Helion

<packt>

Cyberbezpieczeństwo i strategie blue teamów

Walka z cyberzagrożeniami w Twojej organizacji

KUNAL SEHGAL | NIKOLAOS THYMIANIS

Tytuł oryginału: Cybersecurity Blue Team Strategies: Uncover the secrets of blue teams to combat cyber threats in your organization

Tłumaczenie: Piotr Ptaszek

ISBN: 978-83-289-0456-9

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/cystbl
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

CZĘŚĆ 3. Zapytaj ekspertów

Rozdział 1 Tworzenie strategii obrony

Ponieważ liczba cyberataków stale się zwiększa we wszystkich krajach i branżach, zdolność do obrony przed nimi jest absolutną koniecznością dla wszystkich organizacji. Jednak podróż w stronę stworzenia zespołu i osiągnięcia przez niego właściwego poziomu dojrzałości wymaga odpowiedniej kombinacji technologii, procesów i ludzi. Ta droga może się wydawać niełatwa i przytłaczająca dla wielu początkujących. Ta książka ma na celu wspomóc organizacje i profesjonalistów w tej podróży. Ma za zadanie uświadomić czytelnikom, że wszelkie aspekty związane z obroną prowadzoną przez zespół niebieski są zrozumiałe i nie mają słabych punktów.

Specjaliści ds. cyberbezpieczeństwa, którzy są zgrupowani pod sztandarem *zespołu niebieskiego*, identyfikują różne luki w zabezpieczeniach, zwane również podatnościami (ang. *vulnerabilities*), w infrastrukturze i aplikacjach organizacji. Wysiłki te pomagają w łataniu luk i wdrażaniu różnych procedur bezpieczeństwa i kontroli. Cyberprofesjonaliści pracujący w blue teamie zazwyczaj mają talent do kreatywnego myślenia i błyskawicznego reagowania na różnego rodzaju zdarzenia i incydenty związane z bezpieczeństwem. Odpowiadają za ochronę podmiotów gospodarczych przed ryzykiem i zagrożeniami cybernetycznymi.

W tym rozdziale omówimy następujące tematy:

- Sposób, w jaki organizacje odnoszą korzyści z utworzenia zespołu niebieskiego.
- Skład zespołu niebieskiego.
- Zespół czerwony (ang. *red team*).
- Zespół fioletowy (ang. *purple team*).
- Informacje o cyberzagrożeniach.
- Umiejętności wymagane od członków zespołu niebieskiego.

Sposób, w jaki organizacje odnoszą korzyści z utworzenia zespołu niebieskiego

Zanim zaczniemy, ważne jest, aby zrozumieć korzyści, jakich organizacja może oczekiwać po stworzeniu zespołu niebieskiego. W tym rozdziale skupimy się na tym, co organizacja może zyskać po utworzeniu takiego zespołu i jakie działania trzeba podjąć, aby taki zespół odniósł sukces.

Ocena ryzyka

Przede wszystkim firmom zaleca się ocenienie ryzyka i zagrożeń, które mają wpływ na ich aktywa organizacyjne zlokalizowane na całym świecie. Zespół niebieski przeprowadza ocenę ryzyka, aby dowiedzieć się, jak i co należy bronić przed cyberatakami. Zazwyczaj zaleca wdrożenie rygorystycznych procesów bezpieczeństwa i przygotowanie standardowych procedur w celu poprawy bezpieczeństwa organizacji. Często projektuje również strukturę szkolenia z podstaw cyberbezpieczeństwa dla użytkowników końcowych, zwanego **End User Security Awareness**. Pomaga to organizacjom zidentyfikować ich krytyczne zasoby i profil zagrożeń dla każdego zasobu oraz całej organizacji.

