DECEPTIVE RESPONSE

Rozwiązanie TEHTRIS Deceptive Response wdraża do chronionej sieci specjalistyczne pułapki na cyberprzestępców, tzw. honeypoty, pozwalające na analizowanie niebezpiecznej aktywności

PRZYKŁADY ZASTOSOWANIA

- Wykrywanie incydentów
- Polowanie na zagrożenia
- Prace w zakresie kryminalistyki cyfrowej
- Zmniejszanie powierzchni ataku

NAJWAŻNIEJSZE KORZYŚCI

- Szybsze wykrywanie zagrożeń
- Szybsze reagowanie
- Integracja z rozwiązaniem TEHTRIS XDR Platform
- Zdalne i scentralizowane zarządzanie (SaaS)
- Łatwe wdrożenie i użytkowanie

Rozwiązanie **TEHTRIS Deceptive Response oferuje efektywny system alarmowy działający w czasie rzeczywistym i pozwalający pozostawać o krok przed cyberprzestępcami**. Dodając sfałszowane zasoby do swojej sieci możesz wabić atakujących i szczegółowo analizować ich poczynania przy użyciu raportów i paneli prezentujących szczegóły dotyczące zdarzeń.

W przeciwieństwie do produktów, które muszą analizować ogromne ilości danych, co jest obarczone ryzykiem generowania fałszywych alarmów, TEHTRIS Deceptive Response **pozwala skupić się wyłącznie na maszynach i usługach, które faktycznie są atakowane przez cyberprzestępców**.

Cyberprzestępca, który chce zaatakować sieć chronioną przy użyciu rozwiązania TEHTRIS Deceptive Response, może **napotkać na fałszywe maszyny (pułapki), co natychmiast wygeneruje alarm**. Atakujący nie ma zatem czasu na popełnianie błędów, a jego ruchy poprzeczne, mające na celu rekonesans w sieci ofiary, są znacznie utrudnione.

TEHTRIS Deceptive Response wdraża flotę honeypotów, które są **w pełni zintegrowane z rozwiązaniem TEHTRIS XDR Platform**, uzupełniając pozostałe technologie bezpieczeństwa, takie jak SOAR, ekspercka wiedza o cyberzagrożeniach, polowanie na nowe zagrożenia, kontrola zgodności czy zarządzanie incydentami.

Istnieje wiele rodzajów honeypotów, jednak niektóre z nich nie są efektywne, ponieważ cyberprzestępcy zdążyli już dobrze je poznać. Wdrożenie rozwiązania TEHTRIS Deceptive Response jest warte rozważenia z kilku powodów. Po pierwsze, **atakujący będą marnowali czas na atakowanie wabików, zamiast celować w prawdziwe maszyny**, co da Ci możliwość lepszego przygotowania się na kolejne fazy ataku. Co więcej, będziesz mógł **wykryć działania cyberprzestępców już we wczesnej fazie**, podczas której atakujący zajmują się mapowaniem Twojej sieci. Wreszcie, będziesz miał możliwość zrozumienia schematów działania cyberprzestępców, by lepiej zabezpieczyć swoją infrastrukturę.

Autoryzowany partner

itxon systemy informatyczne

Systemy Informatyczne ITXON Sp. z o.o.
ul. Garncarska 34, 42-200 Częstochowa
(34) 399 25 00 / info@itxon.pl / www.itxon.pl

DECEPTIVE RESPONSE

Skuteczne rozwiązanie zaradcze wykorzystujące honeypoty

KLUCZOWE FUNKCJE

- Fałszywe systemy operacyjne
- Fałszywe usługi
- Rozszerzone dzienniki zdarzeń
- Dane historyczne i polowanie na zagrożenia
- Wdrożenie lokalne oraz w chmurze

OBSŁUGIWANE PLATFORMY

- Chmura
- Trunk 801.1Q
- Ethernet
- TCP/IP
- VMware ESXi
- OT (SCADA/ICS)

FUNKCJE

Honeypoty symulują fałszywe usługi, co pozwala wykrywać nawet śladowe symptomy cyberataków.

Ułatwiona analiza danych z dzienników zdarzeń.

Filmy przedstawiające polecenia wpisywane przez atakujących w wierszu poleceń.

Łatwy proces wdrożenia maszyny wirtualnej TEHTRIS Deceptive Response na sprzęcie funkcjonującym w Twojej infrastrukturze (hipernadzorca VMware ESXi).

Łączność internetowa maszyny wirtualnej TEHTRIS Deceptive Response z rozwiązaniem TEHTRIS XDR Platform (monitorowanie śladów włamania oraz zarządzanie w modelu SaaS).

Możliwość wdrożenia honeypotów **we wszystkich sieciach VLAN**.

Integracja z wewnętrznymi i zewnętrznymi sieciami (dostępnymi z internetu).

Autoryzowany partner

itxon
systemy informatyczne

Systemy Informatyczne ITXON Sp. z o.o.
ul. Garncarska 34, 42-200 Częstochowa
(34) 399 25 00 / info@itxon.pl / www.itxon.pl