jamf

WHITE PAPER

Przewodnik po skutecznym reagowaniu na incydenty bezpieczeństwa w systemie macOS

Kiedy dochodzi do cyberataku lub naruszenia bezpieczeństwa, to jak sprawnie i skutecznie organizacja reaguje jest bezpośrednio skorelowane z wielkością poniesionych szkód oraz czasem i kosztami odzyskania danych. Proces ten określany jest jako reagowanie na incydenty bezpieczeństwa i jest krytycznym elementem każdego udanego programu bezpieczeństwa realizowanego przez zespoły IT lub bezpieczeństwa informacji.

Chociaż większość organizacji stosuje solidne praktyki w zakresie ochrony przed zagrożeniami bezpieczeństwa, istnieją narzędzia, przepływy pracy i najlepsze praktyki, dzięki którym organizacja jest przygotowana i gotowa na wypadek ataku cybernetycznego lub naruszenia bezpieczeństwa. A ponieważ liczba komputerów Mac w przedsiębiorstwach rośnie, nadszedł czas, aby udoskonalić praktyki w zakresie bezpieczeństwa komputerów Mac i zapewnić ochronę organizacji.

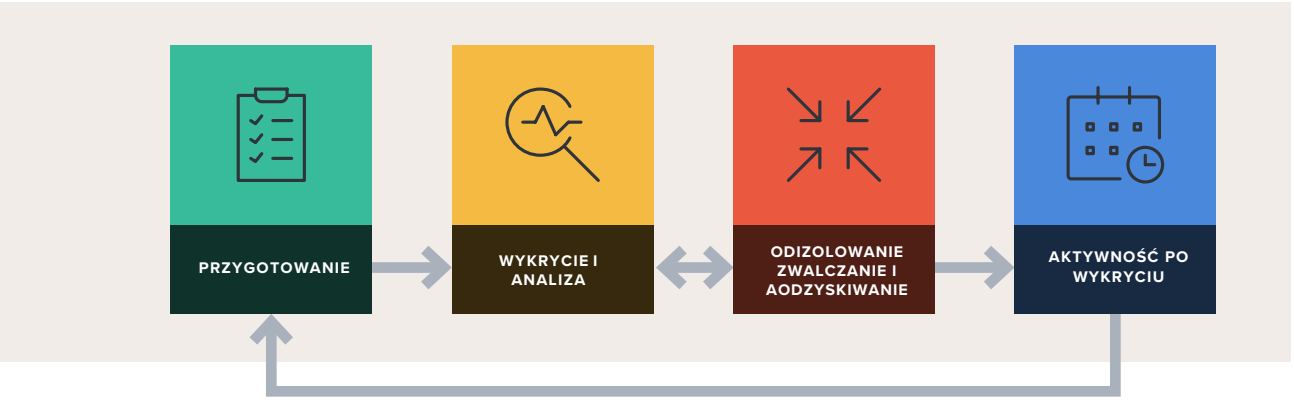
W naszym white paper dowiesz się kroków do:

1. Przygotowania na incydenty
2. Wykrywania i analizy incydentów
3. Ograniczanie, eliminowanie i usuwanie skutków incydentów
4. Monitorowanie działań po zdarzeniu

Wyjątkowe ataki wymagają wyjątkowej obrony

Wraz z rosnącą popularnością komputerów Mac w organizacjach pojawia się potrzeba poświęcenia dodatkowej uwagi ochronie i zabezpieczeniom komputerów Mac w zakresie wykraczającym poza rozwiązania bezpieczeństwa skoncentrowane na systemie Windows. Komputery Mac zawsze były wyposażone we wbudowane narzędzia bezpieczeństwa, ale nowe sposoby ataku i większy udział w rynku wymagają zastosowania lepszych metod ochrony systemu operacyjnego i danych organizacyjnych. Niezależnie jednak od sposobu wykorzystania rozwiązań bezpieczeństwa dla komputerów Mac, reagowanie na incydenty powinno być metodyczne i spójne.

