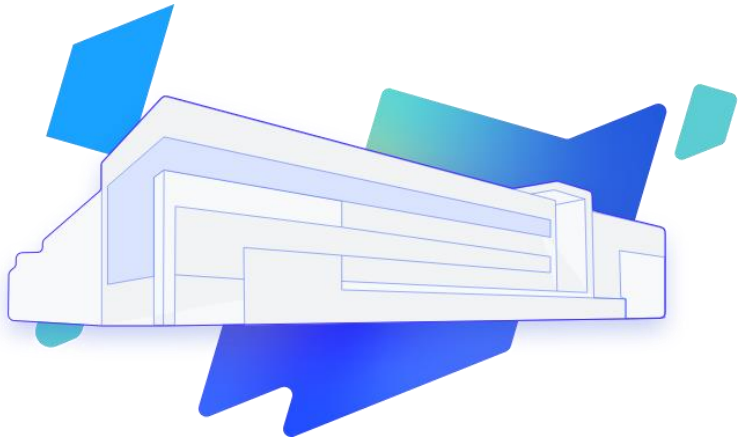
Kim jesteśmy?

Data Center



Exea Data Center to nowoczesne i bezpieczne polskie centrum danych zaprojektowane od podstaw do świadczenia usług w najwyższym standardzie. Jesteśmy jedyną w Polsce serwerownią z oficjalną certyfikacją TIER III. Tworzymy zespół ponad 50 ekspertów.

Specjalizujemy się w dostarczeniu wydajnych, praktycznych i kompleksowych rozwiązań technologicznych, które zapewniają stabilność IT, bezpieczeństwo oraz ciągłość działania.

Nasz zespół CyberSecurity to zespół analityków bezpieczeństwa i inżynierów, którzy w trybie 24/7/365 zajmuje się monitorowaniem i reagowaniem na zagrożenia cyberbezpieczeństwa w organizacji klienta.

ISO 27017 ISOQAR REGISTERED alcumus.com

ISO 27001 ISOQAR REGISTERED alcumus.com

TIER III DESIGN™ TARR Centrum Innowacyjności EXEA Data Center 26 August 2014 UPTIME INSTITUTE CERTIFIED

TIER III FACILITY® TARR Centrum Innowacyjności EXEA Data Center, Phase 1&2 2 November 2015 UPTIME INSTITUTE CERTIFIED

C|EH Certified Ethical Hacker

CompTIA Security+ CERTIFIED·CE

CompTIA PenTest+ CERTIFIED·CE

exea®

Co robimy?

Wykorzystujemy zaawansowane technologie, aby zbierać, analizować i reagować na informacje z różnych źródeł, takich jak systemy antywirusowe, logi z serwerów, urządzeń sieciowych, aplikacji, itp.

W zależności od poziomu wsparcia, zapewniamy ochronę przed atakami hakerskimi, wykrywanie nieprawidłowości w działaniu systemów i aplikacji oraz reagowanie na incydenty bezpieczeństwa, takie jak naruszenia danych, wycieki informacji i inne zagrożenia. Współpracujemy z zespołami ds. bezpieczeństwa wewnątrz organizacji klienta, aby opracowywać i wdrażać strategie bezpieczeństwa oraz dostarczać raporty i analizy dotyczące zagrożeń i incydentów.

Przeprowadzamy również:

- testy penetracyjne,
- testy socjotechniczne.

