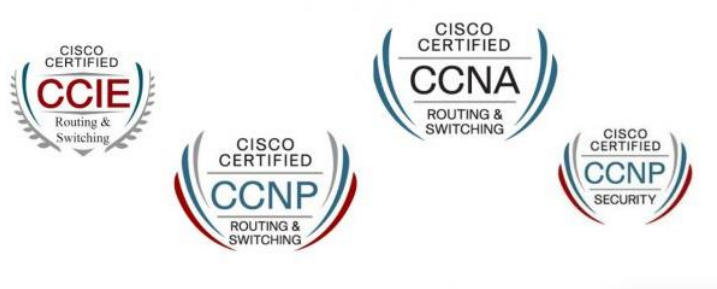
network expert

Security Operations Center

Kwiatek u kożucha czy realna potrzeba?



Nasze specjalizacje

Projektujemy, budujemy i utrzymujemy wszystkie rozwiązania sieciowe.
Nasze działania skupiają się na profesjonalnych sieciach Wifi, wideokonferencjach, switchingu oraz sieciach operatorskich.

Zajmujemy się cyberbezpieczeństwem – projektujemy i wdrażamy kompleksowe usługi bezpieczeństwa dla firm i instytucji.
Nasze usługi obejmują szeroki zakres działań mających na celu zapewnienie kompleksowej ochrony firmy w internecie – od audytów bezpieczeństwa po zapewnienie naszym klientom Security Operations Center.

Oferujemy szeroki wachlarz rozwiązań wideokonferencyjnych.
W naszej ofercie znajduje się zarówno sprzedaż rozwiązań ,jak również ich montaż oraz projektowanie indywidualnych rozwiązań wideokonferencyjnych dla firm w oparciu o sprawdzone i nowoczesne rozwiązania.

Ustawa o KSC – analiza zapisów ustawy

Obowiązki operatorów usług kluczowych:

Art. 8. Operator usługi kluczowej wdraża system zarządzania bezpieczeństwem [...]

2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, **uwzględniających najnowszy stan wiedzy** [...]

e) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;

5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo [...]

Idzie nowe – czyli o NIS2

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw

Wyślij komentarz do projektu (rejestr zmian)

Wnioskodawca:	Minister Cyfryzacji
Data utworzenia:	24-04-2024
Działy:	informatyzacja,
Hasła:	INFORMATYZACJA,
Status projektu:	otwarty
Wykaz prac legislacyjnych:	Rady Ministrów
Numer z wykazu:	UC32
Projekt realizuje przepisy prawa Unii Europejskiej:	Numer i tytuł aktu prawnego Unii Europejskiej: Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80).
Kadencja:	X
Okres kadencji:	2023-...

NIS2 – co zmienia i co wprowadza?

- Więcej sektorów w zależności od istotności dla danego kraju członkowskiego
- Przedsiębiorstwa będą zobowiązane zarejestrować się w wykazie podmiotów kluczowych i ważnych prowadzonym przez ministerstwo ds. cyfryzacji
- Harmonogram zostanie przedstawiony w ciągu miesiąca od wejścia w życie ustawy
- Data rejestracji do 1 kwietnia 2025 roku

NIS2 – co zmienia i co wprowadza?

- Konieczność korzystania z systemu służącego wymianie informacji o incydentach, zagrożeniach i podatnościach
- Kształcenie i szkolenia personelu w dziedzinie cyberbezpieczeństwa

NIS2 – co zmienia?

Sektory kluczowe	Sektory ważne
Energetyka	Usługi pocztowe i kurierskie
Bankowość i rynki finansowe	Gospodarowanie odpadami
Transport	Produkcja, wytwarzanie i dystrybucja chemikaliów
Ochrona zdrowia	Produkcja, przetwarzanie i dystrybucja żywności
Wodociągi i spółki wodno-kanalizacyjne	Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro
Infrastruktura cyfrowa (dostawcy usług chmurowych, ośrodki przetwarzania danych, dostawcy punktu wymiany ruchu internetowego)	Produkcja komputerów, wyrobów elektronicznych
Administracja publiczna	Produkcja urządzeń elektrycznych
Sektor przestrzeni kosmicznej	Produkcja maszyn i urządzeń
Usługi ICT	Produkcja pojazdów samochodowych, przyczep i naczep
	Dostawcy usług cyfrowych
	Organizacje badawcze

NIS2 – co zmienia i co wprowadza?

Art. 67g 1. Minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego może, w drodze decyzji, wydać **polecenie zabezpieczające**.

