POWSTRZYMAJ CYBERATAKI Z THYCOTIC

ZABEZPIECZAJĄC HASŁA, CHRONIĄC URZĄDZENIA KOŃCOWE ORAZ KONTROLUJĄC DOSTĘP DO APLIKACJI

TWÓJ CEL? BEZPIECZEŃSTWO!

Najczęstszymi celami ataków hakerów są hasła do kont uprzywilejowanych, dane logowania do kont administratorów domen, konta root oraz konta super-użytkowników. Wykorzystując podatności na styku urządzeń końcowych i użytkowników, hakerzy szukają możliwości pozyskania i eskalacji uprawnień. Wszystko po to, aby jako zaufany użytkownik uzyskać dostęp do najbardziej wrażliwych i krytycznych danych. Takie działanie jest często nie do wykrycia przez wiele miesięcy. Endpoint Privileged Acces pozwala na rozwiązanie tego problemu, obejmując ochroną dane logowania wszystkich uprzywilejowanych użytkowników w całym przedsiębiorstwie.

PAMIETAJ CZYM RYZYKUJESZ!

Uprzywilejowane poświadczenia
Pełen wgląd

Bardzo często administratorzy IT wykorzystują domyślne nazwy i hasła nie zmieniając ich każdorazowo, tak jak powinno to mieć miejsce. Co gorsza – arkusze kalkulacyjne wykorzystywane do przechowywania danych logowania kont uprzywilejowanych są bardzo zawodne i podatne na błędy oraz ataki. Rezultat? Możliwość uzyskania pełnego wglądu w uprzywilejowane poświadczenia!

Uprzywilejowane poświadczenia
Przyjmowanie

Kontrolowanie uprzywilejowanych poświadczeń w codziennej praktyce może stać się bardzo kłopotliwe lub czasochłonne. Z czasem kontrola poświadczeń ewoluuje w ich przejmowanie. W rezultacie administratorzy o niskim poziomie uprawnień, a nawet użytkownicy biznesowi, uzyskują niebezpiecznie wysokie uprawnienia, co jest zagrożeniem dla całego przedsiębiorstwa.

Uprzywilejowane poświadczenia
Dzielenie się

Wiele działów IT wciąż dzieli się między sobą, takimi samymi uprzywilejowanymi kontami z dostępem do root'a, kontami super-użytkowników czy kontami serwisowymi, lekceważąc zasady bezpieczeństwa wymagające od pracowników rotacji haseł i stosowania wieloskładnikowego uwierzytelniania.

Urządzenia końcowe
Luki

Urządzenia końcowe bardzo często stanowią cel ataków, na które narażona jest sieć. Kontrolowanie aplikacji działających w sieci znacznie zmniejsza ryzyko przeniknięcia do sieci zagrożeń, jakim jest np. ransomware.

Konta uprzywilejowane i uprawnienia administracyjne są bardzo często nieznane, źle zarządzane, niekontrolowane i niezabezpieczane, co naraża organizację na katastrofalne skutki.

thycotic

DC | LONDON | SYDNEY

e: sales@thycotic.com
t: @thycotic
www.thycotic.com

NASZE ROZWIĄZANIE

Jako światowy lider rozwiązań bezpieczeństwa IT nowej generacji Thycotic zapobiega cyberatakom poprzez zabezpieczanie haseł, ochronę urządzeń końcowych i kontrolę dostępu.

Thycotic to kompleksowe rozwiązanie w zakresie bezpieczeństwa, które:

- łączy w sobie najwyższej jakości ochronę kont uprzywilejowanych i haseł ze skutecznym zabezpieczaniem urządzeń końcowych i kontrolą aplikacji Windows i Unix
- znacznie obniża ryzyko ataków opartych o malware, które wycelowane są w urządzenia końcowe i serwery ograniczając możliwość przejścia hakera poza początkowy punkt wejścia oraz zapobiegając instalacji narzędzi do zdalnego dostępu (RAT)
- zapewnia ochronę danych logowania do kont uprzywilejowanych, zapobiegając jednocześnie eskalacji uprawnień poprzez usunięcie lub ograniczenie uprawnień użytkowników biznesowych i administratorów IT, bez wpływu na ich wydajność

Thycotic Secret Server to kompleksowe rozwiązanie z zakresu bezpieczeństwa, pozwalające skutecznie chronić najcenniejsze dane przed cyberatakami, jak i zagrożeniami wewnętrznymi. Rozwiązania Thycotic Secret Server, Privelege Manager, Local Security i Security Analysis chronią uprzywilejowane konta i umożliwiają organizacjom egzekwowanie polityk bezpieczeństwa, zarówno od użytkowników biznesowych, jak i administratorów, a także kontrolują aplikacje, aby zminimalizować zakres ewentualnego ataku bez wpływu na działanie firmy.