Monitorowanie i nadzorowanie

Monitorowanie i nadzorowanie to podstawowe zadania specjalistów zespołu niebieskiego. Organizacje otrzymują od blue teamów zalecenia dotyczące pozyskiwania, wdrażania i uruchamiania różnych narzędzi do monitorowania bezpieczeństwa. Narzędzia te umożliwiają organizacjom rejestrowanie informacji o różnych rodzajach uprawnień dostępu, jakie użytkownicy i pracownicy mają w infrastrukturze sieciowej. Wszystkie działania użytkowników są rejestrowane, a podejrzane działania wyzwalają alerty zgodnie z regułami skonfigurowanymi w różnych narzędziach bezpieczeństwa. Codzienne sprawdzenia, takie jak audyt konfiguracji DNS i zapory sieciowej, codzienne kontrole zgodności na pulpitach różnych wdrożonych narzędzi i inne czynności to niektóre z **kluczowych obszarów odpowiedzialności** (ang. *Key Responsibility Areas*, **KRA**) zespołów niebieskich. Przeprowadzają one również różnego rodzaju wewnętrzne i/lub zewnętrzne oceny podatności sieci. Od czasu do czasu blue teamy pomagają ustalać priorytety i wskazują, jak załatać wykryte luki w zabezpieczeniach zapisane w raportach z testów penetracyjnych. Specjaliści z zespołu niebieskiego są ekspertami w skanowaniu sieci firmowej w celu identyfikacji luk w zabezpieczeniach oraz w analizowaniu przechwyconych pakietów sieciowych pod kątem podejrzanego ruchu przychodzącego i/lub wychodzącego.

Kontrola bezpieczeństwa

Blue teamowi powierza się również zadanie ustanowienia różnego rodzaju technicznej kontroli bezpieczeństwa nad krytycznymi zasobami. Dlatego musi zidentyfikować i sklasyfikować najbardziej krytyczne elementy sieci w organizacji. Organizacje mogą korzystać z **bazy danych zarządzania konfiguracją** (ang. *Configuration Management Database*, **CMDB**) w celu dokumentowania zmian, jakie przeprowadzają w dowolnej konfiguracji tych zasobów. CMDB są również wykorzystywane do scentralizowania zapisu wszystkich elementów sieci w dowolnej infrastrukturze sieciowej. Zasoby, które prawdopodobnie mogą spowodować zamknięcie firmy, jeśli zostaną dotknięte cyberatakami, są klasyfikowane jako *zasoby krytyczne*. Większość z tych zasobów jest chroniona dodatkowymi zabezpieczeniami. Oprócz oceny ryzyka blue teamy przeprowadzają również badania oceny wpływu. Obejmują one określanie wpływu, jaki mogą mieć różne cyberataki, jeśli uderzą w konkretne zasoby krytyczne i jeśli te zasoby ulegną awarii na określony czas. Może to bowiem poważnie wpływać na operacje biznesowe na dużą skalę. Z tego powodu ryzyka i zagrożenia, które oddziałują na każdy zasób należący do kategorii krytycznej, są dokumentowane. Regularne skanowanie zasobów w celu oceny ich podatności na zagrożenia jest przeprowadzane dla wszystkich ujawnionych luk w zabezpieczeniach — zwanych **Common Vulnerabilities and Exposures** (**CVE**) i **Common Weakness Enumeration** (**CWE**). Członkowie zespołu niebieskiego są biegli w ocenie ryzyka i sugerowaniu rekomendacji również dla nich. Większość podatności krytycznych i wysokiego poziomu jest łatana tak szybko, jak to możliwe. W celu zmniejszenia wpływu tych podatności, dla których nie wydano jeszcze poprawek, blue team opracowuje plan wdrożenia kontroli bezpieczeństwa.

Raportowanie i rekomendacje dla kierownictwa

Kierownictwo musi zdecydować, czy stosowane środki kontroli bezpieczeństwa są odpowiednie. Członkowie blue teamu przygotowują dokument o znanych zagrożeniach, na jakie narażona jest firma. Mogą również przeprowadzać analizę kosztów i korzyści dla kierownictwa oraz zalecić wdrożenie minimum tych środków kontroli bezpieczeństwa, które uznano za kluczowe.

Na przykład zespoły niebieskie mogą odkryć, że sieć firmy jest podatna na ataki **Distributed Denial-of-Service** (**DDoS**). Ataki DDoS uniemożliwiają dostęp do sieci rzeczywistym użytkownikom poprzez zalewanie serwerów firmowych żądaniami pochodzącymi z maszyn „zombie". Niedostępność usług może spowodować wtedy utratę dochodów firmy. Im więcej czasu zajmuje zespołowi sieciowemu zablokowanie określonej podsieci adresów IP, tym więcej strat dotyka biznes. Tego rodzaju ataki poważnie unieruchamiają sieć organizacyjną. Blue team nie tylko przeprowadza analizę i próbuje pomóc w blokowaniu adresów IP należących do serwerów C2 atakujących, ale także przeprowadza ocenę wpływu. Aby zapobiec atakom typu DDoS lub jakimkolwiek rodzajom ataków typu **Denial-of-Service** (**DoS**), zespół niebieski zaleca wdrożenie rozwiązań bezpieczeństwa obwodowego. Takie programowe rozwiązania zdecydowanie zmniejszają prawdopodobieństwo narażenia organizacji na ataki DDoS. Choć nie mogą zapobiec ich powstawaniu, to jednak z pewnością mogą uchronić przed nimi Twoją sieć. Rozwiązania zabezpieczające, takie jak obwodowe zapory sieciowe, moduły równoważenia obciążenia i WAF pomagają w wykrywaniu ataków DoS i zapobieganiu ich wpływom na sieć organizacji.

