EXATEL

Cyberbezpieczeństwo - lepiej zapobiegać, niż leczyć

Paweł Caban

Dyrektor Biura Rozwoju Produktów

About **EXATEL**

Wiodący Polski operator o globalnym zasięgu**,**
398 punktów interconnect,
od 1993

Największa sieć światłowodowa w Polsce -
ponad **21 800 km**,
od 2004

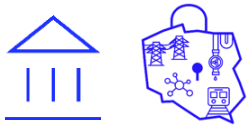
Zaawansowane usługi
Cyberbezpieczeństwa,
własny **SOC**
& **AntyDDoS TAMA**,
od 2019

Komunikacja Satelitarna, własny
Teleport
z **7 nowoczesnymi**
antenami satelitarnymi,
od 2020

1993 **2023**

Klasyfikowany jako **6-ty największa**
Polska firma IT,
prawie 600 pracowników,
z trendem wzrostowym

Usługi Zintegrowane, R&D i
elastyczność biznesowa
są naszym DNA



Sektor Publiczny, Infrastruktura Krytyczna,
projekty **Rządowe i dla Dużego biznesu** są
nasza domeną

Program podnoszenia bezpieczeństwa ICT

Certyfikat 27001,

Świadectwo bezpieczeństwa przemysłowego do poziomu Tajne,

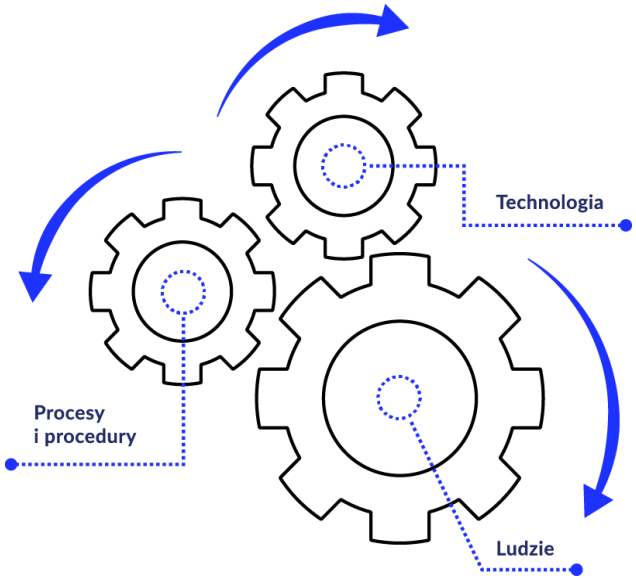
Certyfikaty UE Secret, NATO Secret

Cyberbezpieczeństwo – kluczowe elementy

