Processes Management
- Advanced Threat Hunting (ATH)
- Threat Intelligence (TI)
- Product Security Incident Response Team (PSIRT)
- Vulnerability Management Service (VMS)
- Remediation Service (RES)
- Red Team
- Security Dashboard

2.10 Operating hours

8:00 – 18:00 CET for business hours

In case of emergency CERT is available 24/7

2.11 Communciation methods with Customers

Email, phone

2.12 Other Information

N/A

3 Charter

3.1 Mission statement

Eviden CERT has decades of frontline experience working on the most complex breaches worldwide. We are certified, trained, and routinely face and remediate significant breaches.

Our goal is to support organizations via synergy of our Purple Team to:

- fortify cyber defense & resistance
- leverage business services
- strengthen risk management
- uplift security scoring & demonstrate compliance

3.2 Constituency

We help our customers (public, private and governance organizations) and our whole Atos Group Organization via proactive and reactive measures with extensive network of 17 SOCs supports. This includes security researchers who follow emerging threat actors' rapidly changing tools, tactics, and procedures (TTPs), ethical hackers with a deep understanding of vulnerabilities and exploits, threat hunters proficient at looking beyond alerts to identify threats, and other teams that enrich their capabilities.

3.3 Sponsorship and/or affiliation

Eviden CERT is a commercial organization with its own budget developed via revenue.

In term of affiliation, Eviden CERT is the member of:

FIRST.org

ENISA.europa.eu

Trusted-Introducer.org

3.4 Authority

CERT operates on behalf of Eviden as the legal entity, where Eviden is part of Atos Group. It was created under the authority of Atos Group Head of Security. Eviden CERT manages security issues for internal and external organizations.

4 Policies

4.1 Types of incidents and level of support

Eviden CSIRT being part of CERT deals with all confirmed Computer Security Incidents.

Out of scope areas are:

- Security Incidents without involvement of computing resources (i.e. physical security incident like stolen laptop or unauthorized entry to building)
- Incident related to general malfunction of system that is not associated with cyber attack
- Confirmed penetration test \ Red Team assessments

The level of support varies depending on the specific case that is being handled or organization's needs (e.g. Incident Response, Malware analysis, Threat Intelligence support, identification and remediation of vulnerability).

4.2 Co-operation, interaction, and disclosure of information

Speaking about communication when cooperating with involved organizations, Eviden CERT relies on Traffic Light Protocol (TLP) system, with the classification as follow:

- Clear/White - communication are usually distributed via various methods of public communications (among other: summits, conferences, community blogs)
- Green - Eviden CERT relies on unencrypted email as common method of communication
- Amber – communication is made via S/MIME or PGP encrypted email. When partner cannot rely on S/MIME or PGP, information is sent via unencrypted email with attached document encrypted with previously agreed strong password
- Red – information is distributed verbally with encrypted VoIP to a limited audience. Documents related to specific cases are stored in a secured repository with 2FA access.

4.3 Communication and authentication

Eviden CERT communicates in English and Polish.

For secure communication, S/MIME or PGP email is preferred. If it is necessary to authenticate a person before communicating, this can be done through existing networks of trust in the community. X.509 signed e-mail messages will be authenticated but will be responded to with S/MIME or PGP signed email.

5 Services

5.1 Incident Response

In term of Incident Response, Eviden CERT follows SANS methodology. SANS stands for SysAdmin, Audit, Network, and Security. They're a private organization that focus is security, and they've become an industry standard framework for incident response.

5.1.1 Incident Triage

Before CERT starts operational phase of customer support, preparation step must be completed. This is to ensure that a well-prepared team is equipped with appropriate resources, broad knowledge of the specific organization. Moreover, communication and service documentation are prepared so Team is capable of handling security incidents efficiently in day-to-day operations. This step is done during the on-boarding process.

5.1.2 Incident Coordination

Coordination is divided into technical and managerial.

From the technical perspective, Incident is led by CERT Engineer who is also determining containment, eradication, and recovery strategy.

Management coordination is performed by Security Incident Manager. Apart from tracking all Incidents, this role is also responsible for effective communication.

5.1.3 Incident Resolution

According to SANS framework, Incident resolution is managed by the following steps:

- Identification - gathering events, analysing and deciding about declaration if an incident occurs, identifying the scope
- Containment – stopping the damage, making forensics images, gathering evidence and analysing to assess containment options, gathering intelligence and building IoCs
- Eradication - removing the cause of the incident (malicious code, system changes, passwords changes, IP blocking)
- Recovery - restoring systems to normal business, implementing hardening to avoid similar incidents, monitoring for indicators
- Lessons Learned - reporting on actions documented during previous phases, recommending actions to avoid incidents in the future

5.1.4 Proactive Activities

5.1.4.1 Tabletop Exercise

A tabletop exercise (TTX) is a type of simulation or role-playing exercise that helps organizations test their crisis management or incident response plans in a controlled environment. The exercise involves a hypothetical scenario presented to participants, typically senior leaders, or stakeholders in the organization.

