FIREEYE MANDIANT

Kompleksowa diagnoza bezpieczeństwa:

od infrastruktury po kompetencje zespołu

Mandiant Security Assessment

Monika Karpińska
Bartłomiej Sobczyk

Co wyróżnia usługi Mandiant?

FIREEYE ECOSYSTEM

FireEye Mandiant Security Consulting

Chroń, wykrywaj zagrożenia, reaguj na zaawansowane zdarzenia cyber security, chroń krytyczne zasoby Twojego przedsiębiorstwa

77%

Zaufało nam wiele organizacji – **ponad 77%** z listy Fortune 100[1]

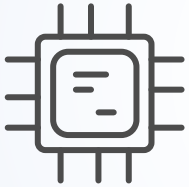
15+

15+ lat doświadczenia w zakresie reakcji i remediacji w najbardziej spektakularnych atakach

Mandiant DNA – Pionierzy w najbardziej zaawansowanym podejściu do Incident Response

Portfolio usług: **assess, transform, train, defend**

Threat Intelligence zasilany informacją z pierwszej linii frontu



Usługi bezpieczeństwa IT wspierane przez **świadomie rozwijaną technologię**

Globalne zasoby to ponad 400 konsultantów w ponad 20 krajach

Zostaliśmy wyróżnieni jako LIDER

- 2019 Forrester Wave: Cybersecurity IR
- 2018 Forrester Wave: External Threat Intel

1: Based on number of Fortune 100 companies who have worked with Mandiant since 2012

Mandiant – portfolio usług

Assess – diagnoza

- Czy byliśmy przedmiotem ataku?
- Czy jesteśmy przygotowani, żeby właściwie zareagować?
- Jak efektywne są nasze zabezpieczenia?

Defend – ochrona

- Usługa detection & response dostarczana przez doświadczonych ekspertów
- Ochrona 24/7
- Wykorzystanie wiodącej technologii i Threat Intelligence

Transform – dojrzałość

Rozwój w kierunku dojrzałej organizacji

- Udoskonalanie procesów
- Usługi w zakresie Remediation & Recommendation

Training – budowa kompetencji Twojego zespołu

- Edukacja w zakresie technolgii FireEye
- Edukacja w zakresie Cyber Security

Assessment – czyli…

Czasami warto powiedzieć „sprawdzam”.
I to zarówno w zakresie naszego środowiska, jak i gotowości ludzi do podjęcia konkretnych działań.
Może warto, aby „sprawdzam” powiedział życzliwy konsultant z ogromnym doświadczeniem,
a nie przedstawiciel grupy cyberprzestępczej?

Portfolio Usług wspieranych wiedzą Threat Intelligence

Assess

Czy byłem przedmiotem ataku?
- Compromise Assessment

Czy jestem przygotowany do reakcji?
- Red Team Assessment
- **Purple Team Assessments**
- **Response Readiness Assessment**
- Tabletop Exercises

Jak efektywny jest mój poziom zabezpieczeń?
- Security Program Assessment
- **Remote Security Assessment**
- **Ransomware Defense Assessment**
- Penetration Testing
- **Cloud Architecture and Security Assessments (Office365, Azure, Amazon Web, Google)**
- Active Directory Security Assessment
- Industrial Controls Healthcheck
- Cyber Insurance Risk Assessment
- Mergers & Acquisitions Risk Assessment
- Embedded Device Assessment

Transform & Train

Rozwój w kierunku dojrzałości
- Cyber Defense Center Development
- Deployment and Integration Services
- Cyber Defense Operations

Szkolenia z najwyższej półki
- Product, Intelligence and Expertise Training
- ThreatSpace Cyber Simulation Exercise

Defend

Usługi Mandiant Managed Defence
- Managed Defense for Endpoint Security
- Managed Defense for Operational Technology (OT)
- Managed Defense Nights & Weekends

Mamy ATAK: Usługi Incident Response

Powiemy o kilku najciekawszych…

Compromise Assessment – opis usługi

O co w tym chodzi?

- Wykrywany i identyfikujemy przeszłe i aktualne włamania, aby odpowiedzieć sobie na pytanie: "Czy byłem/ jestem przedmiotem ataku?"
- Szacunek ryzyka poprzez: identyfikację potencjalnych słabych punktów architektury, istniejących podatności, niewłaściwego użycia, naruszeń polityk i niewłaściwych konfiguracji systemów bezpieczeństwa.
- Zwiększenie odporności organizacji na przyszłe potencjalne ataki, rozwijanie umiejętności właściwego reagowania.