2. Polecenie zabezpieczające dotyczy nieokreślonej liczby podmiotów kluczowych i podmiotów ważnych.

9. Polecenie zabezpieczające zawiera:

6) zakaz korzystania z określonego produktu [...]

NIS2 – co zmienia i co wprowadza?

Inne polecenia zabezpieczające to między innymi:

- Przeprowadzenie analizy ryzyka
- Zastosowanie określonej poprawki
- Zastosowanie szczególnej konfiguracji
- Dokonanie przeglądów planów ciągłości działania

NIS2 – kary

- Art. 73 – zaniechania podlegające karze pieniężnej oraz wysokość kary pieniężnej (art. 73. ust. 3 i ust. 4)
- Art. 73a – nałożenie kary pieniężnej na kierownika podmiotu kluczowego lub podmiotu ważnego

NIS2 – kary dla podmiotów kluczowych

- Wysokość kary pieniężnej nie może przekroczyć **10 000 000 euro** […]
- lub **2% przychodów** osiągniętych przez podmiot kluczowy z działalności gospodarczej […].
- **Kara ta nie może być jednak niższa niż 20 000 zł.**

NIS2 – inne kary

- Nieprzeprowadzenie audytu – do 200 000 zł
- Nieprzeprowadzenie szacowania ryzyka, brak zarządzania ryzykiem – do 150 000 zł
- Niewdrożenie środków technicznych i organizacyjnych uwzględniających wymogi z Art. 8 – do 100 000 zł
- Niepowołanie wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo – do 100 000 zł
- Niezgłoszenie incydentu do CSIRT – do 20 000 zł za każdy niezgłoszony incydent poważny
- Brak wdrożonej/zaktualizowanej dokumentacji – do 50 000 zł

Czy warto miec SOC?

Średni czas wykrycia zagrożenia w 2021 roku wyniósł 212 dni (IBM)

53% ataków na firmy nie zostało wykrytych (Mandiant Security Effectiveness Report)

58% ataków na podmioty państwowe pochodzi z Rosji (Microsoft)

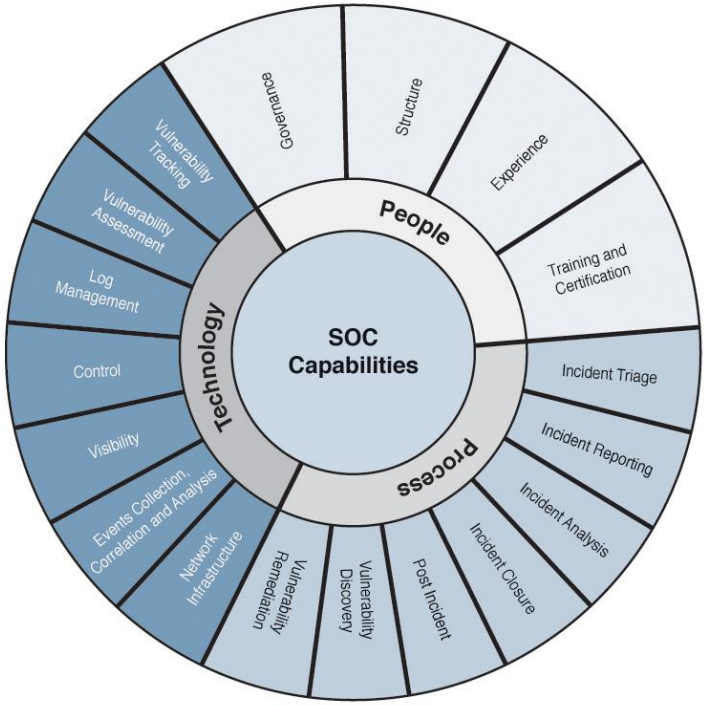
Czy warto miec SOC?

Czym zajmuje się SOC?

- Stała i wnikliwa analiza środowiska informatycznego celem zabezpieczenia przez atakami

Jak to jest osiągane?

- Analiza danych (logi, flowy) pochodzących z infrastruktury oraz zarządzanie logami
- Wykorzystanie Machine Learningu
- Stałe monitorowanie podatności
- Reagowanie i odpowiedź na zdarzenia z zakresu cyberbezpieczeństwa
- Raportowanie
- Współpraca z IT i biznesem
- Szkolenia
- RED TEAM!



Czy warto miec SOC?

network expert

MITRE ATT&CK® coverage

Your current coverage of MITRE ATT&CK® tactics and techniques, based on installed rules. Click a cell to view and enable a technique's rules. Rules must be mapped to the MITRE ATT&CK® framework to be displayed. Learn more.

