



# Outsourcing cyberbezpieczeństwa, który się opłaca

Cyberataki stają się coraz poważniejszym zagrożeniem. Ich liczba skokowo wzrosła w 2022 r. w związku z sytuacją geopolityczną. Z danych CheckPoint wynika, że polskie firmy są atakowane przez hakerów średnio co 9 minut – plasuje to nas na szóstym miejscu w Europie pod względem zagrożeń cybernetycznych. Jak zabezpieczyć się przed włamaniem? Istnieją dwa możliwe scenariusze – budowa własnych struktur bezpieczeństwa oraz ich outsourcing. Firma Synthos zdecydowała się na to drugie rozwiązanie, powierzając swoje bezpieczeństwo teleinformatyczne Netii.

## O KLIENCIE

Synthos S.A. jest jednym z największych producentów surowców chemicznych w Polsce. Działalność Grupy Kapitałowej Synthos S.A. obejmuje produkcję i sprzedaż produktów chemicznych wykorzystanych jako surowce i produkty pośrednie w różnych sektorach przemysłu, szczególnie w przemyśle oponiarskim, w branży budowlanej, branży opakowań oraz segmencie agro.

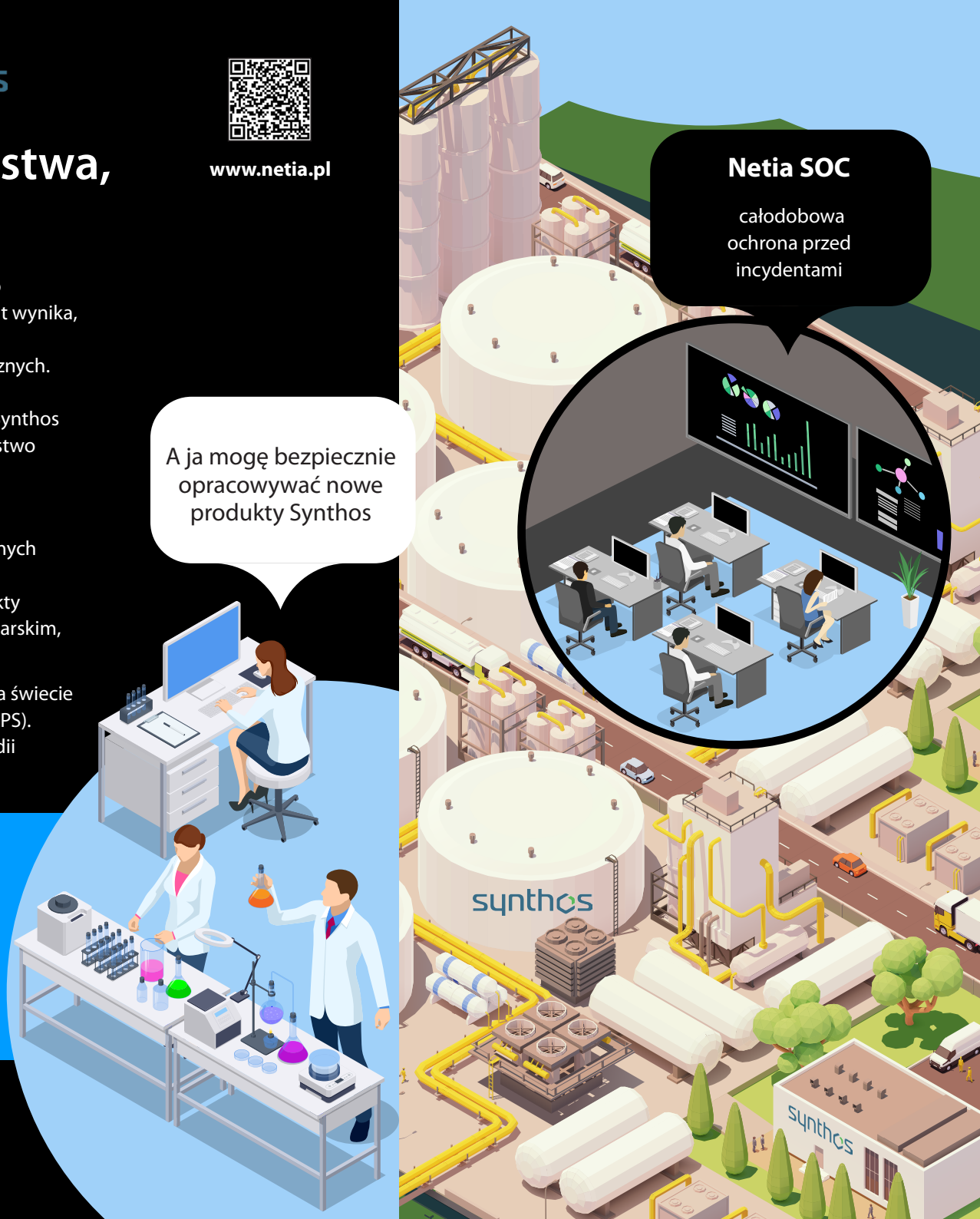
Spółka jest drugim największym producentem kauczuku syntetycznego na świecie i największym europejskim producentem polistyrenu ekspandowanego (EPS). Posiada sześć zakładów produkcyjnych w Polsce, Czechach, Francji, Holandii oraz Niemczech i zatrudnia ponad 3 600 pracowników.