Nasze podejście

- Odpowiednia kombinacja unikalnych technologii – kompleksowa, efektywna i skalowalna diagnoza sytuacji
- Threat Intelligence oraz wiedza i doświadczenie zespołu Mandiant
- Analiza dowodów z sieci, stacji końcowych, logów i wykrytych anomalii w celu potwierdzenia złośliwej aktywności

Wartość

- Identyfikacja krytycznych incydentów bezpieczeństwa
- Uzyskanie atrybucji zidentyfikowanej podejrzanej aktywności
- Identyfikacja luk w zabezpieczeniach oraz obszarów do poprawy w zakresie bezpieczeństwa środowiska

Co nas wyróżnia?

- Dane kontekstowe uzyskane od zespołu Threat Intelligence, technologia FireEye oraz doświadczenie zdobyte podczas setek powłamaniowych analiz śledczych
- Identyfikacja słabości architektury i konfiguracji urządzeń
- Znaczące usprawnienie potencjalnych przyszłych analiz dzięki zdobytej wiedzy

Compromise Assessment w praktyce

Czas trwania usługi

- Średnio 4-6 tygodni
- Czas trwania usługi zależy od wielkości środowiska i szybkości wdrożenia wykorzystywanej technologii
- Usługa dostarczana zdalnie lub on-premise

Co dostajemy na wyjściu? / Deliverables

- Profil zagrożenia dla danego środowiska
- Identyfikację grup atakujących oraz szczegóły przeprowadzonego ataku
- Strategiczne zalecenia w zakresie bezpieczeństwa
- Płynne przejście do usługi IR (Incident Response), jeśli zostanie wykryty bieżący/ trwający atak

Zaangażowanie zasobów

- 2-3 konsuktantów w zakresie IR (Incident Response)

Inne usługi powiązane

- Incident Response Services
- Incident Response Retainer
- Response Readiness Assessment
- Security Program Assessment
- FireEye Endpoint Security
- FireEye Network Security
- FireEye Email Security
- FireEye Managed Defense
- FireEye Threat Intelligence

Purple Team Assessment – opis usługi

O co w tym chodzi?

Ocena zdolności organizacji do przeciwdziałania, wykrywania i reagowania na scenariusze ataków najbardziej odpowiadające danej branży – tak dla infrastruktury w Chmurze, jak i on-prem.

Pełna współpraca Mandiant Purple Team i zespołu bezpieczeństwa nad diagnozą organizacji. Cel to ewaluacja i poprawa możliwości i umiejętności zespołu w zakresie przeciwdziałania, wykrywania i reagowania na realistyczne scenariusze ataków, w każdej ich fazie, podczas pełnego cyklu.

Nasze podejście

- FireEye Threat Intelligence oraz Mandiant Validation – koncentracja na adekwatnych, realistycznych scenariuszach ataków
- Scenariuze ataków zaczerpnięte m.in. z Attack Lifecycle and MITRE AT&CK framework
- Konsultanci "Red Team" i "Incident Responder" pracują z zespołem Klienta na każdym etapie ćwiczenia
- Jeśli zagrożenie nie jest wykrywane, konsultanci pomagają lepiej wykorzystać istniejące narzędzia, zasoby i wiedzę – naprowadzają na trop.

Wartość

- Tabela wyników przed i po ćwiczeniu, prezentująca możliwości w zakresie przeciwdziałania, wykrywania i reagowania na scenariusze ataków
- Krótko- i długoterminowe zalecenia dla organizacji
- Natychmiastowa remediacja podczas realizacji scenariusza – nieoceniona wartość z wykorzystania narzędzia

Co nas wyróżnia?

