Public

RFC 2350

Autor(zy)	:	**Bartosz Misiuro, Magdalena Krajnik Jaworska**
Numer Dokumentu	:	**B000011**
Wersja	:	**1.0**
Status	:	**Final**
Źródło	:	**Eviden**
Data Dokumentu	:	**17 Kwiecień 2024**
Ilosc Stron	:	**20**
Właściciel Dokumentu	:	**Marcin Lipinski**

Signed by / Podpisano przez:

Marcin Lipiński

Date / Data: 2024-04-24 13:39

Role	Names
Recenzent	Magdalena Krajnik Jaworska
Zatwierdzający	Przemyslaw Bukowski
Kontroler Dokumentów	Patrycja Kryske
Właściciel Dokumentu	Marcin Lipinski
Senior Manager	Marcin Lipinski

EVIDEN

Contents

Lista zmian

Version	Date	Description	Author(s)
0.1	11/04/2024	Stworzenie szablonu dokumentu	Magdalena Krajnik Jaworska
0.2	12/04/2024	Wersja robocza	Bartosz Misiuro
1.0	17/04/2024	Wersja finalna	Bartosz Misiuro

Docelowi odbiorcy, sposób komunikacji

Target group	Distribution/publication method
Wszystkie Organizacje zainteresowane Eviden CERT	Eviden Public Storage
Wszyscy pracownicy Eviden	Eviden Public Storage

Terminy i skróty

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 Informacje o dokumencie

Ten dokument opisuje Eviden BDS GDC PL CERT na podstawie RFC 2350.

Głównym celem jest przedstawienie podstawowych informacji dotyczących Eviden BDS GDC PL CERT, w tym:

- Informacje kontaktowe
- Kanał komunikacji
- Misja
- Polityki
- Zakres usług świadczonych przez CERT
- Role i odpowiedzialności
- Itd.

1.1 Data ostatniej aktualizacji

Przedstawioan w rozdziale "Lista zmian".

1.2 Rozpowszechnianie powiadomień o zmianach w dokumencie

Przedstawione w rozdziale " Docelowi odbiorcy, sposób komunikacji".

1.3 Miejsce, gdzie można znaleźć dokument

Obecną wersję tego dokumentu można znaleźć w Eviden Public Storage.

1.4 Poświadczenie dokumentu

Ten dokument został podpisany cyfrowo przez Marcina Lipińskiego, Head of Big Data & Security Global Delivery Center Poland.

2 Informacje kontaktowe

2.1 Nazwa zespołu

Type	Name
Nazwa pełna	Eviden Computer Emergency Response Team
Nazwa skrócona	Eviden CERT

2.2 Adres

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

Kraszewskiego 1

85-240 Bydgoszcz

2.3 Strefa czasowa

CET

2.4 Numer telefonu

Główny numer telefonu: +48 22 444 6500

Numer telefonu dla wsparcia incydentów bezpieczeństwa/zgłoszeń: +48 525 866 415

2.5 Numer faksu

Nie dotyczy

2.6 Adres poczty elektronicznej

- W celu zgloszenia incydentu bezpieczeństwa, skontaktuj sie z: breachresponse@eviden.com
- W celu zgłoszenia notyfikacji/informacji bądź potrzeby wsparcia nie związanej bezpośrednio z incydentem bezpieczeństwa skontaktuj sie z : cert@eviden.com
- W przypadku nagłych sytuacji zadzwoń pod +48 525 866 415