Procesy i procedury

Regulacje zewnętrzne – ustawy, rozporządzenia, normy

Regulacje wewnętrzne – polityki, procedury, instrukcje



Technologie

Systemy IT/OT

Systemy zabezpieczeń IT/OT

Systemy bezpieczeństwa fizycznego

Zasilanie, klimatyzacja, PPoŻ

Personel

Kadra kierownicza

Pracownicy

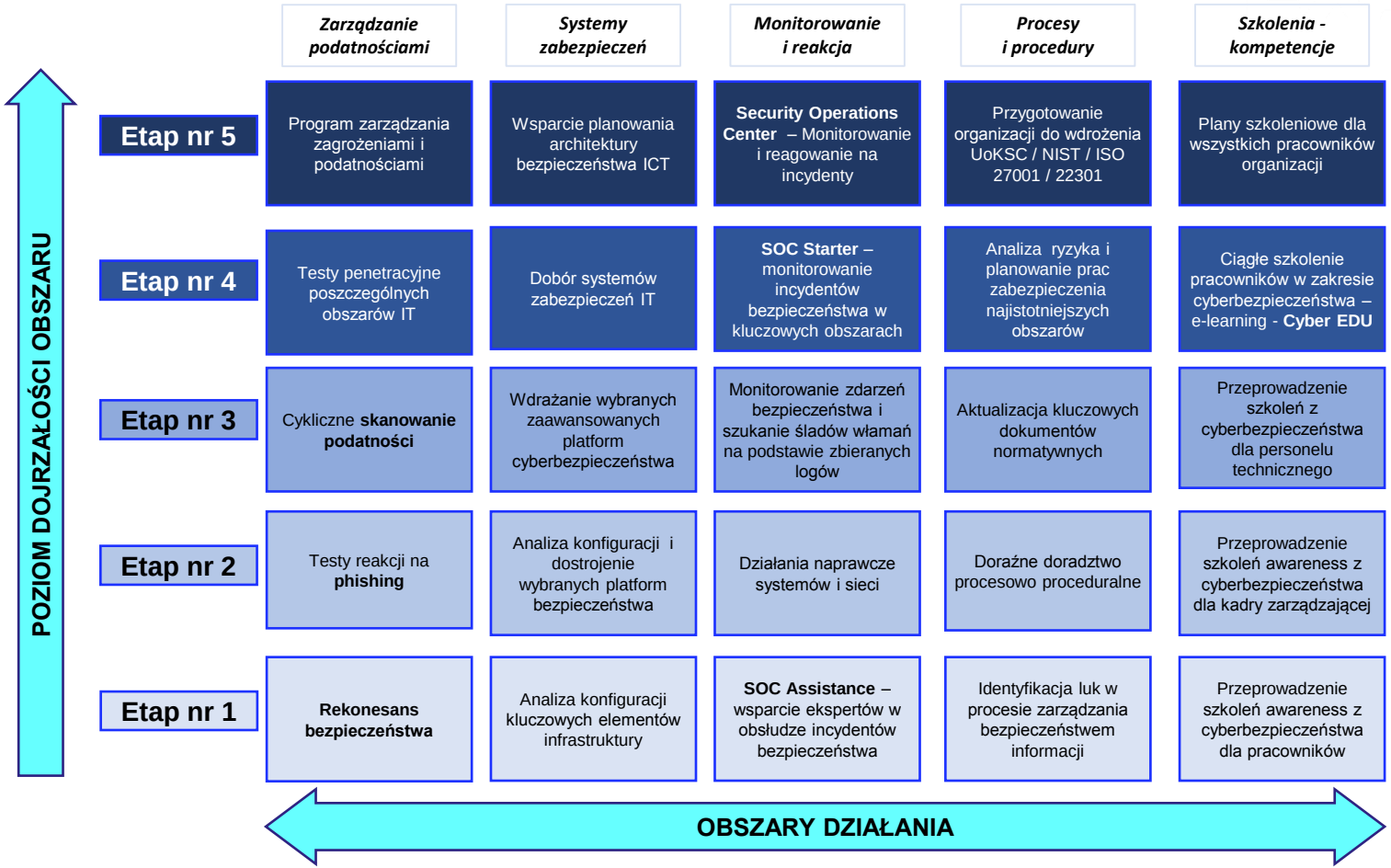
Służby IT

Kooperanci

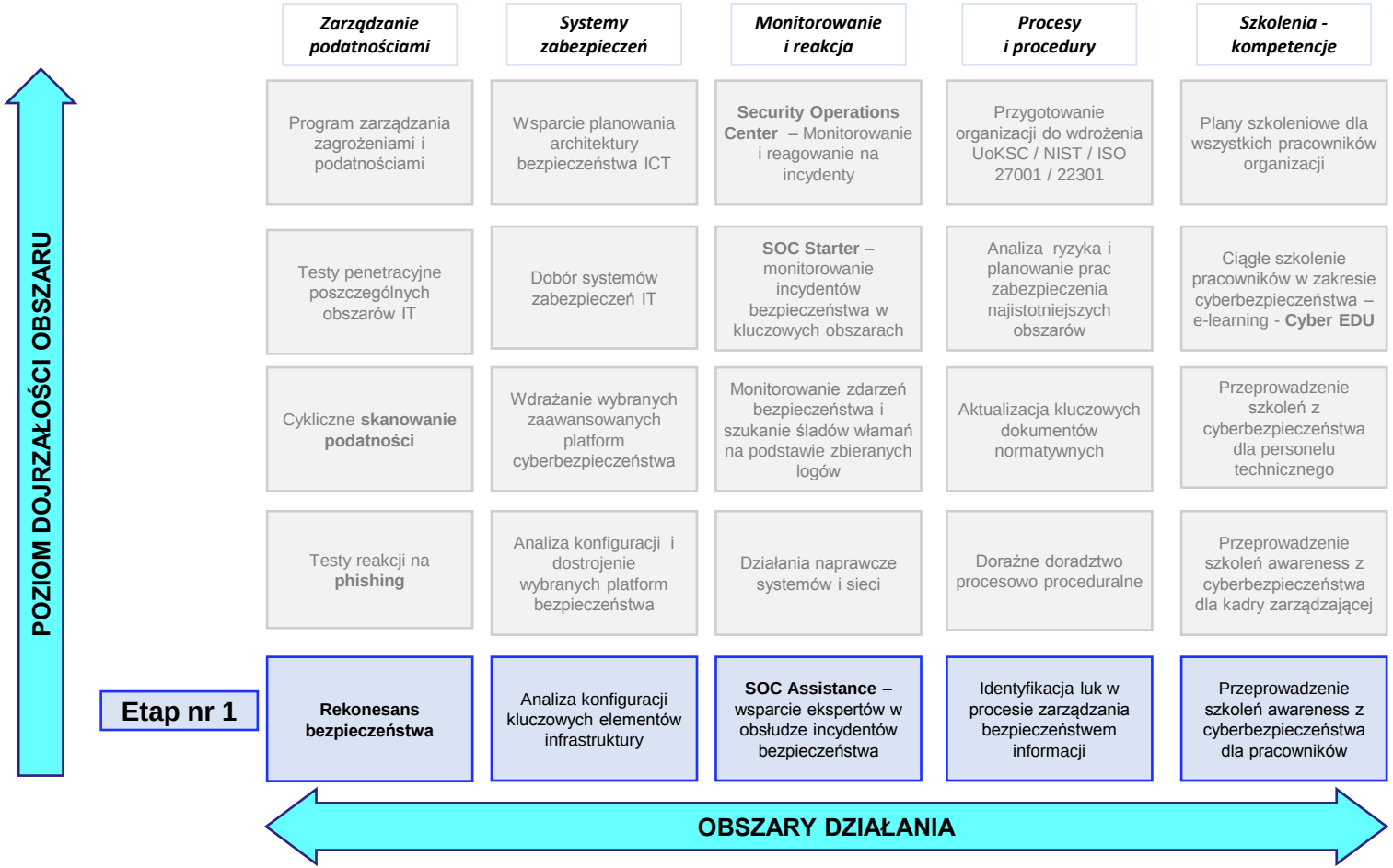
Kluczowe cechy programu podnoszenia bezpieczeństwa

- Program podnoszenia bezpieczeństwa skierowany jest do podmiotów o różnej skali i różnym poziomie dojrzałości w zakresie cyberbezpieczeństwa, **w tym także dla rozpoczynających swoją przygodę z Cyber**.
- Usługi w ramach Programu są realizowane na poziomie procesowo-proceduralnym, technicznym oraz osobowym
- **Usługi skoncentrowane są w 5 obszarach:**
  - zarządzania podatnościami
  - systemów zabezpieczeń
  - monitorowania i reakcji na incydenty bezpieczeństwa IT
  - procesów i procedur zarządzania bezpieczeństwem IT
  - podnoszenia kompetencji personelu w zakresie bezpieczeństwa IT

Elementy programu podnoszenia bezpieczeństwa



ETAP 1 programu podnoszenia bezpieczeństwa



Realizacja programu - Etap nr 1

- **Rekonesans bezpieczeństwa** – próba przełamania zabezpieczeń organizacji:
  - identyfikacja słabych punktów w zakresie cyberbezpieczeństwa z punktu widzenia atakującego
  - zalecenia mitygacyjne,
  - analiza skuteczności istniejących procesów i procedur w zakresie wykrytych słabości.
- **Analiza konfiguracji** pod kątem bezpieczeństwa kluczowych elementów infrastruktury – firewall'e, kontrolery dostępu do sieci (MS AD/LDAP), WLAN, usługi DNS/DHCP/GPO, usługi publikowane w sieci Internet.
- Objęcie usługą **SOC Assistance** – wsparcie personelu organizacji przy analizie i obsłudze incydentu.
- **Analiza skuteczności działania procesów i procedur** zarzadzania bezpieczeństwem funkcjonujących w organizacji, wskazanie brakujących procesów i procedur.
- **Przeprowadzenie szkoleń** Security Awareness dla pracowników.