- Wykorzystanie narzędzia Mandiant Validation w celu zmierzenia efektywności bezpieczeństwa
- Wykorzystanie najnowszych TTPs (Tactics, Techniques and Procedures) zaobserwowanych podczas projektów Incident Response
- Realistyczne podejście do wykrywania i reagowania – doświadczenie
- Udokumentowane strategie skracające czas reakcji i poprawiające efektywność

Purple Team w praktyce

Czas trwania usługi

- 3 tygodnie
- 2 tygodnie testów
- 1 tydzień na przygotowanie raportu

Co dostajemy na wyjściu? / Deliverables

- Szczegółowy raport Purple Team
  - Wysokopoziomowe streszczenie dla Kierownictwa
  - Szczegóły dotyczące testowania każdego scenariusza
  - "Znaleziska" poparte dowodami wraz z zaleceniami w zakresie remediacji
  - Karta wyników wraz z miarami
- Podsumowanie techniczne (opcjonalnie)

Zaangażowanie zasobów

- Dwóch konsultantów – jeden senior Red Teamer i jeden senior w zakresie Incident Response
- Minimum 3 tygodnie koordynatora projektu po stronie klienta
- Kick-off call na tydzień przed rozpoczęciem usługi/ zdefiniowanie listy wymagań
- Wymagania spełnione przed dniem startu usługi

Inne usługi powiązane

- Red Team Assessment
- Tabletop Exercise
- Response Readiness Assessment
- Enterprise Incident Response training course
- Incident Response Retainer

Response Readiness Assessment – opis usługi

O co w tym chodzi?

Ocena i techniczna weryfikacja możliwości w zakresie ochrony przed cyberzagrożeniami dokonana dla sześciu głównych kompetencji w zakresie gotowości na odpowiedź, stanowiąca kombinację:

- przeglądu dokumentacji
- analizy konfiguracji systemów logujących
- zaawansowanych warsztatów
- dedykowanych ćwiczeń
- testów wykrywania i zapobiegania zagrożeniom.

Sześć głównych kompetencji w zakresie Response Readiness

Wartość

Eliminacja niepewności dotyczącej gotowości do podjęcia działań (response readiness) uzyskiwana poprzez ocenę zdolności do zarządzania działaniami w sytuacji zagrożenia atakami najbardziej prawdopodobnymi dla danej organizacji.

Wskazówki zawierające szczegółowe, priorytetyzowane zalecenia oraz roadmapa kreśląca rozwój w zakresie praktycznej i znaczącej poprawy funkcjonowania ochrony przed cyberzagrożeniami.

Co nas wyróżnia?

- Doświadczenie zebrane podczas reagowania na najbardziej zaawanowane i najpoważniejsze ataki na świecie
- Kompleksowa ocena procesu reagowania na zagrożenie (incident response)
- Model warstwowy dla organizacji o różnych wielkościach i unikalnych celach.
- Techniczna weryfikacja wydajności systemów do wykrywania I zapobieganiam.

Response Readiness Assessment – praktycznie

Czas trwania usługi

Faza	Czas
Przegląd dokumentacji	1 tydzień
Warsztaty u Klienta	1 tydzień
Ćwiczenia w zakresie kompetencji, *Poziom II i III*	
Przegląd konfiguracji systemów logujących	0,5 tygodnia
Ćwiczenia, *Poziom II i III*	0,5 tygodnia
Testy wykrywania zagrożenia, *Poziom III*	1 tydzień
Raport i podsumowanie	2 tygodnie

Rezultat

Finalny raport zawierający:

- Ocenę obecnych możliwości obronnych organizacji
- Priorytetyzację zaleceń dla poprawienia wskaźników gotowości do podjęcia działań
- Podsumowanie techniczne
- Roadmapa inicjatyw zalecanych dla poprawy sytuacji *(Poziom II & III)*
- Podsumowanie dla Klierownictwa *(Poziom II & III)*

Zaangażowanie zasobów

Zespół konsultantacyjny (3-4 osoby):

- Project Manager
- 2-3 konsultantów

Zespół IR (Incident Response) po stronie Klienta:

- SOC manager/ analityk
- Managrer zespołu Incident Response
- Lider Threat Intelligence
- Lider Security Engineering

Inne usługi powiązane

- Cyber Defense Transformation Services
- Cyber Defense Operations
- Purple Team Assessment
- Compromise Assessment

Security Assessment for Microsoft Office 365 – opis usługi

O co w tym chodzi?

Proaktywna usługa przeglądu instalacji, identyfikująca powszechne błędy konfiguracyjne, słabe ogniwa procesu i metod eksploatacji, mająca na celu zminimalizowanie ryzyka, optymalizację ochrony i widoczności w ramch instancji O365.