2.7 Pozostała telekomunikacja

Nie dotyczy

2.8 Klucze publiczne i inne informacje o szyfrowaniu

Rodzaj	
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 nEjsitQqrJnutv1ivaSuLikJyQaIJ9wniLZqkQ1tfaM2tQQqI+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/gOmTlxP 3Gf61GPQXUq3iGATmVnCj4blAyC/xkao6byHWNEfkdvjAcUu+3+p1iud44cxtxSD Z07/w19MV1oSXouDDcBzGnwgBNmLSTuummti+Yg4Q146mftFx1BObL5q+F3F6DMs y8fWxzaGD3xdpuAjtvYH29FHI5KT13KwTbbR7XJStLKsoR9owK6rVJ059zCE5Ckx YN3ieH2uJBnuuQGNBGYg3usBDAC9SybMfVRSbvWgi124Dm9oCluTUm0AUbQOKhIi d6REZw0Mje/oO2BMm64cJXXmUUTYIEyQdQkuf0V+0zx9Bl5vHBW99YSX000fhBQi n1aeSgAQG0zSu5NIDhLRB6aFm5SBReL5cxpqCUvrSnlSKzIQjjvCPy+4KsUiiUSl 3lARITA00ij5iTlg0guk7aoYkocdIMdyPzp6lZdAhmDYUaTM6DORDdJkP7FXwQtu 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 Członkowie zespołu

Zespół składa się ze 100+ członków podzielonych na następujące zespoły:

- 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 Godziny pracy

8:00 – 18:00 CET godziny biznesowe.

W nagłych wypadkach CERT jest dostępny 24/7.

2.11 Metody komunikacji z klientami

Adres mail, telefon.

2.12 Inne informacje

Nie dotyczy

3 Statut

3.1 Misja

Eviden CERT ma dziesięcioletnie doświadczenia na pierwszej linii frontu w pracy nad najbardziej złożonymi naruszeniami bezpieczeństwa na całym świecie. Jesteśmy certyfikowani, wyedukowani i regularnie stajemy w obliczu znaczących naruszeń, zajmując się ich usuwaniem.

Naszym celem jest wspieranie organizacji poprzez synergiczne działania naszych zespołów w celu:

- wzmacniania obrony i odporności cybernetycznej
- wykorzystania usług biznesowych
- wzmacniania zarządzania ryzykiem
- podnoszenia wyników w zakresie bezpieczeństwa i zapewniania zgodności

3.2 Obszar Działania

Pomagamy naszym klientom (podmioty prywatne, publiczne, rządowe) jak i także naszej całej Orgnizacji Atos Group poprzez działania proaktywne i reaktywne, korzystając z obszernej sieci 17 Centrów Operacyjnych (Security Operations Center – SOC). Obejmuje to osoby zajmujące sie badaniami bezpieczeństwa cyforwego, którzy śledzą szybko zmieniające się narzędzia, taktyki i procedury (Tools, Tactics & Procedures – TTP) pojawiających się aktorów zagrożeń, etycznych hakerów z głębokim zrozumieniem podatności i exploitów, łowców zagrożeń biegłych w wykrywaniu zagrożeń poza alertami, oraz inne zespoły wzbogacające swoje zdolności.

3.3 Sponsorowanie i przynależność

Eviden CERT jest organizacją komercyjną z własnym budżetem rozwijanym poprzez przychody.

Jeśli chodzi o przynależność, Eviden CERT jest członkiem:

FIRST.org

ENISA.europa.eu

Trusted-Introducer.org

3.4 Upełnomocnienie

CERT działa w imieniu Eviden jako podmiotu prawnego, gdzie Eviden jest częścią Grupy Atos. Został utworzony pod kierownictwem Głównego Kierownika

Bezpieczeństwa Grupy Atos (Atos Group Head of Security). Eviden CERT zarządza kwestiami bezpieczeństwa dla organizacji wewnętrznych i zewnętrznych.

4 Polityki

4.1 Typy incydentów i poziom wsparcia

Eviden CSIRT jako część CERT zajmuje się wszystkimi potwierdzonymi incydentami związanymi z bezpieczeństwem komputerowym.

Obszary poza zakresem to:

- Incydenty bezpieczeństwa bez zaangażowania zasobów obliczeniowych (np. incydent związany z bezpieczeństwem fizycznym, jak kradzież laptopa lub nieautoryzowane wejście do budynku)
- Incydenty związane z ogólnym zakłóceniem systemu, które nie są związane z atakiem cybernetycznym
- Potwierdzone testy penetracyjne \ oceny Red Team'u

Poziom wsparcia różni się w zależności od konkretnego przypadku, który jest rozpatrywany, lub potrzeb organizacji (np. reagowanie na incydent, analiza złośliwego oprogramowania, wsparcie dla śledztw zagrożeń, identyfikacja i usuwanie podatności).