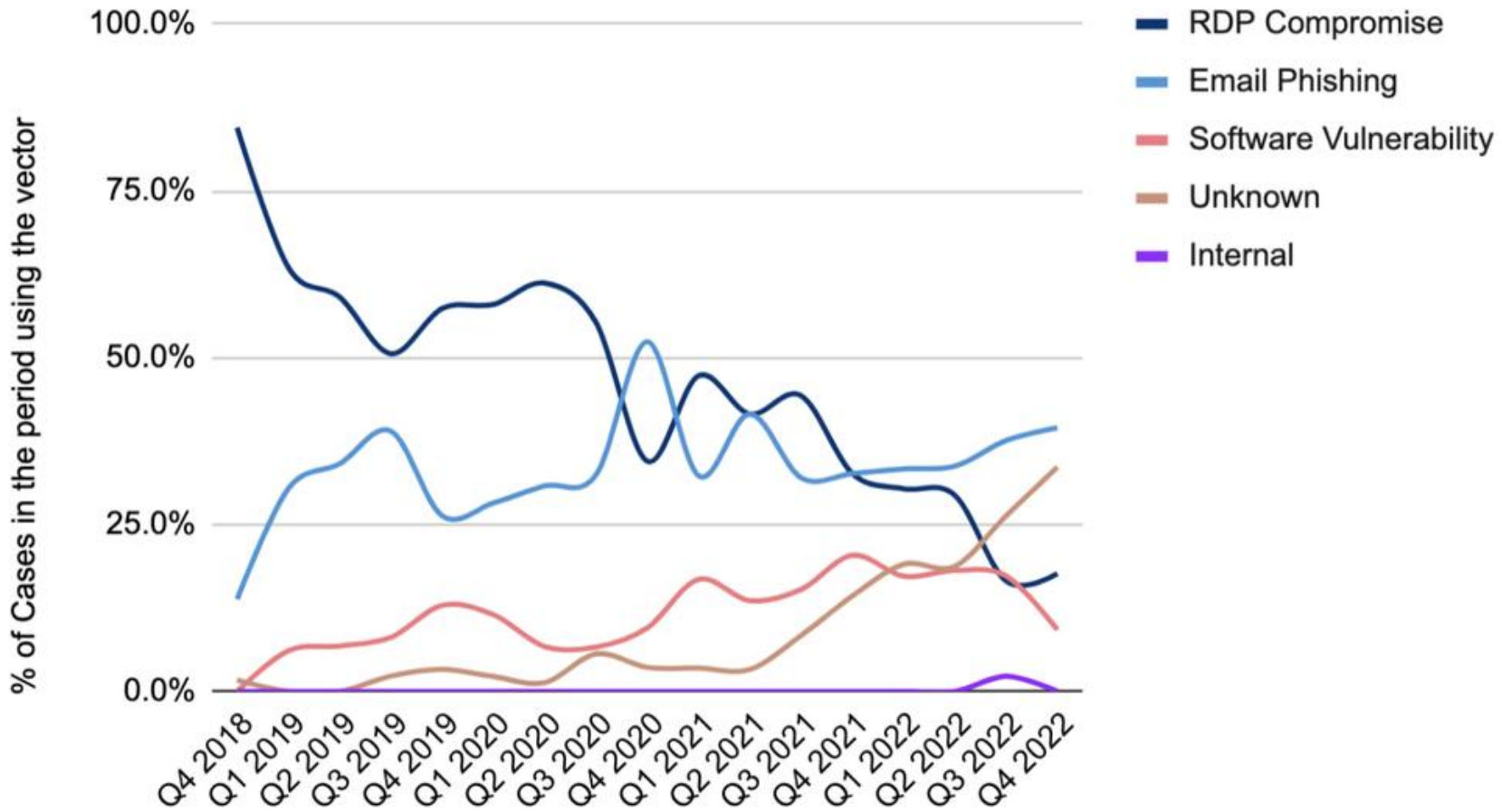
exea®

Agenda

1. Ataki ransomware w liczbach.
2. Ransomware w praktyce - szyfrowanie organizacji.
3. Instrumenty wsparcia dla cyberzagrożeń.
4. Analiza ataku ransomware.
5. Co zrobić, jeśli doszło do zaszyfrowania danych?