Installed rule status 1 | Installed rule type 2

Search for the tactic, technique (e.g.,"defense evasion" or "TA0005") or rule name

Collapse cells Expand cells

Legend (count will include all rules selected)
>10 rules | 7-10 rules | 3-7 rules | 1-3 rules | 0 rules

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credent
1/10 techniques	1/7 techniques	7/12 techniques	11/35 techniques	15/70 techniques	13/40 techniques	29/88 techniques	12/30 te
Disabled Rules: 0	Disabled Rules: 0	Disabled Rules: 0	Disabled Rules: 0	Disabled Rules: 0	Disabled Rules: 0	Disabled Rules: 0	Disable
Enabled Rules: 4	Enabled Rules: 1	Enabled Rules: 66	Enabled Rules: 116	Enabled Rules: 178	Enabled Rules: 100	Enabled Rules: 219	Enablec
Active Scanning Sub-techniques 1/3	Acquire Infrastructure Sub-techniques 0/7	Drive-by Compromise Sub-techniques 0/0	AppleScript Sub-techniques 0/0	Accessibility Features Sub-techniques 0/0	Abuse Elevation Control Mechanism Sub-techniques 4/4	Abuse Elevation Control Mechanism Sub-techniques 4/4	Adversa Middle Sub-tec
Gather Victim Host Information Sub-techniques 0/4	Compromise Accounts Sub-techniques 0/3	Exploit Public-Facing Application Sub-techniques 0/0	CMSTP Sub-techniques 0/0	Account Manipulation Sub-techniques 3/5	Access Token Manipulation Sub-techniques 3/5	Access Token Manipulation Sub-techniques 3/5	Bash Hi Sub-tec
Gather Victim Identity Information Sub-techniques 0/3	Compromise Infrastructure Sub-techniques 0/7	External Remote Services Sub-techniques 0/0	Command and Scripting Interpreter Sub-techniques 6/8	AppCert DLLs Sub-techniques 0/0	Accessibility Features Sub-techniques 0/0	Application Access Token Sub-techniques 0/0	Brute Fo Sub-tec
Gather Victim Network Information Sub-techniques 0/6	Develop Capabilities Sub-techniques 0/4	Hardware Additions Sub-techniques 0/0	Compiled HTML File Sub-techniques 0/0	AppInit DLLs Sub-techniques 0/0	AppCert DLLs Sub-techniques 0/0	BITS Jobs Sub-techniques 0/0	Cloud I Metada Sub-tec
Gather Victim Org Information Sub-techniques 0/4	Establish Accounts Sub-techniques 0/3	Phishing Sub-techniques 2/3	Component Object Model and Distributed COM Sub-techniques 0/0	Application Shimming Sub-techniques 0/0	AppInit DLLs Sub-techniques 0/0	Binary Padding Sub-techniques 0/0	Creden Passwo Sub-tec
Phishing for Information Sub-techniques 0/3	Obtain Capabilities Sub-techniques 1/6	Replication Through Removable Media Sub-techniques 0/0	Container Administration Command Sub-techniques 0/0	Authentication Package Sub-techniques 0/0	Application Shimming Sub-techniques 0/0	Build Image on Host Sub-techniques 0/0	Creden Browse Sub-tec
Search Closed Sources Sub-techniques 0/2	Stage Capabilities Sub-techniques 0/6	Spearphishing Attachment Sub-techniques 0/0	Control Panel Items Sub-techniques 0/0	BITS Jobs Sub-techniques 0/0	Boot or Logon Autostart Execution Sub-techniques 6/15	Bypass User Account Control Sub-techniques 0/0	Creden Sub-tec
		Spearphishing Link		Boot or Logon Autostart Execution Sub-techniques 6/15	Boot or Logon		

Czy warto miec SOC?

Zalety:

- Ochrona 24/7,
- Zmniejsza ryzyko późnego wykrycia wystąpienia zagrożenia,
- Pozwala na proaktywne wykrywanie zagrożeń,
- Zwiększa świadomość zagrożeń, pozwalając na poprawę architektury bezpieczeństwa
- Zarządzanie podatnościami i odpowiednie zarządzenie logami,
- Zgodność z normami i regulacjami RODO, ISO 27000, ustawą o KSC

Czy warto miec SOC?

People, Process and Technology (PPT)

- Ludzie
- Procesy
- Technologie

Czy będzie drogo?

Własny SOC

- 1 analityk III linii – **25 000 PLN brutto**
- 2 analityków II linii – **2x 15 000 PLN brutto**
- 2 analityków I linii – **2x 10 000 PLN brutto**

Szacunkowy koszt – **900 000+ PLN/rok**

Outsourcing net.soc

Keep calm. We have SOC.