ETAP 2 programu podnoszenia bezpieczeństwa

POZIOM DOJRZAŁOŚCI OBSZARU

	Zarządzanie podatnościami	*Systemy zabezpieczeń*	*Monitorowanie i reakcja*	*Procesy i procedury*	*Szkolenia - kompetencje*
	Program zarządzania zagrożeniami i podatnościami	Wsparcie planowania architektury bezpieczeństwa ICT	**Security Operations Center** – Monitorowanie i reagowanie na incydenty	Przygotowanie organizacji do wdrożenia UoKSC / NIST / ISO 27001 / 22301	Plany szkoleniowe dla wszystkich pracowników organizacji
	Testy penetracyjne poszczególnych obszarów IT	Dobór systemów zabezpieczeń IT	**SOC Starter** – monitorowanie incydentów bezpieczeństwa w kluczowych obszarach	Analiza ryzyka i planowanie prac zabezpieczenia najistotniejszych obszarów	Ciągłe szkolenie pracowników w zakresie cyberbezpieczeństwa – e-learning - **Cyber EDU**
	Cykliczne **skanowanie podatności**	Wdrażanie wybranych zaawansowanych platform cyberbezpieczeństwa	Monitorowanie zdarzeń bezpieczeństwa i szukanie śladów włamań na podstawie zbieranych logów	Aktualizacja kluczowych dokumentów normatywnych	Przeprowadzenie szkoleń z cyberbezpieczeństwa dla personelu technicznego
Etap nr 2	Testy reakcji na **phishing**	Analiza konfiguracji i dostrojenie wybranych platform bezpieczeństwa	Działania naprawcze systemów i sieci	Doraźne doradztwo procesowo proceduralne	Przeprowadzenie szkoleń awareness z cyberbezpieczeństwa dla kadry zarządzającej
	Rekonesans bezpieczeństwa	Analiza konfiguracji kluczowych elementów infrastruktury	**SOC Assistance** – wsparcie ekspertów w obsłudze incydentów bezpieczeństwa	Identyfikacja luk w procesie zarządzania bezpieczeństwem informacji	Przeprowadzenie szkoleń awareness z cyberbezpieczeństwa dla pracowników

OBSZARY DZIAŁANIA

Realizacja programu - Etap nr 2

Etap nr 2 obejmuje zadania zdefiniowane w etapie 1,

Rozszerzone o realizację zadań poniżej:

- Analiza konfiguracji i dostrojenie systemów bezpieczeństwa w zakresie posiadanych przez EXATEL kompetencji,
- Testy reakcji pracowników na **phishing** – oparte na dedykowanej dla każdego klienta kampanii – **także jako samodzielna usługa,**
- **Rekonfiguracja** pod kątem bezpieczeństwa systemów oraz sieci mitygujące słabości zidentyfikowane w trakcie rekonesansu,
- Uzupełnienie procesów zarządzania bezpieczeństwem IT o niezbędne procedury – aktualizacja dokumentacji,
- Przeprowadzenie szkoleń Security Awareness dla kadry zarządczej.

