*październik 2019 r.*

**Kolejny krok po MDR to MTR**

**Sophos uruchamia usługę Managed Threat Response**

* Cyberprzestępcy nieustannie rozwijają swoje metody działania, adaptując je do nowych warunków. Teraz coraz częściej stawiają na ataki hybrydowe, co utrudnia skuteczną walkę z niebezpieczeństwami.
* Najnowszy produkt w ofercie lidera rozwiązań dla cyberbezpieczeństwa, Sophos Managed Threat Response (MTR), to w pełni zarządzana usługa, która umożliwia wyszukiwanie, wykrywanie oraz reagowanie na zagrożenia.
* Nową usługę można sprawnie dostosować do oczekiwań każdej organizacji dzięki możliwości dopasowania działań z zakresu oferty oraz trybów reakcji do konkretnych potrzeb danej firmy.

– *Większość dostępnych usług typu MDR ogranicza swoje działanie do powiadamiania o potencjalnych zagrożeniach. Dalsze działania leżą już w gestii klienta* – wyjaśnia **Grzegorz Nocoń, System Engineer Eastern Europe w Sophos**. – *Tymczasem wraz z nową usługą Sophos organizacje nie tylko otrzymują dostęp do znacznie szerszego zakresu informacji, ale również mają możliwość skorzystania z wsparcia dedykowanego zespołu ds. bezpieczeństwa, dostępnego przez całą dobę, siedem dni w tygodniu. Wszystko zgodnie z ich potrzebami oraz preferencjami.*

[Sophos](https://www.sophos.com/en-us.aspx), światowy lider w zakresie [bezpieczeństwa sieci i urządzeń końcowych](https://www.sophos.com/en-us/security-news-trends/reports/gartner.aspx), ogłosił udostępnienie Sophos Managed Threat Response (MTR) – w pełni zarządzanej usługi, która umożliwia wyszukiwanie, wykrywanie i reagowanie na zagrożenia. Nawet w przypadku najbardziej wyrafinowanych i złożonych problemów, ich neutralizację wspomoże dedykowany zespół ds. bezpieczeństwa, dostępny przez całą dobę – siedem dni w tygodniu.

– *Cyberprzestępcy nieustannie rozwijają swoje metody działania, adaptując je do nowych warunków. Teraz coraz częściej stawiają na ataki hybrydowe – połączenie automatyzacji z pomysłowością człowieka. Taka kreatywność utrudnia wykrywanie zagrożeń i ich późniejszą neutralizację. A gdy tylko hackerom uda się przejąć dostęp do danej struktury informatycznej, natychmiast zaczną wykorzystywać takie techniki jak „living off the land”, aby trudniej było usunąć niebezpieczeństwo z infrastruktury informatycznej* – mówi **Grzegorz Nocoń.**

Inne rodzaje zagrożeń to m.in. „fileless attacks” – zespół działań wykorzystujących już zainstalowane na komputerze oprogramowanie. Równie popularne jest wykorzystywanie narzędzi administratorskich takich jak PowerShell do niepożądanego poszerzania uprawnień, nieautoryzowanego kopiowania danych czy dalszego atakowania danego serwera. Szerzej o tym piszą autorzy bloga [SophosLabs Uncut](https://news.sophos.com/en-us/2019/10/01/lemon_duck-powershell-malware-cryptojacks-enterprise-networks/). Takie zagrożenia trudno wykryć z uwagi na to, że atakujący nie wprowadzają na serwer plików o podejrzanym kodzie – wręcz przeciwnie, korzystają z narzędzi wykorzystywanych przez nas na co dzień.

Sophos MTR, skonstruowany w oparciu o [Intercept X Advanced z dodatkiem EDR](https://www.sophos.com/en-us/products/intercept-x.aspx), łączy uczenie maszynowe z ekspercką analizą, aby lepiej wyszukiwać i wykrywać zagrożenia, dokładniej badać ostrzeżenia o zagrożeniach i przeprowadzać działania w celu eliminacji zagrożenia. Akwizycje technologii [Rook Security](https://www.sophos.com/en-us/press-office/press-releases/2019/06/sophos-acquires-rook-security.aspx) oraz [DarkBytes](https://www.sophos.com/en-us/press-office/press-releases/2019/01/sophos-acquires-darkbytes-as-foundation-of-new-mdr-services.aspx) umożliwiły wdrożenie innowacyjnych możliwości, takich jak:

