Cybersecurity
Progress. Protected.

Przechytrz cyberprzestępców dzięki jasnym, praktycznym informacjom

Problem

Cyberprzestępcy nie działają tylko oportunistycznie. Są zorganizowani, wytrwali i nieustannie udoskonalają swoje taktyki, tak aby **zmaksymalizować skutki swoich działań i zyski**. Od karteli zajmujących się oprogramowaniem ransomware po grupy kradnące dane – wiele z nich funkcjonuje obecnie jak sprawne, globalne przedsiębiorstwa. Cechują się jasnym podziałem ról, globalnym zasięgiem i zaawansowaniem technicznym. **Przychody z ataków ransomware wciąż rosną**, a wymuszenia stają się coraz bardziej ukierunkowane i agresywne. W tej rzeczywistości zespoły ds. bezpieczeństwa potrzebują czegoś więcej niż tylko prostych wskaźników naruszenia bezpieczeństwa. Potrzebują **dogłębnych, kontekstowych informacji** o tym, jak działają te grupy, czego szukają i jak je powstrzymać, zanim wyrządzą rzeczywiste szkody.

256 DNI

średni czas potrzebny organizacji na pełne odzyskanie sprawności po ataku ransomware

Źródło: Forrester: 2024 Ransomware Breach Benchmarks, By Industry

50%

w ujęciu rok do roku wzrost liczby ataków ransomware (2025)

Źródło: Analizy ESET dotyczące stron ujawniających wycieki danych

O 15% BARDZIEJ NISZCZYCIELSKIE

są ataki ransomware w porównaniu z innymi rodzajami naruszeń

Źródło: Forrester: 2024 Ransomware Benchmarks, By Region

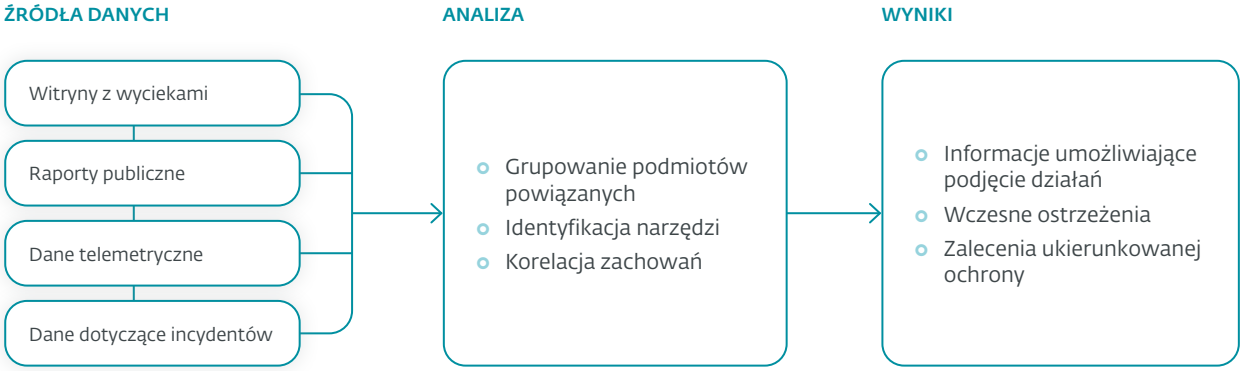
Rozwiązanie

ESET THREAT INTELLIGENCE ECRIME REPORTS

ESET eCrime Reports pozwalają **oddzielić ziarno od plew** dzięki informacjom wywiadowczym **stworzonym z myślą o konkretnych działaniach**. Każdy raport przedstawia jasny obraz **sposobu działania grup cyberprzestępczych** – od wykorzystywanych przez nie narzędzi i infrastruktury po strategie generowania zysków. Otrzymujesz informacje, które pomogą Ci zakłócić ich działalność, a nie tylko wykrywać złośliwe oprogramowanie. Informacje te, wspierane przez globalne zespoły badawcze ESET, opierają się na rzeczywistych danych telemetrycznych, dogłębnej analizie technicznej i bezpośrednim monitorowaniu działalności w podziemiu. To nie tylko dane – to **przewaga strategiczna**.

JAK TO DZIAŁA

Zamiast skupiać się na znanych grupach RaaS i ogólnych przeglądach, analizujemy rzeczywistych przestępców stojących za atakami.



CO WYRÓŻNIA RAPORTY ESET ECRIME

Proaktywna obrona

Zdobądź informacje nie tylko o grupach zajmujących się cyberprzestępczością, ale także o partnerach, którzy faktycznie przeprowadzają ataki. Zobacz, jak działają, i przewiduj ich kolejne ruchy – dzięki temu będziesz o krok przed nimi.

Wydajność operacyjna

Korzystaj z przejrzystych, wyselekcjonowanych informacji opartych na prawdziwych incydentach, aby odciąć się od szumu. Ułatw swojemu zespołowi wykrywanie zagrożeń, szybsze reagowanie i skupianie się na poszukiwaniach tam, gdzie jest to najważniejsze.

Ekskluzywna widoczność

Wyjdź poza publiczne źródła informacji o zagrożeniach, uzyskując głębszy wgląd w taktyki monetyzacji, infrastrukturę i zachowania podmiotów powiązanych w praktyce – wszystko to poparte globalną telemetrią i badaniami firmy ESET.

Co zawierają ESET eCrime Reports?

Rodzaj dostępu	Co zawierają raporty	eCrime Reports	eCrime Reports Advanced
Podsumowanie aktywności CO MIESIĄC	○ Najnowsze kampanie ransomware i infostealerów przedstawione w formie przejrzystych, strategicznych wniosków ○ Kto jest celem ataków, jak przebiegają ataki, co poszło nie tak ○ Kluczowe wnioski, wskaźniki IoC i wytyczne dotyczące wzmocnienia odporności	✓	✓
Analiza techniczna OKRESOWO	○ Dogłębna analiza konkretnych podmiotów stanowiących zagrożenie (np. FIN7) ○ Pełny łańcuch ataku: od początkowego dostępu do kradzieży danych ○ Taktyki atakujących, narzędzia, infrastruktura, mapowanie MITRE ATT&CK®, wskaźniki IOC	✓	✓
Miesięczny przegląd CO MIESIĄC	○ Przegląd najnowszych działań związanych z oprogramowaniem ransomware i infostealerami, gotowy do przedstawienia kadrze kierowniczej ○ Kluczowe trendy, znaczące incydenty, pojawiające się zagrożenia ○ Pomaga kierownictwu ocenić ryzyko i ustalić priorytety bez technicznej złożoności	✓	✓
eCrime feed	○ Najnowsze i wyselekcjonowane wskaźniki IoC dotyczące gangów ransomware, ich podmiotów powiązanych oraz kampanii wykorzystujących programy do kradzieży danych ○ Dostępne w standardowym formacie STIX/TAXII	✓	✓
ESET AI Advisor	○ Wykorzystuje analizy dotyczące cyberprzestępczości do udzielania odpowiedzi na pytania związane z zagrożeniami ○ Pomaga w interpretacji incydentów i zachowań atakujących ○ Zapewnia zespołom i decydentom natychmiastowy dostęp do informacji o zagrożeniach	✗	✓
Dostęp do serwera MISP	○ Bezpośrednia integracja z wyselekcjonowanymi danymi wywiadowczymi dotyczącymi zagrożeń ○ Automatyczne pobieranie wskaźników IOC w celu wzbogacenia mechanizmów obronnych ○ Usprawnia przepływ pracy, przyspiesza wykrywanie i wspiera reagowanie na incydenty	✗	✓