- Obsługa 24/7
- Monitoring + zarządzanie incydentami, szacowanie ryzyka itd.
- Zarządzanie podatnościami
- Zespół Red Team

Szacunkowy koszt – **100 000 – 240 000 PLN / rok**

Zespół SOC

SOC I

SOC II

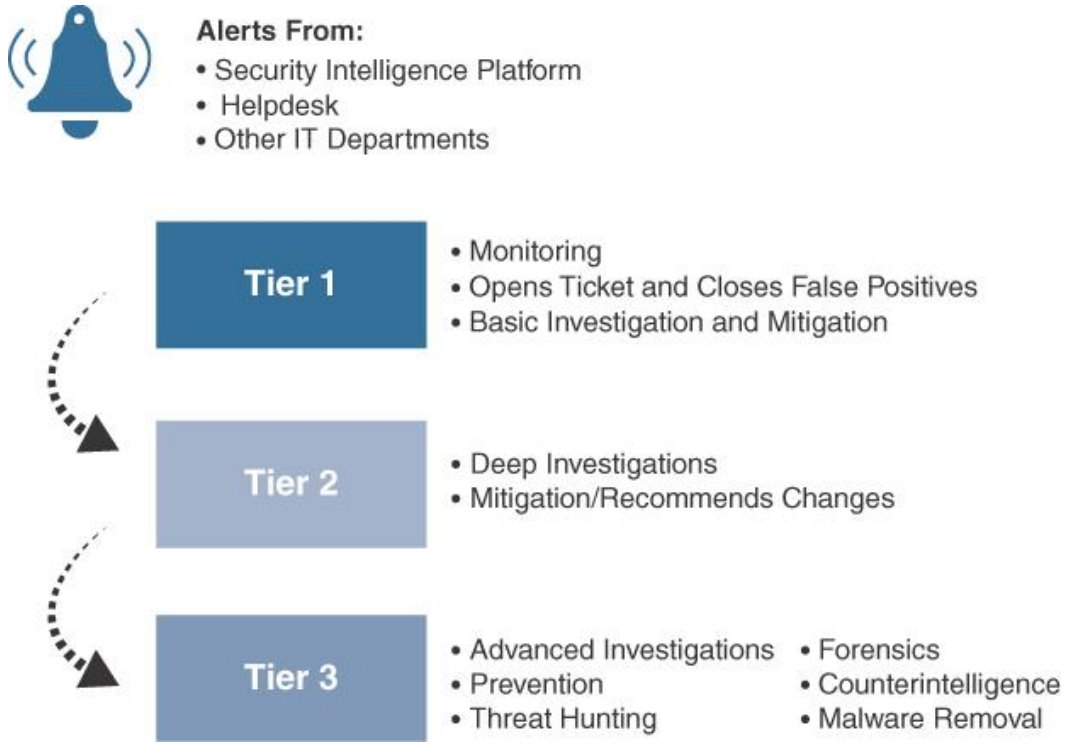
SOC III

Narzędzia wykorzystywane w SOC

- SIEM + SOAR,
- XDR,
- NGFW,
- IPS/IDS,
- NAC,
- WAF/proxy,
- Bazy threat intelligence,
- Skanery podatności.

Procesy w SOC

Instrukcje krok po kroku w celu zarządzania incydentami (1000+)




SM3

SIM3

- SIM3 jest narzędziem do badania dojrzałości usług reagowania na incydenty
- Odnosi się do czterech obszarów działania:
  - Organizacja
  - Ludzie
  - Narzędzia
  - Procesy

Table 1- Overview of SIM3v2i parameters [12]

Parameter number	Parameter description	Parameter number	Parameter Description
O-1	Mandate	T-6	Resilient Messaging
O-2	Constituency	T-7	Resilient Internet Access
O-3	Authority	T-8	Incident Prevention Toolset
O-4	Responsibility	T-9	Incident Detection Toolset
O-5	Service Description	T-10	Incident Resolution Toolset
O-6	Public Media Policy	P-1	Escalation to Governance Level
O-7	Service Level Description	P-2	Escalation to Press Function
O-8	Incident Classification	P-3	Escalation to Legal Function
O-9	Participation in CSIRT Systems	P-4	Incident Prevention Process
O-10	Organisational Framework	P-5	Incident Detection Process
O-11	Security Policy	P-6	Incident Resolution Process
H-1	Code of Conduct/Practice/Ethics	P-7	Specific Incident Processes
H-2	Staff Resilience	P-8	Audit & Feedback Process
H-3	Skillset Description	P-9	Emergency Reachability Process
H-4	Staff Development	P-10	Best Practice Internet Presence
H-5	Technical Training	P-11	Secure Information Handling Process
H-6	Soft Skills Training	P-12	Information Sources Process
H-7	External Networking	P-13	Outreach Process
T-1	IT Assets & Configuration	P-14	Governance Reporting Process
T-2	Information Sources List	P-15	Constituency Reporting Process
T-3	Consolidated Messaging System(s)	P-16	Meeting Process
T-4	Incident Tracking System	P-17	Peer Collaboration Process
T-5	Resilient Voice Calls		