Dzięki współpracy z Netią nasze zabezpieczenia zostały uzupełnione między innymi o monitoring 24/7 oraz wsparcie w analizie i mitygacji zagrożeń. W obecnych, niebezpiecznych czasach jest to wymóg nie tylko techniczny, ale coraz częściej również formalny. Budowa własnego SOC jest dla większości, nawet dużych firm nieefektywna kosztowo i skomplikowana. Stąd kluczowe jest znalezienie solidnego partnera, który uzupełni systemy bezpieczeństwa wdrażając ustandaryzowane procesy i rozwiązania.

A ja mogę bezpiecznie opracowywać nowe produkty Synthos

## Netia SOC

całodobowa  
ochrona przed  
incydentami



# Bezkompromisowe bezpieczeństwo



## WYZWANIE

Pracownicy Synthos doskonale zdawali sobie sprawę z tego, jak ważna jest ochrona biznesu przed cyberatakami. Brakowało im jednak czasu i kompetencji, aby samodzielnie wdrożyć rozwiązania, które skutecznie chroniłyby firmowe dane i infrastrukturę IT w 6 lokalizacjach. Co więcej, budowa własnego zespołu specjalistów ds. cyberbezpieczeństwa byłaby zbyt trudna i kosztowna. W związku z tym firma zdecydowała się na usługę Netia SOC (Security Operations Center), realizowaną przez zaufanego i dobrze znanego w Polsce integratora usług DATA i rozwiązań ICT.

## DLACZEGO NETIA?

### Kompleksowa oferta

Netia stworzyła dla Klienta niestandardową ofertę w zakresie cyberbezpieczeństwa, obejmującą trzy linie wsparcia. W ramach świadczonej usługi Netia SOC zapewniona jest nie tylko całodobowa ochrona infrastruktury IT, ale także: wsparcie w zakresie tworzenia scenariuszy ewentualnych ataków, poszukiwanie luk w zabezpieczeniach, pomoc w rozwiązywaniu wykrytych problemów oraz zgłaszanie ewentualnych incydentów do CSIRT. Dokładnie takich kompetencji poszukiwał Synthos.

### Redundancja zasobów

Netia dysponuje dwoma niezależnymi ośrodkami Security Operations Center w Warszawie i Katowicach oraz pięcioma obiektami Data Center. Dzięki temu infrastruktura teleinformatyczna Klienta

jest chroniona przez cały czas, nawet jeśli w jednym z ośrodków doszłoby do awarii.

### Renomowany dostawca

Netia zatrudnia najlepszych ekspertów w branży. Wielu z nich może pochwalić się kilkunastoletnim doświadczeniem w monitoringu bezpieczeństwa teleinformatycznego. Co ważne, jest to zespół na stałe pracujący w Netii (a nie zewnętrzni konsultanci), który gwarantuje swoje wsparcie w trybie 24/7/365.

### Najnowocześniejsze technologie cybersecurity

Usługi cyberbezpieczeństwa od Netii oparte są o najnowocześniejsze i cenione na całym świecie technologie i dostawców. Wśród nich takie rozwiązania, jak SIEM i SOAR oparte o technologię LogPoint.

## PROCES

Wdrożenie usługi Netia SOC rozpoczęło się od konfiguracji oprogramowania cybersecurity i jego integracji z rozwiązaniami Klienta, zaczynając od systemów krytycznych. Inżynierowie Netii dołożyli wszelkich starań, aby cały proces odbył się jak najszybciej i w możliwie najbezpieczniejszy sposób.

Wykorzystane oprogramowanie cały czas uczy się specyfiki działalności firmy Synthos, dzięki czemu ewoluuje wraz ze zmieniającymi się potrzebami biznesowymi. Równolegle, eksperci Netii dbają o utrzymanie infrastruktury, wdrażając wymagane zmiany konfiguracji i aktualizacje oprogramowania.

## KORZYŚCI BIZNESOWE



### Całodobowa ochrona nad danymi

Ekspersi Netii cały czas czuwają nad bezpieczeństwem infrastruktury teleinformatycznej Synthos. Szukają potencjalnych luk w zabezpieczeniach, analizują wyniki symulowanych ataków oraz przygotowują rekomendacje zmian i raporty, dokumentujące podjęte działania.



### Możliwość korzystania z wiedzy ekspertów

W razie jakichkolwiek wątpliwości Klient może zwrócić się do ekspertów Netii po fachową wiedzę i wsparcie. Co więcej, ma możliwość skorzystania ze szkoleń z zakresu cyberbezpieczeństwa dla swoich pracowników.



### Znaczne oszczędności

Budowa własnego zespołu SOC jest bardziej kosztowna niż outsourcing usług z obszaru cyberbezpieczeństwa. Powierzając Netii zadanie ochrony własnej infrastruktury IT, można uzyskać wysoką jakość usług SOC przy relatywnie niskiej cenie, m.in. dzięki częściowej automatyzacji niektórych procesów.



### Większa swoboda w rozwoju

Dzięki temu, że kwestie cyberbezpieczeństwa są w rękach specjalistów Netii, pracownicy Synthos mogą się skupić na innych działaniach. Jednym z możliwych scenariuszy na przyszłość jest praca nad systemami automatyki przemysłowej.