* **Wyszukiwanie zagrożeń przez ekspertów.** Sophos MTR przewiduje potencjalne zachowania atakującego oraz identyfikuje cechy charakterystyczne ataku. Eksperci Sophos proaktywnie wyszukują i sprawdzają potencjalne zagrożenia. Badając incydenty, które wystąpiły na mniejszą skalę, odkrywają nowe, wcześniej niedostrzegalne luki w zabezpieczeniach systemów.
* **Zaawansowane wykrywanie nieautoryzowanej obecności.** Sophos MTR wykorzystuje sprawdzone techniki badawcze w celu odróżnienia działań rzeczywistych użytkowników od taktyk, technik i procedur (TTP) zazwyczaj wykorzystywanych przez atakujących. W połączeniu z ulepszoną telemetrią od [Sophos Central](https://www.sophos.com/en-us/products/sophos-central.aspx), która w ramach usługi zapewnia wgląd w pełen obraz działań przeciwnika, możliwe jest szybkie określenie skali oraz powagi danego zagrożenia – za czym idzie możliwość podjęcia decyzji o sposobie reakcji.
* **Szybka reakcja na zagrożenia dzięki ludzkim umysłom oraz automatyzacji maszyn.** Wyszkolony zespół światowej klasy ekspertów zbiera i wykorzystuje wiedzę z zakresu cyberbezpieczeństwa oraz istniejących zagrożeń, aby potwierdzić, z jakiego rodzaju atakiem mają do czynienia ­– a następnie podejmuje działania, aby sprawnie i precyzyjnie zneutralizować zagrożenie.
* **Odkrywanie możliwości infrastruktury i wskazówki z zakresu bezpieczeństwa**. Dzięki stałej czujności i nieustannemu audytowi zasobów, Sophos MTR umożliwia uzyskanie cennych informacji o zasobach w danej organizacji oraz potencjalnych problemach. To oznacza także możliwość lepszego oszacowania wpływu danego zagrożenia na infrastrukturę informatyczną organizacji oraz ich skuteczniejsze wykrywanie. Wytyczne i praktyczne porady udzielane przez zespół ekspertów umożliwiają zaadresowanie słabości w infrastrukturze informatycznej lub jej konfiguracji. W ten sposób organizacje mogą sprawnie i proaktywnie poprawiać swój poziom bezpieczeństwa.

Sophos MTR jest już dostępny u [zarejestrowanych partnerów Sophos](https://www.sophos.com/en-us/partners.aspx) na całym świecie. Nową usługę można sprawnie dostosować do oczekiwań każdej organizacji dzięki możliwości dopasowania działań z zakresu oferty oraz trybów reakcji do konkretnych potrzeb oraz preferencji danej firmy.

**Co mówią nasi partnerzy oraz branżowi analitycy:**

Przedsiębiorstwa muszą codziennie walczyć z wyrafinowanymi atakami ze wszystkich stron. W takiej sytuacji absolutnie niezbędna jest nie tylko możliwość szybkiego wykrywania zagrożeń, ale również sprawnego reagowania. Wielu dostawców twierdzi, że oferuje takie możliwości, ale niewielu z nich rzeczywiście podejmuje działania konieczne do eliminacji zagrożeń w ramach oferowanych usług z zakresu MDR. Tymczasem Sophos MTR łączy wysoko oceniany EDR ze specjalistyczną ekspertyzą i niezwykłą skarbnicą wiedzy o zagrożeniach pozyskiwanej w ramach [SophosLabs](https://www.sophos.com/en-us/labs.aspx), aby stworzyć zupełnie nową ofertę odpowiadającą na rosnące potrzeby rynku.

Aaron Sherrill, starszy analityk ds. bezpieczeństwa informacji w 451 Research

Jedynym sposobem na ochronę przed dzisiejszymi zaawansowanymi zagrożeniami jest połączenie najlepszych narzędzi z najświetniejszymi ludzkimi umysłami. Sophos Managed Threat Response zupełnie zmienia zasady gry, łącząc uczenie maszynowe z ekspercką analizą – w ten sposób oferuje nowe proaktywne podejście do cyberbezpieczeństwa. Spersonalizowana oferta wspiera nasze możliwości w zakresie wykrywania zagrożeń i pomaga w zaoferowaniu naszym klientom lepszej ochrony.

Jeremy Weiss, lider ds. cyberbezpieczeństwa w [CDW](https://www.cdw.com/)

Cyberprzestępcy nigdy nie śpią – zawsze działają. To oznacza, że organizacje potrzebują całodobowej ochrony. Dzięki Sophos Managed Threat Response klienci Total Tech mają poczucie, że sytuacja jest cały czas pod kontrolą – nawet podczas drugiej czy trzeciej zmiany. Eksperckie wskazówki to kolejna niesamowita zaleta tej oferty – dzięki nim możemy natychmiast podejmować działania w celu wzmocnienia naszych struktur informatycznych.

Ken Hamilton, prezes/CEO [Total Tech International Inc](https://us-west-2.protection.sophos.com/?d=1totaltech.com&u=aHR0cHM6Ly93d3cuMXRvdGFsdGVjaC5jb20v&e=a2hhbWlsdG9uQDF0b3RhbHRlY2guY29t&h=84c12791874d4ffc8378affacc6d3714&t=VTZ1c25nYjVxWm5nN05jd1VaL0tiQVRpMGFtMTMxNHhDa3VqaXdrT1dLWT0=).

**O Sophos:**

Sophos jest liderem rozwiązań bezpieczeństwa IT nowej generacji z szerokim portfolio produktów do kompleksowej ochrony urządzeń końcowych, sieci, poczty i urządzeń mobilnych oraz narzędzi do szyfrowania. Producent oferuje unikalną koncepcję Synchronized Security, czyli pełną integrację i komunikację między poszczególnymi produktami.

Ponad 100 milionów klientów w ponad 150 krajach zaufało rozwiązaniom Sophos i wskazuje je jako najlepsze do ochrony przed złożonymi zagrożeniami i utratą danych. Produkty Sophos są dostępne za pośrednictwem globalnego kanału dystrybucji obejmującego 26 tysięcy partnerów. Sophos, z siedzibą w Oxford w Wielkiej Brytanii, jest notowany na Londyńskiej Giełdzie Papierów Wartościowych pod symbolem „SOPH”. Więcej informacji na [www.sophos.com](http://www.sophos.com).