Nasze podejście

Ewaluacja powszechnych dla O365 platform autentykacyjnych i kontroli dostępu w zakresie sześciu głównych obszarów:

Architektura bezpieczeństwa/ hardening	Zarządzanie tożsamością i dostępem
Ochrona danych	Disaster Recovery
Widoczność	Wykrywanie i reagowanie na zagrożenia

Wartość

- Zaadresowanie powszechnych błędów konfiguracyjnych
- Redukcja powierzchni ataków na platformę O365
- Rozszerzony monitoring, widoczność i wykrywalność
- Priorytetyzacja zaleceń w zakresie rozbudowy bezpieczeństwa

Co nas wyróżnia?

- Ogromne doświadczenie zespołu Mandiant w zakresie analiz śledczych włamań na platformę O365
- Koncentracja zarówno na krótkoterminowej kwarantannie, jak i długoterminowej kontroli i właściwej konfiguracji
- Opcjonalna usługa zdalnych testów w celu zdiagnozowania poprawności użycia i zastosowania przygotowanych zaleceń

Security Assessment for Microsoft Office 365 – w praktyce

Czas trwania usługi

- Zasadniczo 4 tygodnie:
  - 0.5 tygodnia – zdalny przegląd dokumentacji
  - 0.5 tygodnia – warsztaty na miejscu u Klienta
  - 2 tygodnie – przegląd konfiguracji
  - Opcjonalnie: 1 tydzień zdalnych testów
  - 1 tydzień – przygotowanie raportu

Rezultat

- Snapshot pokazujący bieżący poziom bezpieczeństwa konfiguracji O365 dla instancji
- Specyficzne najlepsze praktyki dla O365
- Praktyczne zalecenia celem poprawienia widoczności i wykrywalności zagrożeń
- Priorytetyzację zaleceń w zakresie umacniania zabezpieczeń

Zaangażowanie zasobów

- 2 senior konsultantów z zespołu Mandiant
- Po stronie Klienta:
  - Zasoby odpowiedzialne za Azure Active Directory oraz zarządzanie usługą Cloud
  - Zasoby odpowiedzialne za architekturę bezpieczeństwa oraz działania operacyjne
  - Administrator poczty

Inne usługi powiązane

- Incident Response Services
- Incident Response Retainer
- Red Team Assessments
- Penetration Testing
- Compromise Assessment
- Tabletop Exercise

Security Program Assessment – opis usługi

O co w tym chodzi?

Niezależna analiza dojrzałości programu bezpieczeństwa, obejmująca 10 krytycznych domen, zgodna ze standardami danej branży oraz wymogami regulacyjnymi.

Nasze podejście

- Zebranie dokumentacji i jej szczegółowa analiza
- Interaktywne warsztaty i spotkania kadry zarządzającej
- Obserwacje
- Rekomendacje
- Strategie wykonawcze

Wartość

- Minimalizacja ryzyka ataku i kradzieży danych
- Minimalizacja zasięgu i siły rażenia potencjalnego incydentu
- Uzyskanie zgody na poprawę stanu bieżącego
- Priorytetyzacja budżetu i zasobów

Co nas wyróżnia?

- Doświadczenie i wiedza płynące z usług Mandiant Incident Response oraz Threat Intelligence
- Skoncentrowana na ryzykach i praktyczna strategia wykonawcza w zakresie rozwoju dojrzałości programu bezpieczeństwa odpornego na zaawansowane cyberzagrożenia
- Ewaluacja programu bezpieczeństwa, uwzględniająca wielkość organizacji oraz branżę w celu dostarczenia analiz porównawczych, punktów odniesienia oraz danych do karty ryzyk

Security Program Assessment – w praktyce

Czas trwania usługi

- 6 tygodni
- 1 tydzień – Przegląd i analiza dokumentacji
- 2 tygodnie - Warsztaty
- 2 tygodnie – Przygotowanie raportu oraz strategii wykonawczej
- 1 tydzień – sesja QA oraz dostarczenie propozycji raportu

Rezultat

- Zaobserwowane mocne strony i szanse rozwoju
- Rekomendacje strategiczne i taktyczne
- Strategię wykonawczą (zasoby, czas, pieniądze)
- Streszczenie dla Kierownictwa

Zaangażowanie zasobów

- 3 konsultantow
- CISO i zespół bezpieczeństwa informacji, zaangażowana kadra kierownicza oraz po jednym ekspercie z każdej domeny

Inne usługi powiązane

- Penetration Testing
- Red Team Operations
- Threat Diagnostics
- Transformation Services (Design and Build)

FIREEYE MANDIANT

Dziękujemy!