Ataki ransomware w liczbach

Ransomware Attack Vectors



COVEWARE

exea®

Average and median ransom Payment in Q4 2022

Average Ransom Payment

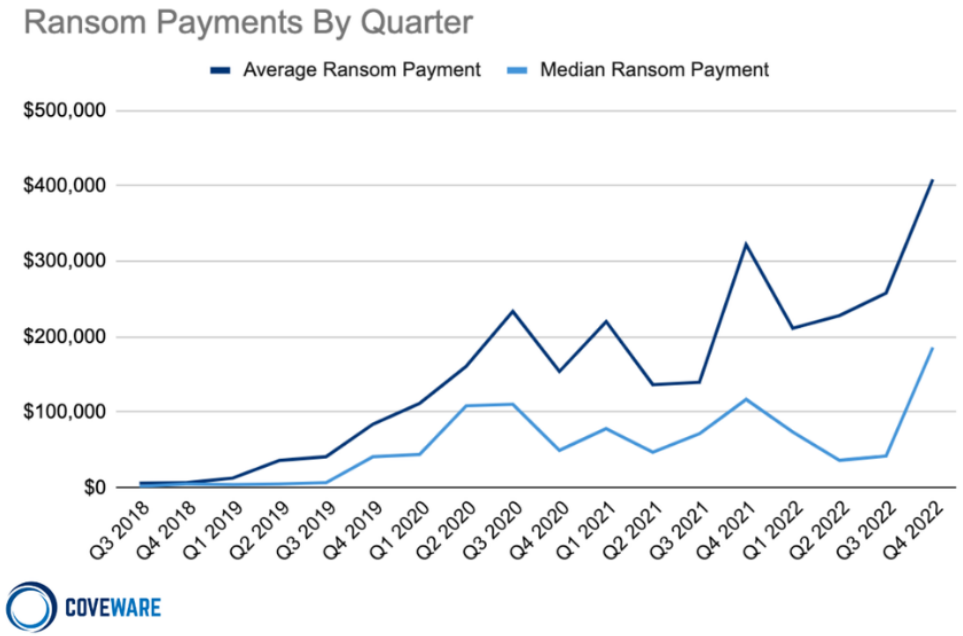
$408,644

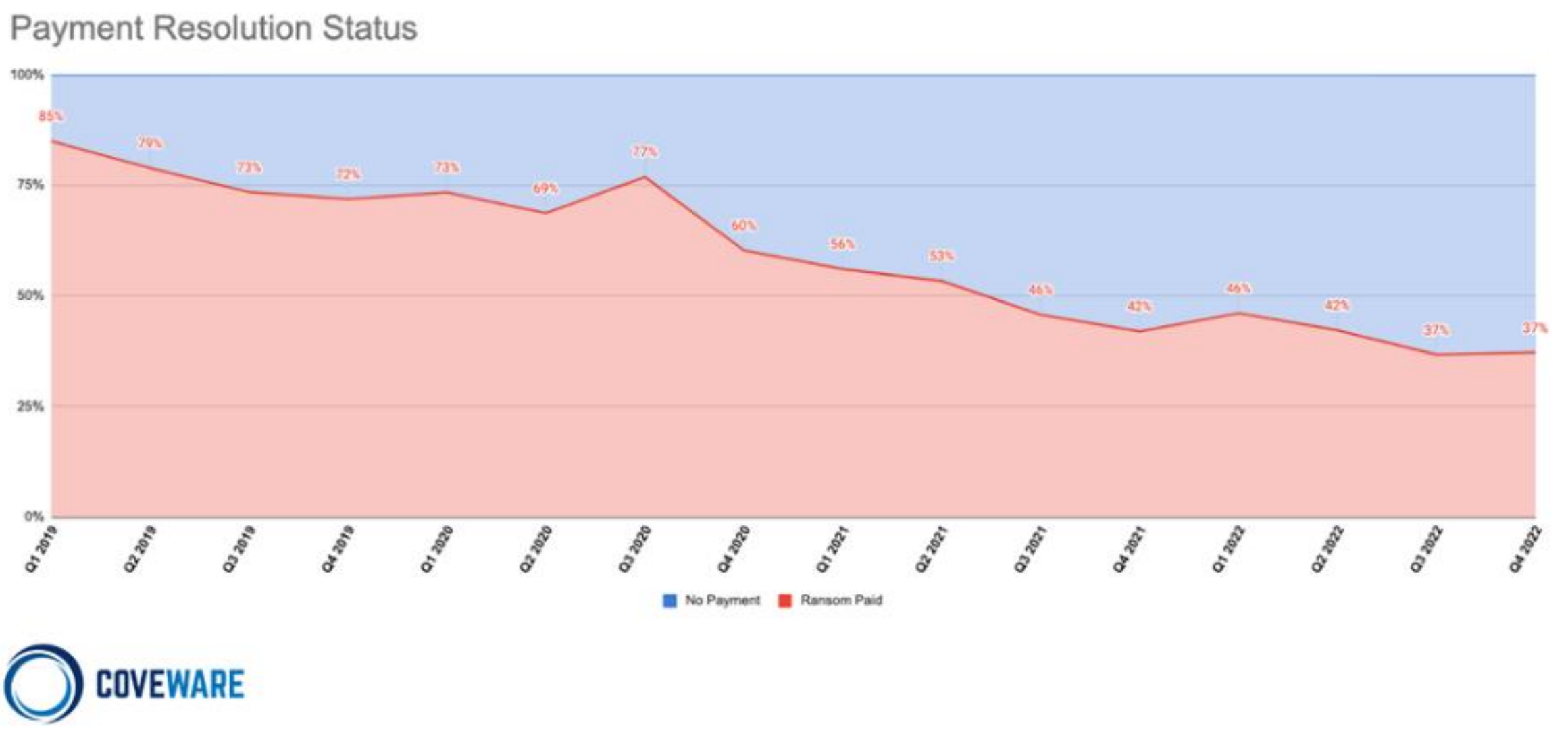