Rozwiązanie to pomaga unieważnić dotychczasowe nieprawidłowo przypisane uprawnienia administracyjne zwykłych użytkowników, jednocześnie bezproblemowo podnosząc uprawnienia odpowiednim użytkownikom, gdy wymagają tego zaufane aplikacje.

Uzupełniając braki w kontroli uprawnień, rozwiązanie Thycotic zapewnia również kontrole aplikacji. Sprawdza, które z nich mogą być uruchamiane na końcówkach i serwerach, przez co zapobiega przedostawaniu się złośliwego oprogramowania do sieci wewnętrznej.

W odróżnieniu od innych rozwiązań bezpieczeństwa klasy enterprise, produkty Thycotic są szybkie we wdrożeniu, proste w obsłudze, łatwo się skalują, a ponadto posiadają bardzo atrakcyjną cenię. Znajdź potwierdzenie u jednej z ponad 7500 firm na całym świecie, w tym przedsiębiorstw z listy Fortune 500, które skorzystały z technologii Thycotic!

AWARDS & RECOGNITIONS

Deloitte. Technology Fast 500

CIO Review 20 MOST PROMISING ENTERPRISE SECURITY COMPANIES

Inc. 500

THE GOLDEN BRIDGE AWARDS BEST WORLDWIDE

SCawards

BEST OF vmworld

e: sales@thycotic.com
t: @thycotic
www.thycotic.com

Nasi administratorzy IT byli gotowi zacząć pracę na produktach Thycotic w kilka minut, zaś sam poziom ochrony nad kontami uprzywilejowanymi natychmiast się poprawił. Dzięki Secret Server, który pomaga nam zarządzać poufnymi danymi logowania do uprzywilejowanych kont, staliśmy się bardziej efektywni i znacznie zmniejszyliśmy ryzyko wystąpienia zagrożeń bezpieczeństwa, które mogą dotyczyć tak dużych firm, jak nasza.

Michael Boeglin,

Dyrektor Infrastrukury Globalnej – International Rescue Committee

NASZE INNOWACYJNE PRODUKTY

OCHRONA HASEŁ

Secret Server

Dostępny jako licencja lokalna w chmurze oraz w wersji darmowej. Tworzy podstawową warstwę zabezpieczeń zarządzaną z poziomu administratora, aby ochronić przed cyberatakami, które uderzają w konta uprzywilejowane, czyli rdzeń całego przedsiębiorstwa.

Privileged Behavior Analytics

Privileged Behavior Analytics pomaga administratorom IT i oficerom bezpieczeństwa szybko wykrywać naruszenia ochrony, zanim wywołają one szkodliwe efekty, analizować dystrybucję uprzywilejowanych kont i dostępów do nich w całej organizacji oraz dodają warstwę bezpieczeństwa do rozwiązania Secret Server.

Password Reset Server

To proste, samoobsługowe zarządzanie hasłami, które odciąży Twój dział IT od czasochłonnych i nieefektywnych procesów oraz wymusi wzmocnienie kontroli haseł użytkowników końcowych.

OCHRONA KOŃCÓWEK I KONTROLA DOSTĘPU

Privilege Manager

Privilege Manager to zaawansowane rozwiązanie do zarządzania aplikacjami łączące w sobie zarządzanie przywilejami, białą listę aplikacji oraz działającą w czasie rzeczywistym inteligencję dla końcówek Windows i Mac.

Group Management Server

Pozwala wybranym pracownikom spoza działu IT, na bezpieczne zarządzanie grupami Active Directory, bez konieczności przypisywania im kont uprzywilejowanych.

Security Analysis Solution for Windows

Identyfikuje błędy konfiguracji zabezpieczeń za pomocą protokołu SCAP (Security Content Automation Protocol) a następnie automatycznie je koryguje.

Unix Protection

Umożliwia administratorom Secret Server korzystanie z dwóch dodatkowych funkcji: białej listy unixowych komend oraz zarządzanie kluczami SSH. Biała lista poleceń zapewnia ograniczenie uprawnień administratorów tylko do podzbioru poleceń SSH, podczas uruchamiania sesji za pośrednictwem Secret Server. Zarządzanie kluczami SSH może zabezpieczyć i rotować prywatne lub publiczne pary kluczy SSH, aktualizując jednocześnie klucze publiczne na końcówkach, gdy zajdzie taka potrzeba.