4.2 Współpraca, interakcja i ujawnienie informacji

Mówiąc o komunikacji przy współpracy z zaangażowanymi organizacjami, Eviden CERT polega na systemie protokołu Traffic Light Protocol (TLP), z klasyfikacją następującą:

- Clear/White - komunikacja jest zazwyczaj rozprowadzana za pomocą różnych metod publicznych (między innymi: szczyty, konferencje, blogi społecznościowe)
- Green - Eviden CERT polega na niezaszyfrowanej poczcie e-mail jako powszechnym sposobem komunikacji
- Amber – komunikacja odbywa się za pomocą zaszyfrowanej poczty e-mail S/MIME lub PGP. Jeśli partner nie może polegać na S/MIME lub PGP, informacje są wysyłane za pomocą niezaszyfrowanej poczty e-mail z załączonym dokumentem zaszyfrowanym wcześniej ustalonym silnym hasłem.
- Red – informacje są rozprowadzane werbalnie za pomocą zaszyfrowanego VoIP do ograniczonej publiczności. Dokumenty związane z konkretnym przypadkiem przechowywane są w zabezpieczonym repozytorium z dostępem 2FA.

4.3 Komunikacja i uwierzytelnianie

Eviden CERT komunikuje się w języku angielskim oraz polskim.

W przypadku bezpiecznej komunikacji preferowany jest e-mail S/MIME lub PGP. Jeśli konieczne jest uwierzytelnienie osoby przed przystąpieniem do komunikacji, może to być zrealizowane poprzez istniejące sieci zaufania w społeczności. Sygnowane wiadomości e-mail X.509 będą uwierzytelniane, jednak odpowiedzi będą udzielane poprzez e-mail sygnowany S/MIME lub PGP.

5 Usługi

5.1 Reagowanie na incydenty

W zakresie reagowania na incydenty, Eviden CERT stosuje metodologię SANS. SANS oznacza SysAdmin, Audit, Network i Security. Jest to prywatna organizacja, której głównym obszarem działalności jest bezpieczeństwo, a stała się ona standardowym modelem ramowym dla reagowania na incydenty.

5.1.1 Wdrożenie usługi

Przed rozpoczęciem fazy operacyjnej wsparcia klienta przez CERT, należy zakończyć etap przygotowawczy. Ma to zapewnić, że zespół jest odpowiednio przygotowany, wyposażony w odpowiednie zasoby oraz szeroką wiedzę na temat konkretnej organizacji. Ponadto, przygotowana jest dokumentacja komunikacji i usług, aby zespół był w stanie skutecznie zarządzać incydentami bezpieczeństwa w codziennej pracy operacyjnej. Ten etap jest realizowany podczas procesu wdrożenia.

5.1.2 Koordynacja incydentów

Z technicznego punktu widzenia incydent jest prowadzony przez Inżyniera CERT, który jest również odpowiedzialny za określenie strategii ograniczenia, likwidacji i odzyskiwania.

Koordynacja zarządcza jest wykonywana przez Kierownika Incydentu Bezpieczeństwa. Oprócz śledzenia wszystkich incydentów, ta rola jest również odpowiedzialna za skuteczną komunikację.

5.1.3 Rozwiązanie incydentu

Zgodnie z ramowym modelem SANS, rozwiązanie incydentu jest zarządzane za pomocą następujących kroków:

- Identyfikacja - zbieranie zdarzeń, analizowanie i decydowanie o zadeklarowaniu incydentu, identyfikacja zakresu
- Ograniczenie - zatrzymanie szkód, tworzenie obrazów śledczych, zbieranie dowodów i analiza w celu oceny opcji ograniczenia, zbieranie informacji wywiadowczych i tworzenie IoC
- Likwidacja - usunięcie przyczyny incydentu (złośliwy kod, zmiany w systemie, zmiany haseł, blokowanie IP)
- Odzyskiwanie - przywracanie systemów do normalnego funkcjonowania biznesu, wdrażanie zaostrzeń w celu uniknięcia podobnych incydentów, monitorowanie wskaźników

- Wyniki i wnioski - raportowanie działań udokumentowanych podczas poprzednich faz, zalecanie działań zapobiegających incydentom w przyszłości

5.1.4 Działania proaktywne

5.1.4.1 Tabletop Exercise

Tabletop Exercise (TTX) to rodzaj symulacji lub ćwiczeń w formie gry, które pomagają organizacjom przetestować ich zarządzanie kryzysowe lub plany reagowania na incydenty w kontrolowanym środowisku. Ćwiczenie polega na przedstawieniu uczestnikom hipotetycznego scenariusza, zwykle kierownikom wyższego szczebla lub interesariuszom w organizacji.