+58% from Q3 2022

Median Ransom Payment

$185,972

+342% from Q3 2022

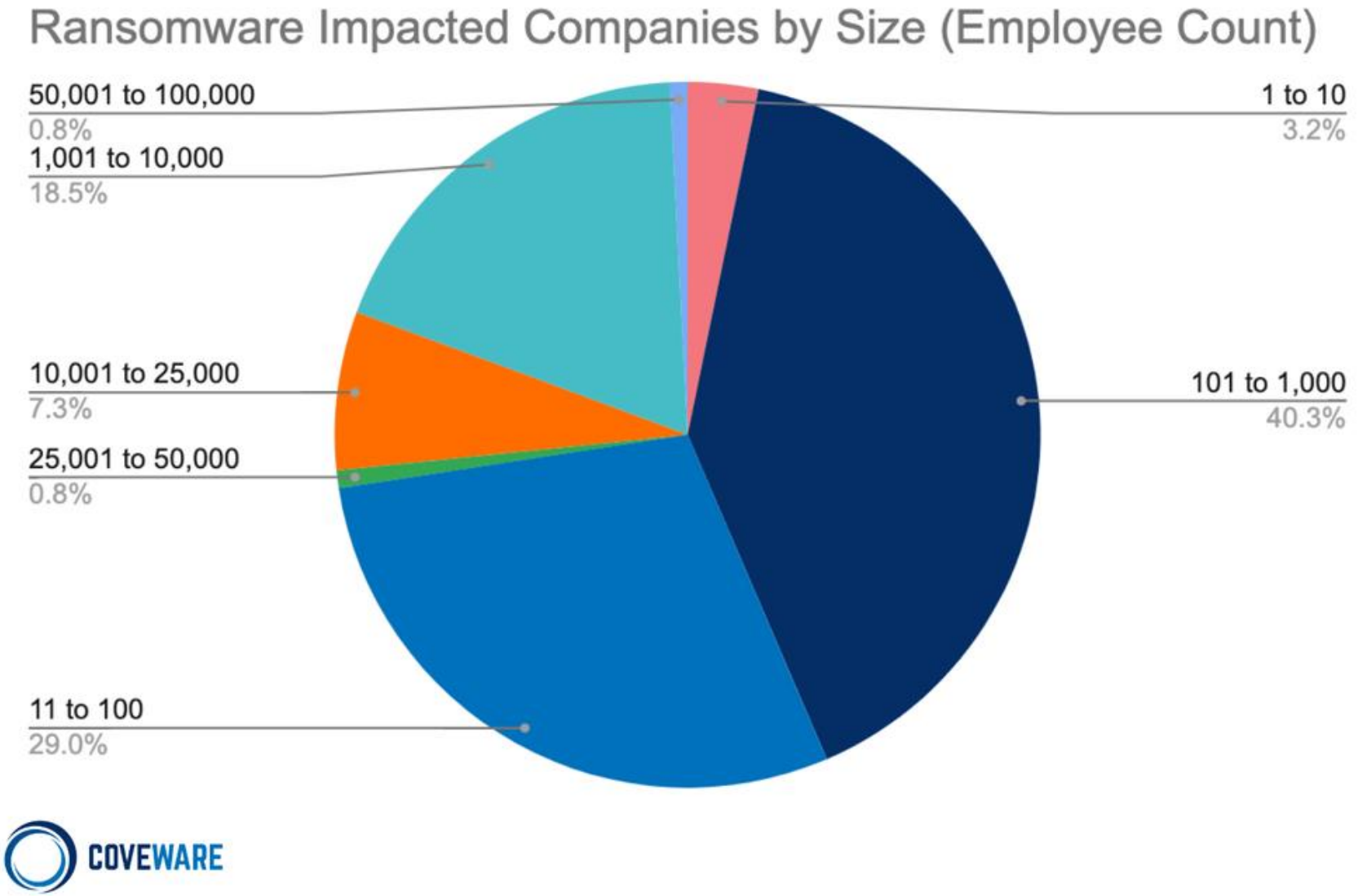




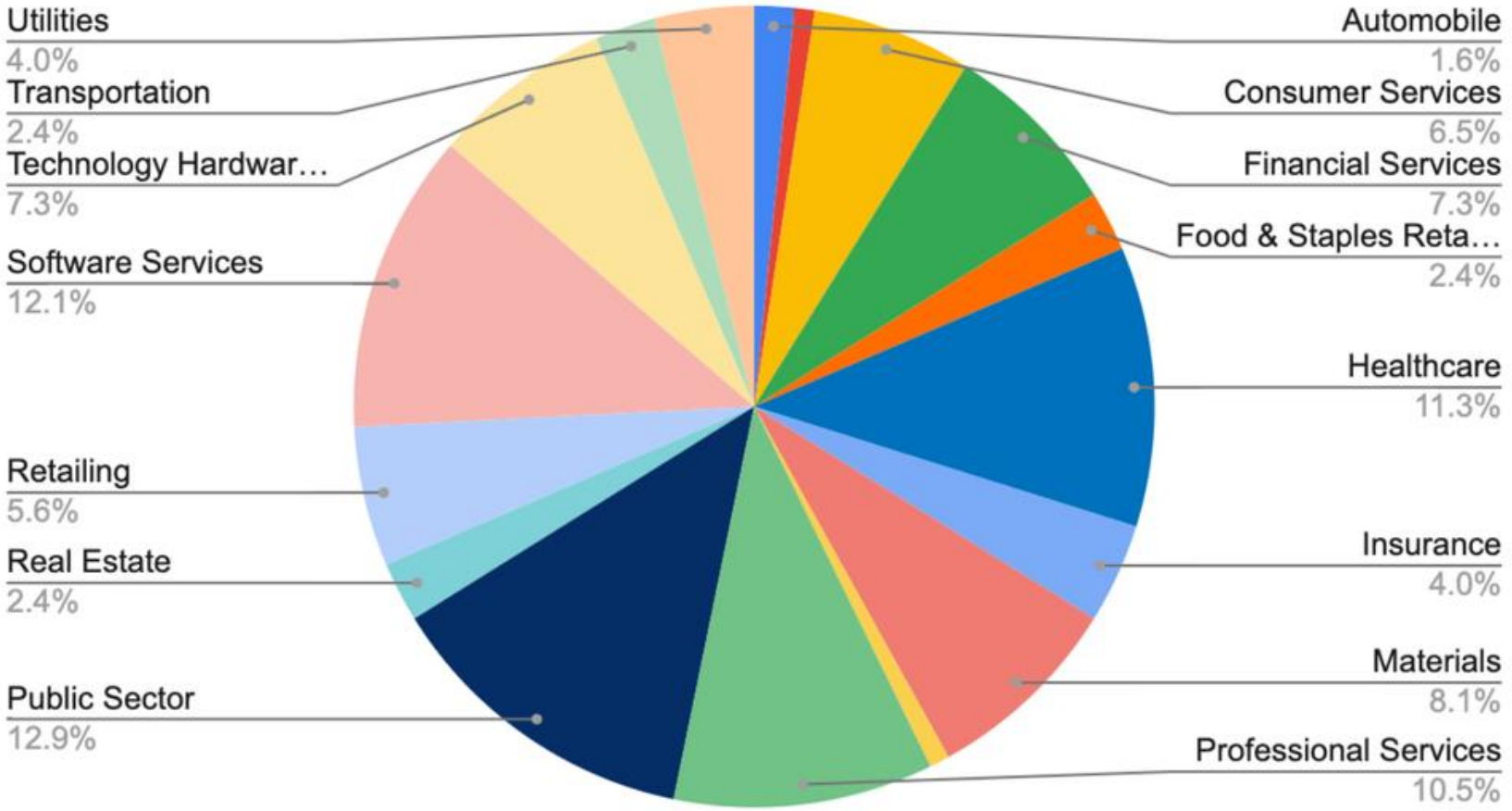
COVEWARE

W ciągu ostatnich 4 lat skłonność