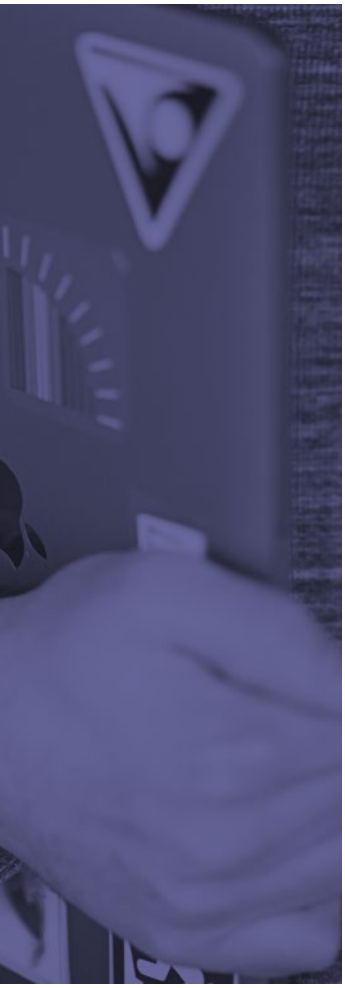
Zgodnie z założeniami National Institute of Standards and Technology (NIST), cztery elementy reakcji na incydenty bezpieczeństwa to:



Krok 1: Przygotowanie na incydenty

Bezpieczeństwo jest priorytetem dla prawie każdej organizacji, a wraz z przejściem na większą liczbę pracowników zdalnych, będzie jeszcze ważniejsze. Administratorzy IT potrzebują, aby punkty końcowe były jak najbezpieczniejsze. Punkty końcowe muszą być zarządzane, monitorowane, łatane i konfigurowane pod kątem bezpieczeństwa. Aby to zrobić, potrzebne są różne narzędzia.

Jamf Pro oferuje pulpity nawigacyjne, które pozwalają na bieżąco kontrolować stan urządzeń Mac i sygnalizują sprzęt wymagający uwagi. Dzięki opatentowanej funkcji Smart Group, administratorzy IT mogą wskazać urządzenia, które wymagają aktualizacji, rekonfiguracji lub poprawek, aby poprawić ich stan bezpieczeństwa. Wszystko to odbywa się zdalnie i może być zautomatyzowane bez fizycznego kontaktu z urządzeniem.



Aby zapewnić widoczność tego, co dzieje się na urządzeniu, Jamf Protect - korporacyjna ochrona punktów końcowych przeznaczona dla komputerów Mac - gromadzi informacje o procesach i plikach oraz inne analizy behawioralne; wszystkie te informacje są pomocne w analizie w czasie rzeczywistym i po jej zakończeniu, aby zidentyfikować złośliwą aktywność i wygenerować alerty. Ważne rzeczy do odnotowania:

- Zapobieganie zagrożeniom Jamf Protect automatycznie blokuje i poddaje kwarantannie złośliwe oprogramowanie i adware. Organizacje, które chcą ograniczyć konkretne niechciane oprogramowanie, mogą to również zdefiniować w Jamf Protect za pomocą sygnatur, TeamID deweloperów itp.
- Typowe wzorce ataków na system macOS są wykrywane za pomocą analityki wbudowanej w Jamf Protect. Aby zapewnić, że mechanizmy wykrywania prawidłowo ograniczają ryzyko, analizy są mapowane do MITRE ATT&CK® Framework i zapewniają niezawodne pokrycie wektorów ataku.
- Jamf Protect gromadzi solidny poziom danych związanych z każdym zidentyfikowanym atakiem, dzięki czemu można zobaczyć wszystkie procesy, użytkowników, grupy i informacje binarne w momencie wykrycia zagrożenia.
- Dane i alerty mogą być wysyłane z Jamf Protect do Twojego SIEM. Dodatkowo, dane dziennika z macOS Unified Logging mogą być wysyłane bezpośrednio do Twojego SIEM lub innego systemu raportowania.
- Wiele ataków ma wspólne reakcje, które można skonfigurować i zautomatyzować dla pożądanych reakcji i działań naprawczych za pomocą Jamf Pro.
- Dodatkowe procesy reagowania mogą być uruchamiane automatycznie lub ręcznie podczas reagowania na incydenty w Jamf Pro, wykorzystując scoping do Smart Groups, aby wypchnąć polityki i profile konfiguracji.

Polityki i profile konfiguracyjne pozwalają na:

IZOLACJA SIECI	Odizoluj urządzenia, które mogą być poddane aktywnemu atakowi, gdzie należy ograniczyć szkody.
POLE KARNE	Ograniczenie niezaufanemu użytkownikowi dostępu do zasobów korporacyjnych.
BLOKADA URZĄDZEŃ	Zablokuj użytkownikom dostęp do urządzenia na czas badania podejrzanej aktywności.
USUWANIE OBIEKTÓW	Usuń zdalnie z urządzenia niechciane aplikacje, wtyczki lub pliki.
KWARANTANNA URZĄDZEŃ	Jeśli incydent wymaga fizycznego dostępu do urządzenia i nie można go odzyskać zdalnie, należy poddać urządzenie kwarantannie i odizolować je do czasu uzyskania fizycznej kontroli przez dział IT.
SKRYPTY / KOMENDY	Wykorzystanie skryptów i poleceń do zdalnego odzyskiwania danych lub informacji o urządzeniu bez jego fizycznego dotykania.
NIESTANDARDOWE KOMUNIKATY DLA UŻYTKOWNIKÓW	Przekazywanie informacji takich jak próby ataków czy polityki organizacyjne i najlepsze praktyki bezpośrednio do użytkowników końcowych.
ODZYSKANIE URZĄDZENIA	Zdalnie przywróć system macOS i aplikacje na urządzenie, które wymaga przywrócenia czystego stanu.