SIM3

network expert

O-7: Service Level Description

Have service levels been defined for the services that your CSIRT offers? This can range from something as simple as the requirement to send a first (human) reaction to incident reports within a set amount of time, to more extensive "SLA" type requirements.

0 We never really discussed this.

1 We have a basic understanding of the level of service expected of us, but it was never written down.

2 We don't have a formal written service level description, therefore we wrote something for our own purposes. Our management has not formally approved this.

3 We have a written service level description approved by our team management.

4 We have a written service level description approved by our team management. In the periodic review of our team it is checked if and how we meet our service level(s).

SIM3

network expert

T-1: IT Resources List

Does your CSIRT have access to a list or database that describes the hardware, software, etc. commonly used in the constituency, or at least in vital parts of the constituency, so that the CSIRT can provide targeted advice? This question is about "asset management" (ISO terminology) or the "Configuration Management Database" (CMDB: ITIL terminology). The CSIRT will normally not maintain a CMDB, but at least they need to have access to it if it exists. In the absence of an advanced solution, the CSIRT may consider maintaining a limited version of such a list themselves, with the help of their security contacts in the constituency.

0 We don't really know.

1 We have a good idea of the most important IT resources, but there is no list for this.

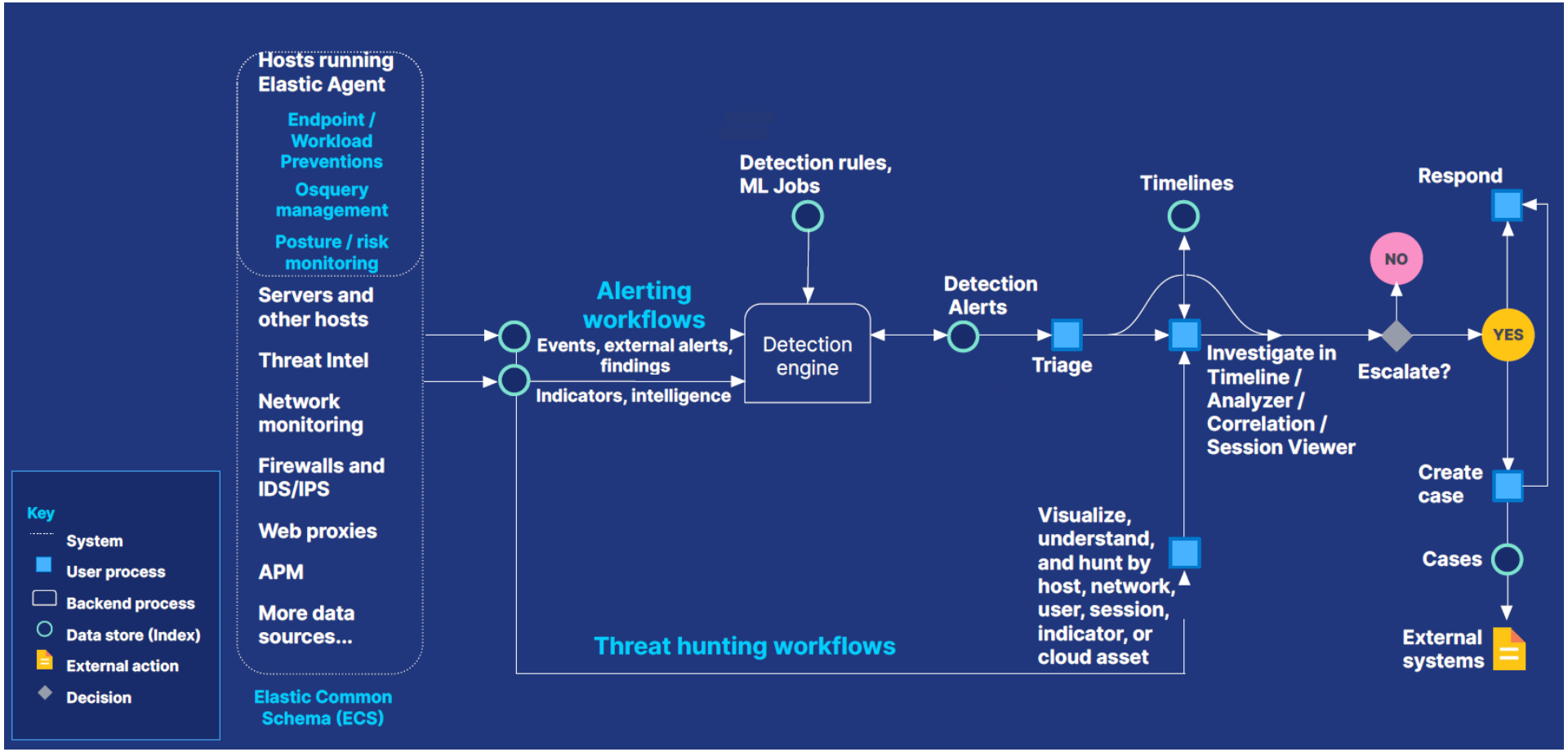
2 We don't have a formal IT resources list, therefore we wrote something for our own purposes. Our management has not formally approved this.