ofiar oprogramowania ransomware do zapłacenia okupu dramatycznie spadła, z 85% ofiar w I kwartale 2019 r. do 37% ofiar w IV kwartale 2022 r.

exea


Ransomware Impacted Companies by Size (Employee Count)
50,001 to 100,000
0.8%
1,001 to 10,000
18.5%
10,001 to 25,000
7.3%
25,001 to 50,000
0.8%
11 to 100
29.0%
1 to 10
3.2%
101 to 1,000
40.3%
COVEWARE

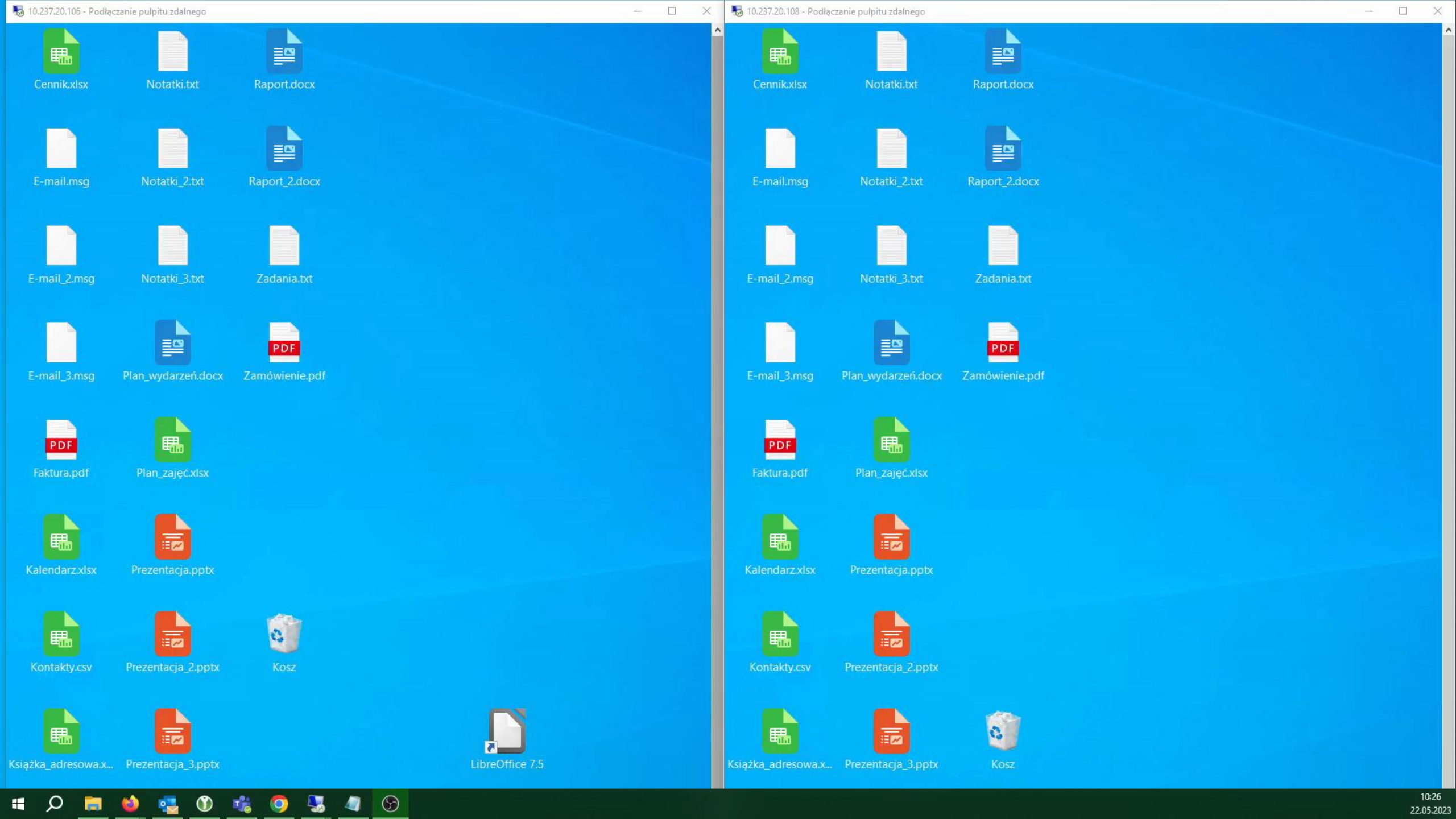
Industries Impacted by Ransomware Q4 2022