Podczas ćwiczenia uczestnicy są proszeni o omówienie i ocenę swojej reakcji na scenariusz, zidentyfikowanie luk w ich istniejących planach oraz opracowanie strategii radzenia sobie z tymi lukami. Scenariusz może opierać się na realistycznym zagrożeniu lub zdarzeniu, takim jak cyberatak, klęska żywiołowa lub naruszenie bezpieczeństwa fizycznego.

Ćwiczenia przy stole są zaprojektowane tak, aby były interaktywne i współpracujące, z uczestnikami pracującymi razem, aby ocenić sytuację, podejmować decyzje i efektywnie komunikować się. Ćwiczenie może być prowadzone przez zewnętrznego konsultanta lub przeprowadzane wewnętrznie przez członków organizacji.

5.1.4.2 Ocena kompromitacji (Compromise Assessment)

Ocena kompromitacji to rodzaj analizy z zakresu cyberbezpieczeństwa, która ma na celu ustalenie, czy systemy lub sieci organizacji zostały skompromitowane przez atakujących cybernetycznych. Celem oceny kompromitacji jest wykrycie i zidentyfikowanie nieautoryzowanego dostępu lub działalności, która mogła wystąpić w środowisku organizacji.

Ocena zwykle obejmuje szczegółową analizę systemów informatycznych organizacji, w tym serwerów, punktów końcowych i urządzeń sieciowych, w celu zidentyfikowania wszelkich wskaźników kompromitacji (indicators of compromise – IOCs). IOCs mogą obejmować podejrzany ruch sieciowy, próby nieautoryzowanego dostępu, nietypowe zachowanie systemu lub obecność złośliwego oprogramowania lub innego szkodliwego oprogramowania.

Ocena kompromitacji może być przeprowadzana w ramach planu reagowania na incydenty, po podejrzanym naruszeniu bezpieczeństwa lub wycieku danych. Może także być przeprowadzana regularnie w ramach proaktywnej strategii bezpieczeństwa, w celu zidentyfikowania potencjalnych podatności i zapobiegania przyszłym atakom.

Ocena może być przeprowadzana wewnętrznie przez zespół bezpieczeństwa organizacji lub przez zewnętrznego konsultanta ds. bezpieczeństwa. Może ona obejmować zarówno narzędzia zautomatyzowane, jak i analizę ręczną, a także może wymagać dostępu do logów sieciowych, konfiguracji systemu i innych danych z zakresu bezpieczeństwa.

5.1.4.3 Wywiad z zagrożeń cybernetycznych (Cyber Threat Intel)

Wywiad z zagrożeń cybernetycznych (Cyber Threat Intelligence - CTI) odnosi się do zbierania, analizy i rozpowszechniania informacji dotyczących zagrożeń cybernetycznych, takich jak złośliwe oprogramowanie, podatności i aktorzy zagrożeń. CTI skupia się na identyfikowaniu i reagowaniu na zagrożenia cybernetyczne i jest podzbiorem szerszej kategorii Wywiadu Zagrożeń (TI).

Zosłao udowodnione że wywiad z zagrożeń cybernetycznych przynosi duże korzyści na każdym poziomie jednostek rządowych, stanowych, lokalnych, i terytorialnych (every level of state, local, tribal, and territorial - SLTT) - od wysokich kierowniczych stanowisk, takich jak główni urzędnicy ds. bezpieczeństwa informacji (CISO), szefowie policji i twórcy polityki, po osoby działające operacyjnie, takie jak specjaliści ds. technologii informacyjnych i funkcjonariusze policji. Ponadto dostarcza wartość również innym ekspertom, takim jak oficerowie ds. bezpieczeństwa, księgowi oraz analitycy ds. terroryzmu i przestępczości. Prawidłowo stosowany wywiad z zagrożeń cybernetycznych może dostarczyć większego wglądu w zagrożenia cybernetyczne, umożliwiając szybszą, bardziej ukierunkowaną reakcję, a także rozwój i alokację zasobów.