3 We have access to a formal IT resources list, and this has been approved by our team management.

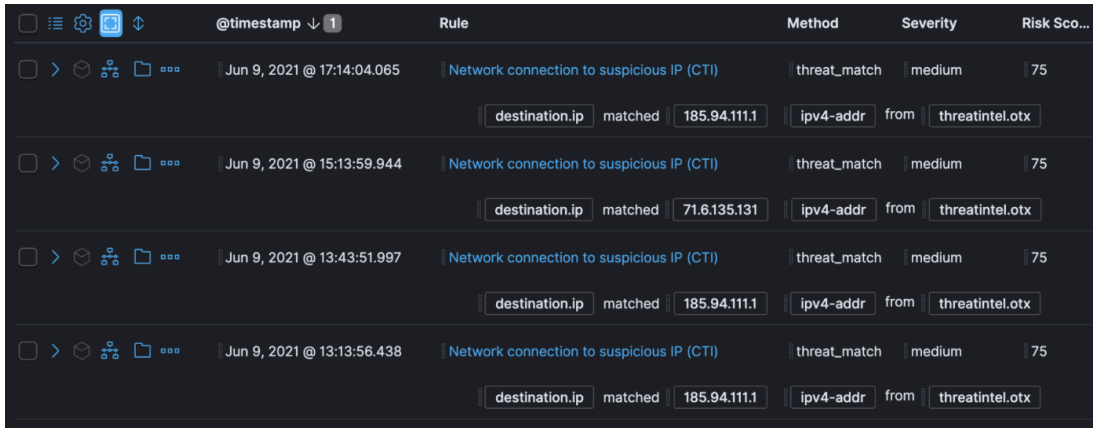
4 We have access to a formal IT resources list, and this has been approved by our team management. In the periodic review of our team it is checked if this list is useful and sufficiently accurate for the goals of our team.