COVEWARE

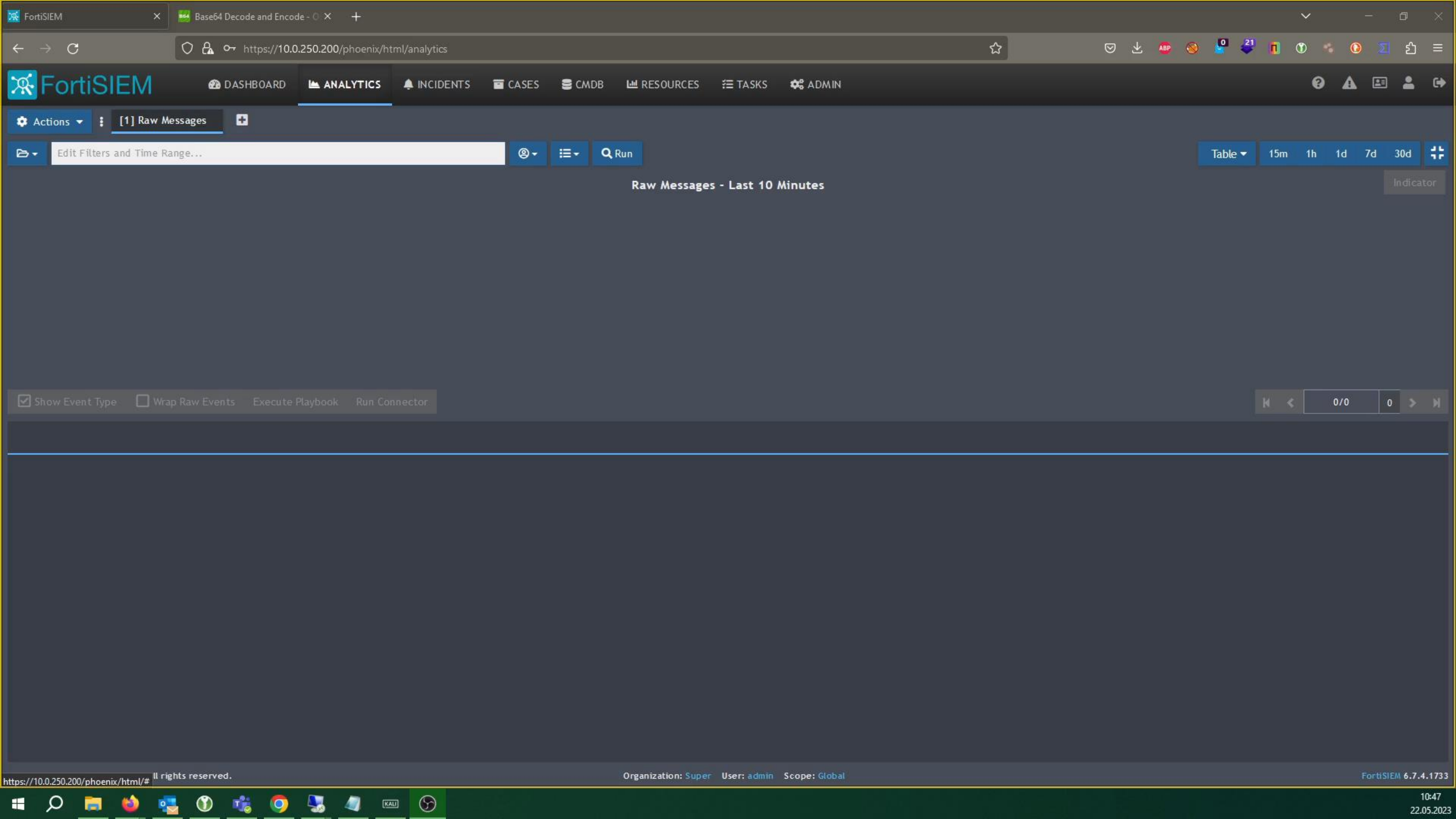
exea®

Ransomware w praktyce - szyfrowanie organizacji.


10.237.20.106 - Podłączanie pulpitu zdalnego
Cennik.xlsx
Notatki.txt
Raport.docx
E-mail.msg
Notatki_2.txt
Raport_2.docx
E-mail_2.msg
Notatki_3.txt
Zadania.txt
E-mail_3.msg
Plan_wydarzeń.docx
Zamówienie.pdf
Faktura.pdf
Plan_zajęć.xlsx
Kalendarz.xlsx
Prezentacja.pptx
Kontakty.csv
Prezentacja_2.pptx
Kosz
Książka_adresowa.x...
Prezentacja_3.pptx
LibreOffice 7.5
10.237.20.108 - Podłączanie pulpitu zdalnego
Cennik.xlsx
Notatki.txt
Raport.docx
E-mail.msg
Notatki_2.txt
Raport_2.docx
E-mail_2.msg
Notatki_3.txt
Zadania.txt
E-mail_3.msg
Plan_wydarzeń.docx
Zamówienie.pdf
Faktura.pdf
Plan_zajęć.xlsx
Kalendarz.xlsx
Prezentacja.pptx
Kontakty.csv
Prezentacja_2.pptx
Książka_adresowa.x...
Prezentacja_3.pptx
Kosz
10:26
22.05.2023

Instrumenty wsparcia dla cyberzagrożeń.

Analiza ataku ransomware.


FortiSIEM
Base64 Decode and Encode -
https://10.0.250.200/phoenix/html/analytics
FortiSIEM
DASHBOARD
ANALYTICS
INCIDENTS
CASES
CMDB
RESOURCES
TASKS
ADMIN
Actions
[1] Raw Messages
Edit Filters and Time Range...
Run
Table
15m
1h
1d
7d
30d
Raw Messages - Last 10 Minutes
Indicator
Show Event Type
Wrap Raw Events
Execute Playbook
Run Connector
0/0
0
ll rights reserved.
Organization: Super
User: admin
Scope: Global
FortiSIEM 6.7.4.1733
https://10.0.250.200/phoenix/html/#
10:47
22.05.2023

Co zrobić, jeśli doszło do zaszyfrowania?

1) **Powiadomienie odpowiednich służb oraz zgłoszenie incydentu.**
2) **Postępowanie zgodnie z przyjętymi procedurami lub jeśli ich brak wykorzystanie sprawdzonych instrukcji:**
   - **CERT_Polska_Poradnik_ransomware.pdf**
   - **GOV - Łagodzenie skutków ataków szkodliwego oprogramowania**
3) **NO MORE RANSOM**