During the exercise, participants are asked to discuss and evaluate their response to the scenario, identify gaps in their existing plans, and develop strategies to address those gaps. The scenario may be based on a realistic threat or event, such as a cyber-attack, natural disaster, or physical security breach.

Tabletop exercises are designed to be interactive and collaborative, with participants working together to assess the situation, make decisions, and communicate effectively. The exercise may be facilitated by an external consultant or conducted internally by organization members.

5.1.4.2 Compromise Assessment

A compromise assessment is a type of cybersecurity analysis that is performed to determine whether an organization's systems or networks have been compromised by cyber attackers. The goal of a compromise assessment is to detect and identify any unauthorized access or activity that may have occurred within an organization's environment.

The assessment typically involves a detailed analysis of an organization's IT systems, including servers, endpoints, and network devices, to identify any indicators of compromise (IOCs). IOCs can include suspicious network traffic, unauthorized access attempts, unusual system behaviour, or the presence of malware or other malicious software.

Compromise assessments may be conducted as part of an incident response plan, following a suspected security breach or data leak. They may also be performed regularly as part of a proactive security strategy, to identify potential vulnerabilities and prevent future attacks.

The assessment may be conducted internally by an organization's own security team or by an external security consultant. It may involve both automated tools and manual analysis, and may require access to network logs, system configurations, and other security data.

5.1.4.3 Cyber Threat Intel

Cyber Threat Intelligence (CTI) specifically refers to the collection, analysis, and dissemination of information about cyber threats, such as malware, vulnerabilities, and threat actors. CTI is focused on identifying and responding to cyber threats and is a subset of the broader category of Threat Intelligence (TI).

Cyber threat intelligence has proved beneficial to every level of state, local, tribal, and territorial (SLTT) government entities from senior executives, such as Chief Information Security Officers (CISOs), police chiefs, and policy makers, to those in the field, such as information technology specialists and law enforcement officers. In addition, it provides value for other experts as well, such as security officers, accountants, and terrorism and criminal analysts. Properly applied cyber threat intelligence can provide greater insight into cyber threats, allowing for a faster, more targeted response as well as resource development and allocation.

5.1.4.4 Red Teaming Service

Red teaming is a cybersecurity technique that involves simulating an attack on an organization's systems and networks to identify potential vulnerabilities and improve defensive measures. It is a type of offensive security testing that is designed to simulate the tactics and techniques used by real-world attackers.

Red teaming is typically conducted by a team of cybersecurity experts who are tasked with attempting to breach an organization's defences using a variety of tools and techniques. This can include social engineering tactics, phishing attacks, and other methods commonly used by attackers.

The goal of red teaming is not only to identify potential vulnerabilities and weaknesses, but also to test an organization's response and incident management procedures. This can help organizations to identify areas where their defences may be lacking and to improve their overall cybersecurity posture.

Red teaming is often used in conjunction with other cybersecurity techniques, such as penetration testing and vulnerability scanning, to provide a comprehensive assessment of an organization's security defences. It is an important part of a proactive cybersecurity strategy, as it allows organizations to identify and address potential security risks before they can be exploited by real-world attackers.

6 Incident Reporting Forms

6.1 Cusotmers contracted with Eviden CERT

Eviden CERT has Authorized Callers List for each of the Customer which contains the list of People who can report security incident to be supported by CERT. Security Incident can be reported by Person from the list or email approval from the Authorized Person needs to be provided to SOC together with CERT Intake Form. The list has been prepared during the onboarding of the customer and can be updated by CERT during the operation.

Eviden SOC is the first line for CERT, available 24/7 and all Security Incidents to be supported by CERT should be reported to SOC.

6.2 Cusotmers not contracted with Eviden CERT

Eviden Digital Forensics and Incident Response (DFIR) services help clients investigate, contain and recover business operations from a cyberattack. Our certified experts identify external or internal malicious threat actors across endpoints, networks, applications, cloud, operational technology, and the Internet of Things (IoT).

For round-the-clock cyber breach support, organizations can contact CERT immediately via 24/7 phone:

- +48 525 866 415

or email:

- breachresponse@eviden.com

More details regarding ad-hoc support, can be found within the Official Page.

7 Disclaimer

While all precautions have been taken while preparing this document, information, notifications, alerts, and responses to security incidents, Eviden CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained in our guidance

Appendix A

Use this Appendix only if it adds value to the policy – for example to add here picture of Poster. It is more likely this information should be included in the related Process(es)/Procedure(s) or other documentation.