elastic

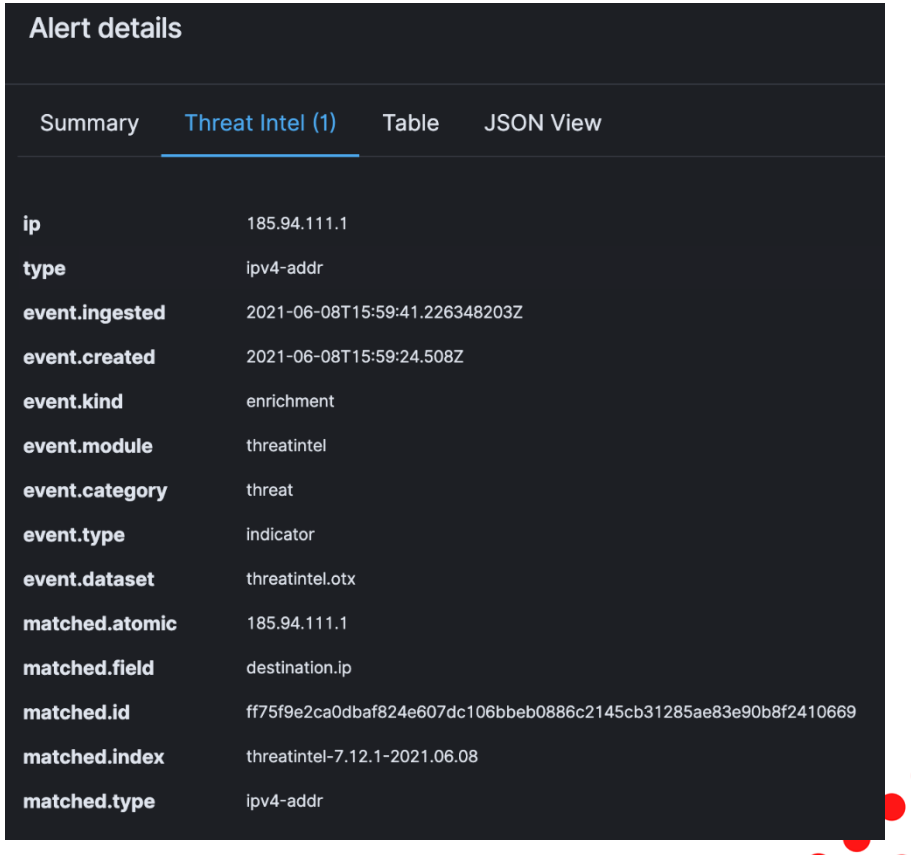
Elastic SIEM



Elastic SIEM



@timestamp ↓ 1	Rule	Method	Severity	Risk Sco...
Jun 9, 2021 @ 17:14:04.065	Network connection to suspicious IP (CTI)	threat_match	medium	75
	destination.ip matched 185.94.111.1 ipv4-addr from threatintel.otx			
Jun 9, 2021 @ 15:13:59.944	Network connection to suspicious IP (CTI)	threat_match	medium	75
	destination.ip matched 71.6.135.131 ipv4-addr from threatintel.otx			
Jun 9, 2021 @ 13:43:51.997	Network connection to suspicious IP (CTI)	threat_match	medium	75
	destination.ip matched 185.94.111.1 ipv4-addr from threatintel.otx			
Jun 9, 2021 @ 13:13:56.438	Network connection to suspicious IP (CTI)	threat_match	medium	75
	destination.ip matched 185.94.111.1 ipv4-addr from threatintel.otx			



Alert details

Summary | Threat Intel (1) | Table | JSON View

ip	185.94.111.1
type	ipv4-addr
event.ingested	2021-06-08T15:59:41.226348203Z
event.created	2021-06-08T15:59:24.508Z
event.kind	enrichment
event.module	threatintel
event.category	threat
event.type	indicator
event.dataset	threatintel.otx
matched.atomic	185.94.111.1
matched.field	destination.ip
matched.id	ff75f9e2ca0dbaf824e607dc106bbeb0886c2145cb31285ae83e90b8f2410669
matched.index	threatintel-7.12.1-2021.06.08
matched.type	ipv4-addr

Dzień z życia SOC-owca...

PowerShell Download and Execute

t winlog.event_data.ScriptBlockText

```
cd [redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
32.exe" -OutFile
[redacted]
4332.exe"; Start
-Process [redacted]
[redacted]f4332.ex
e"
```

Dzień z życia SOC-owca...

network expert

k winlog.event_data.CommandLine

powershell -Command "

Endpoints

Hosts running Elastic Defend

Filter your data using KQL syntax

Refresh

Auto ref... 10 seconds

Showing 4 endpoints

Endpoint	Agent status	Policy	Policy status	OS	IP address	Version	Last active	Actions
ubuntu-2004	Healthy Isolated	Elastic Defend integr... re...	Success	Linux	[redacted]	8.5.0	Sep 27, 2022...	▫▫▫
windows-10	Healthy	Elastic Defend integr... re...	Success	Windows	[redacted]	8.5.0	Sep 27, 2022...	▫▫▫
windows-329	Healthy	Elastic Defend integr... re...	Success	Windows	[redacted]	8.5.0	Sep 27, 2022...	▫▫▫
elastic-523	Healthy	Elastic Defend integr... re...	Success	macOS	[redacted]	8.5.0	Sep 27, 2022...	▫▫▫

Rows per page: 10

1

Dzień z życia SOC-owca...