Najważniejsze cechy rozwiązań Thycotic:

Proste bezpieczeństwo
Łączy wielowarstwowe zasady zabezpieczeń z łatwym zarządzaniem dostępami dla administratorów IT, silnym podziałem zadań w oparciu o role oraz 256-bitowe szyfrowanie klasy militarnej.

Ochrona wydajności
Umożliwia bezproblemowe zwiększenie uprawnień użytkowników dla zatwierdzonych aplikacji, minimalizując ryzyko uruchomienia aplikacji nieautoryzowanych.

Egzekwowanie punktów końcowych
Automatyczne egzekwowanie polityk, w celu odpowiedniego przypisania uprawnień dla użytkowników biznesowych i administratorów, które nadawane są zgodnie z zasadą najmniejszych przywilejów.

Szybkość i prostota
Oprogramowanie instaluje się w ciągu kliku minut, jest łatwe w użyciu i elastyczne, dzięki czemu można wykonywać działania przy minimalnym nakładzie pracy.

Wysoka skalowalność
Obsługuje różnie środowiska niezależnie od ich rozproszenia, wszystkie najważniejsze systemy operacyjne, bazy danych, aplikacje, hiperwizory, urządzenia sieciowe i brzegowe, działając zarówno lokalnie, jak i w chmurze.

Stały dostęp
Zapewnia opcję wysokiej dostępności (HA), odzyskiwania danych po awarii (DR), tworzenia gorącej kopii zapasowej i kopii lustrzanych baz danych oraz wyjątkowy, nielimitowany tryb administracyjny - w przypadku rzeczywistej awarii.

Prosta konfiguracja
Z łatwością może być dopasowany do potrzeb użytkownika, bez konieczności marnowania czasu i pieniędzy na dodatkowych kosztownych konsultantów.

Razem z audytem
Gotowe, zaawansowane szablony raportów bezpieczeństwa zgodne z obowiązującymi regulacjami dostępne są przy minimalnym wkładzie pacy.

Odkryj

- automatyczną identyfikację i bezpieczne przechowywanie kont uprzywilejowanych!
- opcję wykrywania użytkowników posiadających nieprawidłowo przypisane prawa administracyjne!
- funkcję wyszukiwania błędnych konfiguracji zabezpieczeń!
- możliwość wykrywania wszystkich uprzywilejowanych kont i przechowuj hasła w bezpieczny sposób!
- Zrób to wszystko w ciągu kilku minut, zamiast tracić niezliczone godziny pracy!

Zarządzaj

- kontroluj i analizuj aktywności uprzywilejowanych kont i użytkowników!
- audytuj i raportuj zgodnie ze standardami!
- automatycznie rotując hasłami i chroniąc dostęp do krytycznych systemów!
- automatycznym ostrzeganiem członków swojego zespołu w przypadku nietypowego wykorzystania danych do logowania!
- Uzyskaj zgodność ze standardami bezpieczeństwa dla pełnego spektrum użytkowników!

Monitoruj, kontroluj

- monitoruj, nagrywaj, zbieraj, i zarządzaj aktywnością kont uprzywilejowanych!.
- elastycznie twórz białą i czarną listę!
- kontroluj eskalacje uprawnień dla aplikacji na końcówkach, wycofując lub ograniczając przywileje dla administratorów IT i użytkowników biznesowych!
- ograniczaj uprawnienia dla użytkowników biznesowych i IT, aby zatrzymać złośliwe oprogramowanie na końcówkach!
- dowiedz się, jak są używane Twoje konta uprzywilejowane i powstrzymaj nadużycia!
- zapewnij pełen obraz swojemu SOC, dzięki integracji z SIEM w zakresie wykorzystania kont uprzywilejowanych!

Zabezpieczaj, chroń

- zapobiegaj i wykrywaj nieautoryzowane użycia uprzywilejowanych kont, usuwaj je lub ograniczaj eskalację uprawnień!
- zablokuj punkty końcowe poprzez ograniczenie ryzyka uruchomienia przez nieuprawnionych użytkowników!
- zabezpiecz konta uprzywilejowane oraz użytkowników biznesowych i administratorów przed hakerami i złośliwym oprogramowaniem!
- konta administracyjne tak, aby zmniejszać ryzyko bez wpływu na wydajność!
- zatrzymaj atak złośliwego oprogramowania na punktach końcowych poprzez ograniczenie hakerom możliwości przekraczania punktu wejścia!

e: sales@thycotic.com
t: @thycotic
www.thycotic.com