5.1.4.4 Usługa Red Team

Red Team to technika cyberbezpieczeństwa polegająca na symulowaniu ataku na systemy i sieci organizacji w celu zidentyfikowania potencjalnych podatności i poprawy środków obronnych. Jest to rodzaj testów bezpieczeństwa ofensywnego, który ma na celu symulowanie taktyk i technik stosowanych przez rzeczywistych atakujących.

Red Team jest zwykle prowadzony przez zespół ekspertów ds. cyberbezpieczeństwa, którzy mają za zadanie próbę sforsowania obrony organizacji za pomocą różnorodnych narzędzi i technik. Może to obejmować taktyki inżynierii społecznej, ataki phishingowe i inne metody powszechnie stosowane przez atakujących.

Celem Red Team jest nie tylko zidentyfikowanie potencjalnych podatności i słabych miejsc, ale także testowanie reakcji organizacji i procedur zarządzania incydentami. Może to pomóc organizacjom zidentyfikować obszary, w których ich obrona może być niewystarczająca, oraz poprawić ogólny stan ich cyberbezpieczeństwa.

Red Team jest często stosowany w połączeniu z innymi technikami cyberbezpieczeństwa, takimi jak testy penetracyjne i skanowanie podatności, aby zapewnić wszechstronną ocenę obrony organizacji. Jest to istotna część proaktywnej strategii cyberbezpieczeństwa, ponieważ pozwala organizacjom zidentyfikować i rozwiązać potencjalne ryzyka bezpieczeństwa, zanim mogą zostać wykorzystane przez rzeczywistych atakujących.

.

6 Formularze zgłaszania incydentów

6.1 Klienci korzystający z usług Eviden CERT

Eviden CERT posiada Listę „Autoryzowanych Dzwoniących” dla każdego Klienta, która zawiera listę osób, które mogą zgłaszać incydenty bezpieczeństwa, aby uzyskać wsparcie ze strony CERT. Incydent bezpieczeństwa można zgłosić osobiście z listy lub w przypadku zgłoszenia przez osobę spoza listy, konieczne jest uzyskanie zgody drogą mailową od Osoby Autoryzowanej, która musi zostać przekazana do SOC wraz z Formularzem Przyjęcia CERT. Lista zostaje przygotowana podczas wdrażania klienta i może być aktualizowana przez CERT w trakcie działania.

Eviden SOC jest pierwszą linią dla CERT, dostępną 24/7, i wszystkie Incydenty Bezpieczeństwa, które mają być wspierane przez CERT, powinny być zgłaszane do SOC.

6.2 Klienci niekorzystający z usług Eviden CERT

Usługi Cyfrowego Śledztwa i Reagowania na Incydenty (Digital Forensics and Incident Response – DFIR) Eviden pomagają klientom w dochodzeniu, zabezpieczaniu i przywracaniu działalności biznesowej po ataku cybernetycznym. Nasi certyfikowani eksperci identyfikują zewnętrznych lub wewnętrznych złośliwych aktorów zagrożeń we wszystkich punktach końcowych, sieciach, aplikacjach, chmurze, technologii operacyjnej oraz Internecie Rzeczy (IoT).

Dla całodobowego wsparcia w przypadku naruszenia cybernetycznego, organizacje mogą skontaktować się z CERT natychmiast telefonicznie 24/7 pod numerem:

- +48 525 866 415

Lub mailowo:

- breachresponse@eviden.com

Więcej szczegółów dotyczących wsparcia ad hoc można znaleźć na Official Page.

7 Zastrzeżenia

Mimo podjęcia wszelkich środków ostrożności podczas przygotowywania tego dokumentu, informacje, powiadomienia, alerty i odpowiedzi na incydenty bezpieczeństwa, Eviden CERT nie ponosi odpowiedzialności za błędy lub pominięcia, ani za szkody wynikające z wykorzystania informacji zawartych w w tym dokumencie.