ETAP 3 programu podnoszenia bezpieczeństwa

POZIOM DOJRZAŁOŚCI OBSZARU

	Zarządzanie podatnościami	*Systemy zabezpieczeń*	*Monitorowanie i reakcja*	*Procesy i procedury*	*Szkolenia - kompetencje*
	Program zarządzania zagrożeniami i podatnościami	Wsparcie planowania architektury bezpieczeństwa ICT	**Security Operations Center** – Monitorowanie i reagowanie na incydenty	Przygotowanie organizacji do wdrożenia UoKSC / NIST / ISO 27001 / 22301	Plany szkoleniowe dla wszystkich pracowników organizacji
	Testy penetracyjne poszczególnych obszarów IT	Dobór systemów zabezpieczeń IT	**SOC Starter** – monitorowanie incydentów bezpieczeństwa w kluczowych obszarach	Analiza ryzyka i planowanie prac zabezpieczenia najistotniejszych obszarów	Ciągłe szkolenie pracowników w zakresie cyberbezpieczeństwa – e-learning - **Cyber EDU**
Etap nr 3	Cykliczne **skanowanie podatności**	Wdrażanie wybranych zaawansowanych platform cyberbezpieczeństwa	Monitorowanie zdarzeń bezpieczeństwa i szukanie śladów włamań na podstawie zbieranych logów	Aktualizacja kluczowych dokumentów normatywnych	Przeprowadzenie szkoleń z cyberbezpieczeństwa dla personelu technicznego
	Testy reakcji na **phishing**	Analiza konfiguracji i dostrojenie wybranych platform bezpieczeństwa	Działania naprawcze systemów i sieci	Doraźne doradztwo procesowo proceduralne	Przeprowadzenie szkoleń awareness z cyberbezpieczeństwa dla kadry zarządzającej
	Rekonesans bezpieczeństwa	Analiza konfiguracji kluczowych elementów infrastruktury	**SOC Assistance** – wsparcie ekspertów w obsłudze incydentów bezpieczeństwa	Identyfikacja luk w procesie zarządzania bezpieczeństwem informacji	Przeprowadzenie szkoleń awareness z cyberbezpieczeństwa dla pracowników