Rule name	Count of records
Multiple Logon Failure from the same Source Address	8,118
Privileged Account Brute Force	30
Multiple Logon Failure Followed by Logon Success	7
Enumeration of Privileged Local Groups Membership	4

Dzień z życia SOC-owca...

registry.data.strings	1
registry.data.type	SZ_DWORD
registry.hive	HKLM
registry.key	SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
registry.path	HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
registry.value	DisableAntiSpyware

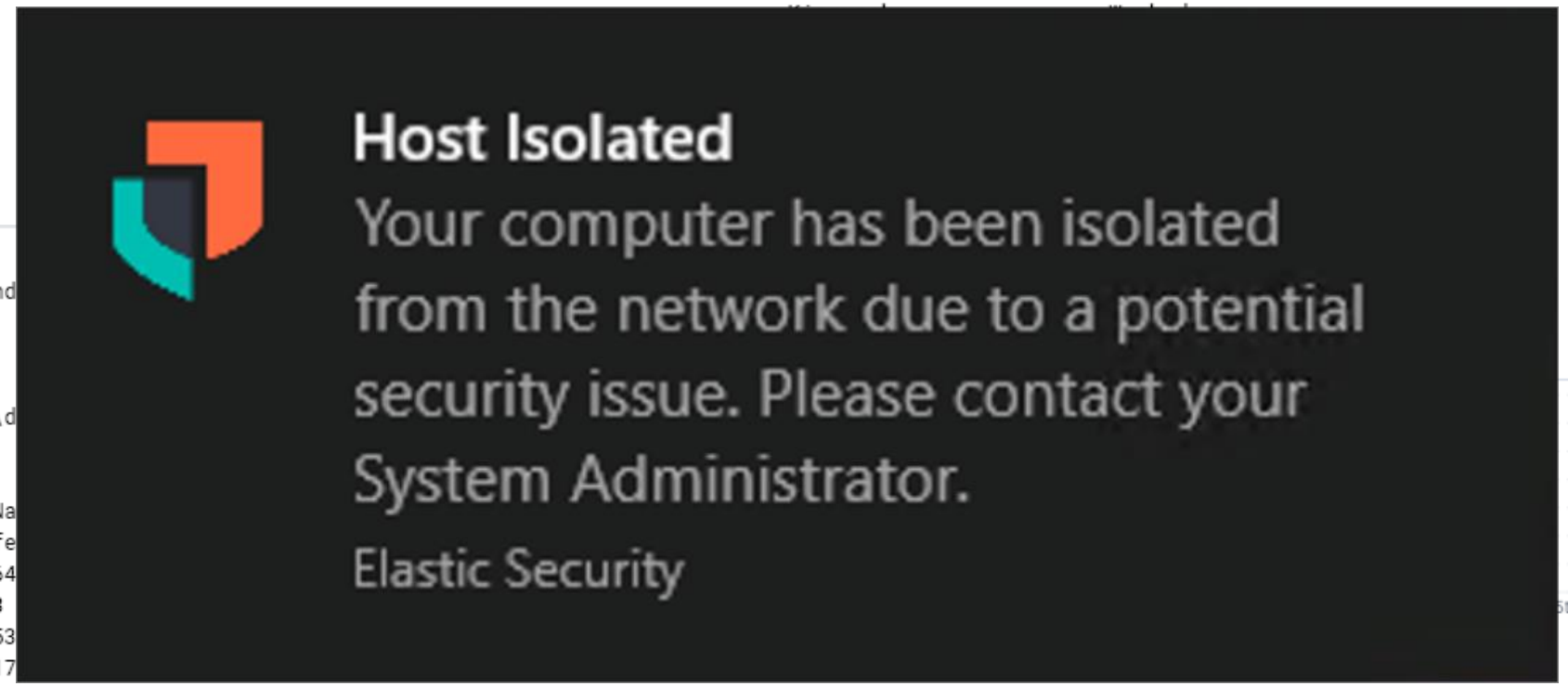
isableAntiSpyware

Dzień z życia SOC-owca...

Platforma filtrowania systemu Windows zezwoliła na połączenie.

Informacje dotyczące aplikacji:
Identyfikator procesu: 4
Nazwa aplikacji: System

Informacje dotyczące sieci:



Czas wystąpień

Platforma filtrowania systemu Wind

Informacje dotyczące aplikacji:
Identyfikator procesu:
Nazwa aplikacji: \d

Informacje dotyczące sieci:
Kierunek: Na
Adres źródłowy: fe
Port źródłowy: 64
Adres docelowy: ff02::1:3
Port docelowy: 53
Protokół: 17

Informacje dotyczące filtru:
Identyfikator wykonawczy filtru: 2272593
Nazwa warstwy: Odebranie/zaakceptowanie
Identyfikator wykonawczy warstwy: 46

Nieznane

Czy SOC jest remedium na całe zło tego swiata?

- Niewłaściwa alokacja budżetu,
- SOC jako niechciane dziecko,
- „Mnie to nie dotyczy”,
- Brak odpowiednich procedur, playbooków,
- Brak planów rozwoju,
- „Problem zazwyczaj siedzi między monitorem, a krzesłem”