Krok 2: Wykrywanie i analiza

Nawet jeśli zespół bezpieczeństwa jest w stanie zaalarmować w przypadku wskazania ataku, nie powinien popadać w samozadowolenie. Pomimo przygotowań i wdrożonych mechanizmów zapobiegawczych, zespoły bezpieczeństwa powinny założyć, że ataki przebiją się przez ich najlepszą obronę i być gotowe do zaangażowania.

Wyobraź sobie, że użytkownik końcowy przypadkowo pobiera skompromitowaną aplikację... Nadszedł czas, aby Twoje rozwiązanie zabezpieczające punkty końcowe wzięło się do pracy. Kiedy dochodzi do incydentu bezpieczeństwa, a Ty nie masz pojęcia, jakie są jego skutki, musisz zebrać odpowiednie informacje, przeanalizować zagrożenie i mieć możliwość odizolowania tego urządzenia, aby zapobiec dalszemu zanieczyszczeniu.

Zespoły bezpieczeństwa zawsze potrzebują większej widoczności podczas badania incydentu i często gromadzą logi z różnych systemów i urządzeń w systemach SIEM lub innych systemach agregacji logów, próbując uzyskać taką widoczność. W trakcie dochodzenia lub audytu organizacja może uzyskać pełny i dostosowany do potrzeb obraz tego, co dzieje się we flocie komputerów Mac.

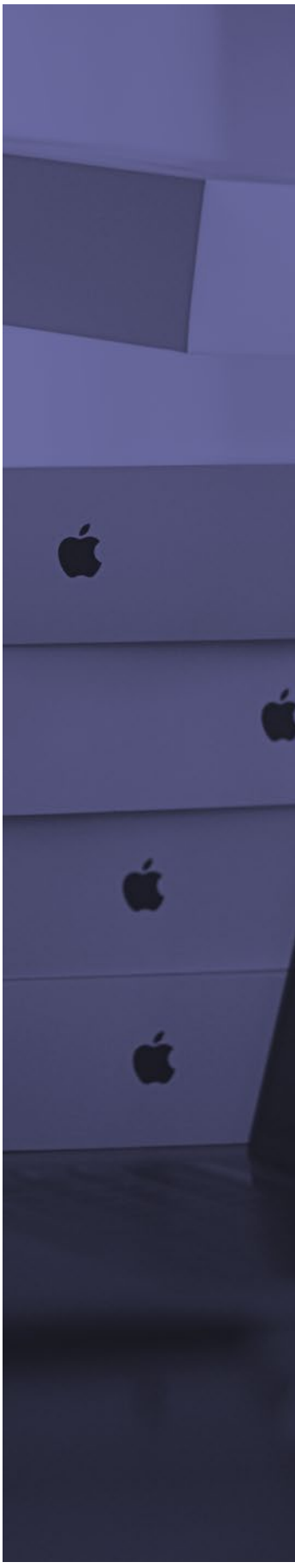
Krok 3: Ograniczanie, zwalczanie i odbudowa

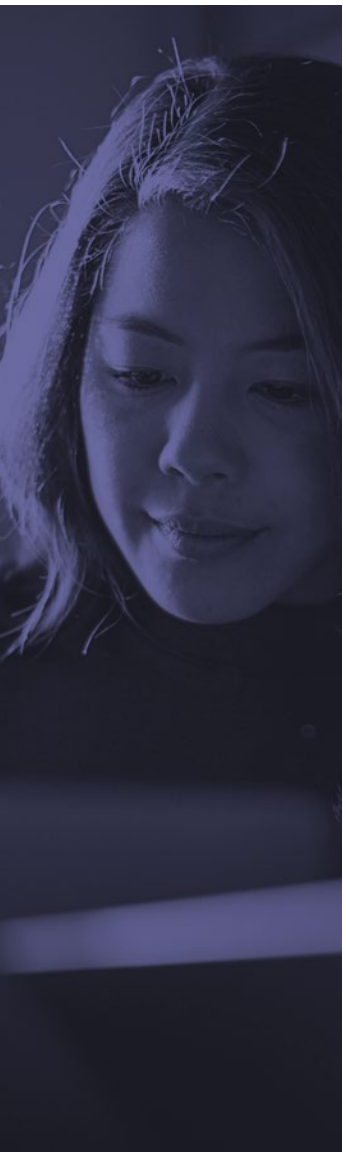
Kiedy atak jest aktywny w Twojej sieci, czas ma kluczowe znaczenie. Po pierwsze, należy powstrzymać atak i zapobiec jego rozprzestrzenieniu się na inne systemy. Dzięki Twojemu przygotowaniu, odpowiednie procesy zostaną prawdopodobnie zablokowane przez Jamf Protect, ale to nie oznacza, że inne, nie tak oczywiste przyczółki napastników zostaną zlikwidowane. W celu zminimalizowania możliwości wystąpienia szkód podczas reakcji na alarm oparty na aktywności, Jamf Protect wykorzystuje technologię Smart Group, a także wszystkie polecenia zarządzania urządzeniami mobilnymi (MDM) i Jamf Pro. Przykłady zautomatyzowanych reakcji obejmują:

- Izolowanie maszyny w sieci, aby mogła rozmawiać tylko z infrastrukturą zarządzającą.
- Ograniczenie dostępu do chmury lub zasobów korporacyjnych.
- Dostarczanie użytkownikowi końcowemu wskazówek, że na jego urządzeniu znajduje się złośliwa aktywność i aby powstrzymał się od dalszych działań.

Gdy urządzenie jest już bezpieczne, a atak został powstrzymany, zespoły IT i bezpieczeństwa będą chciały dalej badać, co się stało na urządzeniu i czy istnieją inne skrypty, binaria, backdoory, nowe dane uwierzytelniające lub jakiekolwiek dodatkowe zagrożenia, które wciąż się utrzymują. Dzięki Jamf, zespoły mogą:

- Pobierz zablokowane binarki z kwarantanny do sprawdzenia.
- Usuń zidentyfikowane binaria lub inne pliki.
- Identyfikacja nowozainstalowanych aplikacji.
- Zidentyfikuj nowe lokalne konta użytkowników.





Po tym jak Jamf złagodzi atak, urządzenia nadal muszą być przywrócone do stanu zaufanego. Dzięki możliwościom polityk Jamf Pro i Smart Groups, możesz oczyścić swoje środowisko bez dodatkowych kosztów ogólnych przez:

- Uruchamianie niestandardowych skryptów / poleceń w celu zresetowania ustawień zabezpieczeń.
- Niestandardowe komunikaty dla użytkowników końcowych kierujące ich do dodatkowych zasobów pomocy.
- Ponowne zainstalowanie systemu macOS oraz wszelkich aplikacji

Krok 4: Czynności po zdarzeniu

Jamf Protect w porę powiadamia zespoły IT i zespoły ds. bezpieczeństwa o możliwości wystąpienia incydentu i dostarcza narzędzi do dokładnej analizy tego, co się stało. Podczas gdy procesy ograniczania, eliminacji i odzyskiwania są często tworzone na zamówienie w świecie Windows, Jamf przenosi tę funkcjonalność na komputery Mac, dzięki czemu zespoły mogą reagować i podejmować działania naprawcze w sposób najlepiej wspierający firmę Apple przy następnym incydencie bezpieczeństwa.

Po wystąpieniu incydentu:

- Jamf Protect nadal monitoruje i informuje o wszelkich dodatkowych zagrożeniach i działaniach.
- Jamf Protect Analytics można dostosować i rozszerzyć, aby objąć dodatkowe ukierunkowane zagrożenia, które identyfikuje zespół IT lub InfoSec.
- Dodaj informacje o zidentyfikowanych zagrożeniach binarnych do niestandardowej listy zapobiegania, aby zapewnić ochronę całej floty komputerów Mac
- Zapewnienij, że użytkownicy końcowi będący celem ataku są ponownie certyfikowani w zakresie edukacji operacyjnej InfoSec.

Lepsze zabezpieczenia komputerów Mac zaczynają się już dziś

Aby skutecznie ocenić incydent bezpieczeństwa i określić potencjalne zagrożenia wynikające z naruszenia, Jamf Pro w połączeniu z Jamf Protect umożliwia monitorowanie, zapobieganie, wykrywanie i reagowanie na niezliczoną ilość ataków, które mogą być skierowane przeciwko flocie Mac.

Od pobierania przez użytkowników końcowych zagrożonych aplikacji do prób spear phishingu lub ataków ransomware, środki zaradcze pozwalają na podjęcie niezbędnych działań w celu zabezpieczenia sprzętu, oprogramowania i danych organizacji.

Przetestuj funkcje reagowania na incydenty bezpieczeństwa za pomocą bezpłatnej wersji próbnej.

KONTAKT