OBSZARY DZIAŁANIA

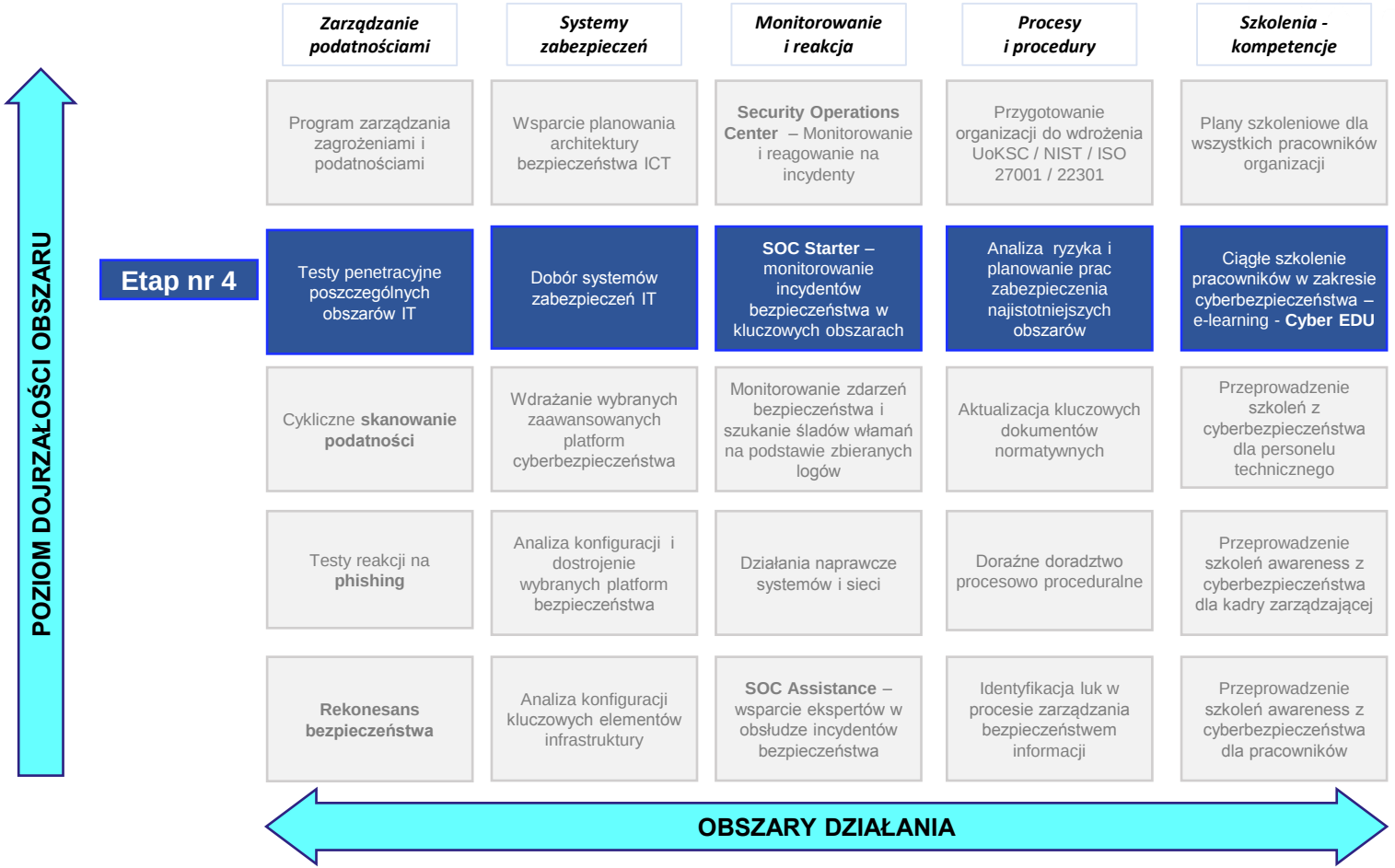
Realizacja programu - Etap nr 3

Etap nr 3 obejmuje zadania zdefiniowane w etapie 1 i 2,

Rozszerzone o realizację zadań poniżej:

- Wdrożenie cyklicznego identyfikowania i mitygacji podatności opartego o skaner podatności oraz ekspercką wiedzę konsultantów EXATEL,
- Wdrożenie niezbędnych platform bezpieczeństwa na bazie zidentyfikowanych podatności i zagrożeń,
- Rozszerzenie zakresu usługi SOC Assistance o aktywne poszukiwanie śladów niedopuszczalnej aktywności w systemach – **Threat Hunting**,
- Aktualizacja i uzupełnienie dokumentacji procesów i procedur zarządzania bezpieczeństwem informacji,
- Przeprowadzenie szkoleń personelu IT/Security w formie warsztatów.

ETAP 4 programu podnoszenia bezpieczeństwa



Realizacja programu - Etap nr 4

Etap nr 4 obejmuje zadania zdefiniowane w etapach 1 do 3,

Rozszerzone o realizację zadań poniżej:

- Przeprowadzenie testów penetracyjnych dla kolejnych obszarów IT,
- Analiza architektury systemów IT pod kątem doboru optymalnych systemów bezpieczeństwa na bazie przeprowadzonej analizy ryzyka,
- **Objęcie organizacji usługą SOC** w zakresie ograniczonym do krytycznych elementów infrastruktury,
- Wdrożenie formalnego procesu analizy ryzyka,
- Wdrożenie **ciągłego szkolenia pracowników** w zakresie cyberbezpieczeństwa poprzez dostarczoną przez EXATEL platformę e-learningową **„Cyber EDUKACJA”**.

ETAP 5 programu podnoszenia bezpieczeństwa

POZIOM DOJRZAŁOŚCI OBSZARU

	Zarządzanie podatnościami	*Systemy zabezpieczeń*	*Monitorowanie i reakcja*	*Procesy i procedury*	*Szkolenia - kompetencje*
Etap nr 5	Program zarządzania zagrożeniami i podatnościami	Wsparcie planowania architektury bezpieczeństwa ICT	**Security Operations Center** – Monitorowanie i reagowanie na incydenty	Przygotowanie organizacji do wdrożenia UoKSC / NIST / ISO 27001 / 22301	Plany szkoleniowe dla wszystkich pracowników organizacji
	Testy penetracyjne poszczególnych obszarów IT	Dobór systemów zabezpieczeń IT	**SOC Starter** – monitorowanie incydentów bezpieczeństwa w kluczowych obszarach	Analiza ryzyka i planowanie prac zabezpieczenia najistotniejszych obszarów	Ciągłe szkolenie pracowników w zakresie cyberbezpieczeństwa – e-learning - **Cyber EDU**
	Cykliczne **skanowanie podatności**	Wdrażanie wybranych zaawansowanych platform cyberbezpieczeństwa	Monitorowanie zdarzeń bezpieczeństwa i szukanie śladów włamań na podstawie zbieranych logów	Aktualizacja kluczowych dokumentów normatywnych	Przeprowadzenie szkoleń z cyberbezpieczeństwa dla personelu technicznego
	Testy reakcji na **phishing**	Analiza konfiguracji i dostrojenie wybranych platform bezpieczeństwa	Działania naprawcze systemów i sieci	Doraźne doradztwo procesowo proceduralne	Przeprowadzenie szkoleń awareness z cyberbezpieczeństwa dla kadry zarządzającej
	Rekonesans bezpieczeństwa	Analiza konfiguracji kluczowych elementów infrastruktury	**SOC Assistance** – wsparcie ekspertów w obsłudze incydentów bezpieczeństwa	Identyfikacja luk w procesie zarządzania bezpieczeństwem informacji	Przeprowadzenie szkoleń awareness z cyberbezpieczeństwa dla pracowników

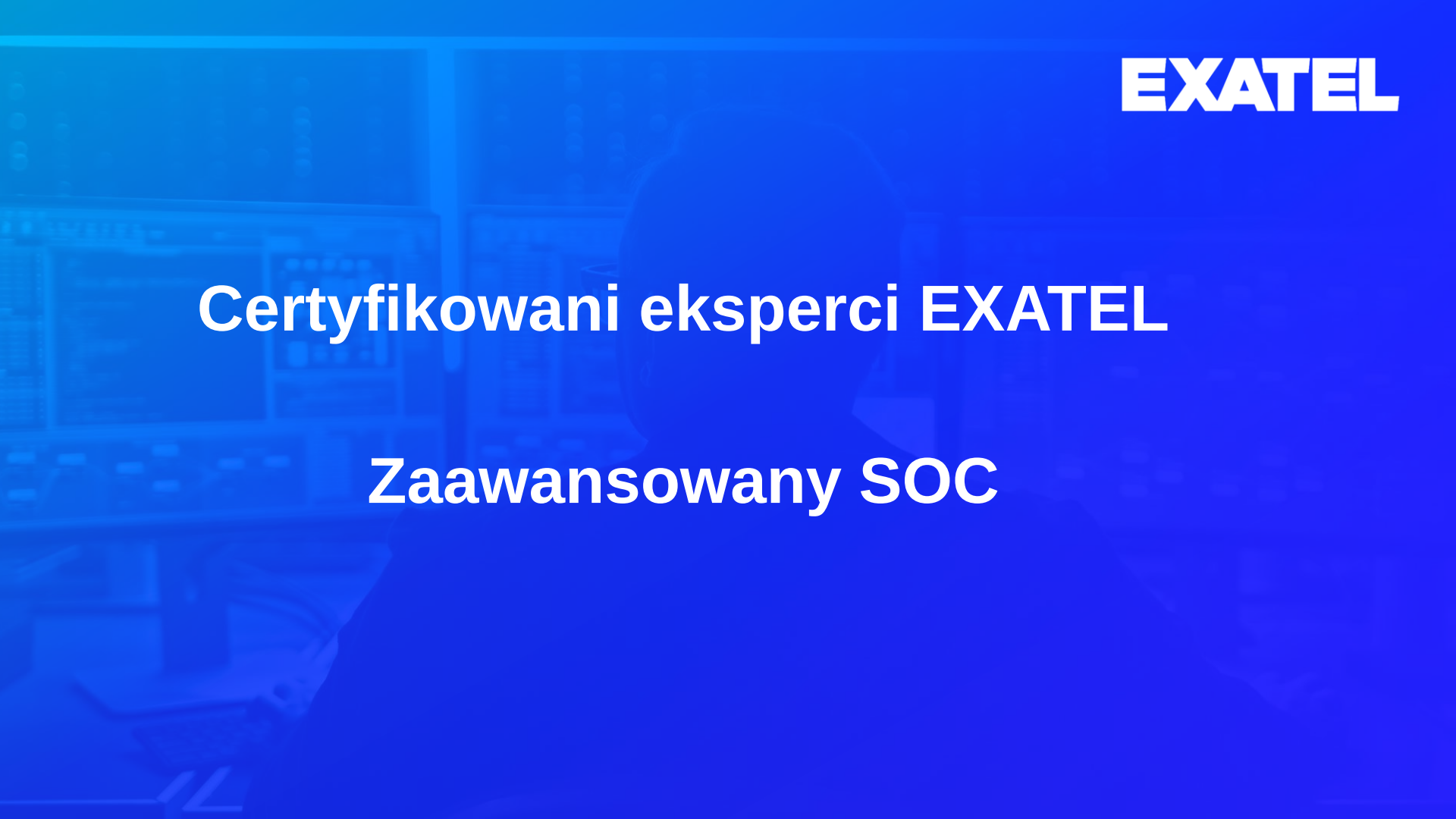
OBSZARY DZIAŁANIA

Realizacja programu - Etap nr 5

Etap nr 5 obejmuje zadania zdefiniowane w etapach 1 do 4,

Rozszerzone o realizację zadań poniżej:

- Wdrożenie procesu zarządzania podatnościami,
- Wsparcie procesu planowania architektury IT w celu spełnienia wymagań związanych z bezpieczeństwem,
- Wdrożenie w organizacji **Security Operations Center**,
- Przygotowanie organizacji do spełnienia wymagań UoKSC; ISO 27001; ISO 22301; NIST,
- Wdrożenie programów rozwoju kompetencji w zakresie cyberbezpieczeństwa dedykowanych dla poszczególnych grup pracowników organizacji.


EXATEL
Certyfikowani eksperci EXATEL
Zaawansowany SOC

Centrum bezpieczeństwa EXATEL

Usługi z obszaru cyberbezpieczeństwa teleinformatycznego oparte są na 3 fundamentach:

ludziach, technologii i procesach.

Personel

- **Ponad 30 specjalistów**, wyłącznie obywatele polscy, zatrudnieni na umowę o pracę.
- **25 certyfikatów**, minimum 2-3 letnie doświadczenie zawodowe.

25

certificates

Certyfikat 27001, Świadectwo bezpieczeństwa przemysłowego do poziomu Tajne, Certyfikaty UE Secret, NATO Secret

ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, CISA, OSCP, OSWP, CEH, CySA+, CompTia Security+, CCIE, CCNP, CCNA, CCDA, PCNSE, GCIH, CIHE, OSCE, OSWE, CISSP, CCS,

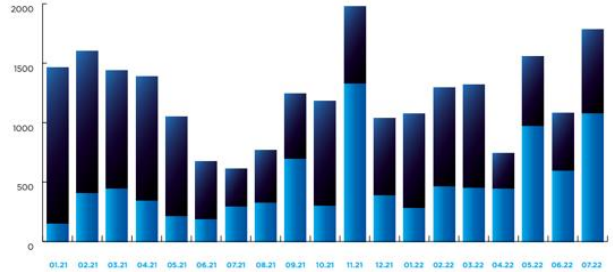
Zespoły

- Zespół Bezpieczeństwa Ofensywnego
- Zespół Monitorowania i Reagowania
- Zespół Procesowo-Proceduralny

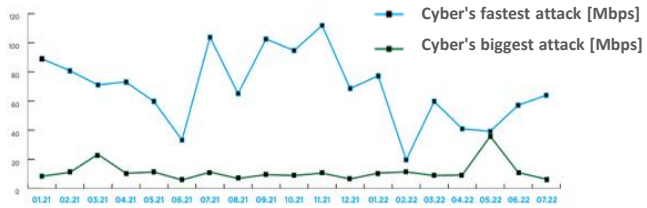
Usługi monitorowania naruszeń i reagowania na incydenty cyberbezpieczeństwa

Security Operations Center - wyspecjalizowana komórka organizacyjna, która odpowiada za identyfikację, prewencję i ochronę zasobów IT przed różnego rodzaju cyberzagrożeniami.

DDoS mitigations in EXATEL - monthly



Cyber attacks registered in EXATEL - monthly



3 linie wsparcia SOC:

- **1 linia** – wyspecjalizowana w obsłudze klienta, monitoringu stanu bezpieczeństwa ICT, selekcji i priorytetyzacji incydentów,
- **2 linia** – odpowiedzialna za zarządzanie incydentami, raportowanie, zalecenia mitygacyjne,
- **3 linia** – eksperci od zaawansowanych technik ataku i najbardziej skomplikowanych zagrożeń, administratorzy platform bezpieczeństwa.

250
projektów
of security level verification in our Customers

1400
incydentów
monthly, supported by EXATEL SOC

>1000
mitygacji
monthly, of DDoS attacks,

Dziękuję

EXATEL

EXATEL S.A.
Ul. Perkuna 47
04-164 Warszawa
NIP: 527 010 45 68

facebook.com/EXATELPL

twitter.com/exatel_pl

youtube.com/c/EXATEL_polska