Założenie blue teamu przynosi wiele innych korzyści; powyżej został zaprezentowany jedynie przegląd tych podstawowych. Teraz skupimy się na tym, jakie osoby należy zatrudnić w takim zespole.

Skład zespołu niebieskiego

Blue team składa się z wielu osób o różnorodnych umiejętnościach. Skład zespołu różni się w zależności od potrzeb organizacji. W tej sekcji przyjrzymy się kilku typowym rolom, które zwykle pełnią członkowie zespołu.

Analityk

Podstawowa rola w cyberbezpieczeństwie to *analityk SOC*, pracujący w firmowym **Security Operations Center** (**SOC**). Analityk cyberbezpieczeństwa jest również nazywany analitykiem triażu. Analityk SOC reaguje na alerty dotyczące incydentów o określonej wadze i bada dowody. Ta rola ma charakter reaktywny. Organizacje zwykle mają w SOC role na **poziomie 1** (**L1**), **2** (**L2**) i **3** (**L3**). L1 to rola analityka o małym doświadczeniu, podczas gdy L3 to rola w SOC wymagająca największego doświadczenia. W większości przypadków większy numer poziomu oznacza większy poziom odpowiedzialności i wymagań dotyczących doświadczenia.

SOC monitoruje ruch w sieci IT pod kątem nietypowych lub podejrzanych zachowań. Pewne podejrzane działania mogą wskazywać na istnienie w sieci złośliwych podmiotów lub programów, takich jak trojany i ransomware. Starsi analitycy (ang. *senior analysts*) analizują alerty generowane przez systemy do **zarządzania incydentami i zdarzeniami bezpieczeństwa** (ang. *Security Incident and Event Management*, **SIEM**), takie jak Splunk, IBM QRadar, LogRhythm i inne. Analitycy pracują nad segregacją i identyfikacją podejrzanych zdarzeń oraz określają, czy alerty są fałszywie pozytywne, czy prawdziwie pozytywne. W przypadku prawdziwie pozytywnych alertów przestrzegana jest wstępnie zdefiniowana **standardowa procedura operacyjna** (ang. *Standard Operating Procedure*, **SOP**), zgodnie z dokumentami zwanymi *playbook* lub *runbook*. Analiza i śledztwo przeprowadzane przez młodszych analityków (ang. *junior analysts*) pomagają ustanowić kontekst incydentów bezpieczeństwa, które się wydarzyły. Określają również dotkliwość problemu związanego z bezpieczeństwem i stosują do niego odpowiednią ocenę ryzyka. Incydenty bezpieczeństwa o poziomie krytycznym i wysokim są natychmiast przekazywane do **cyberratownika** (ang. *Incident Responder*, **IR**) w zespole SOC.

Cyberratownik

Cyberratownik jest również znany jako analityk odpowiedzi na incydenty. Taki specjalista ocenia, czy zgłoszony alarm to atak, czy też trwałe zagrożenie dla sieci firmowej. Daje gwarancję, że sytuacja zostanie opanowana tak szybko, jak to możliwe, a organizacja będzie potrafiła zareagować i odzyskać poprzedni stan zgodnie z określonymi planami. IR zwykle bada zakres cyberataku.

W oparciu o skalę problemu związanego z cyberbezpieczeństwem cyberratownik opracowuje strategię naprawczą. Wiąże się to z badaniem charakterystyki incydentu. Obejmuje ono zasoby biznesowe będące celem złośliwego oprogramowania i wskazuje rodzaje szkodliwych działań przez nie przeprowadzanych. Następnie IR rekomenduje odpowiedni sposób postępowania. Wraz z odpowiednimi zespołami implementuje środki zaradcze, takie jak inicjowanie zgłoszeń IT w celu ponownego zobrazowania zaatakowanego systemu. Cyberratownik często przeprowadza szkolenia użytkowników mające na celu zwiększenie ich świadomości w zakresie bezpieczeństwa, zalecone przez CISO (ang. *Chief Information Security Officer*). Powiadamia również dyrektorów o zakresie ewentualnego naruszenia ochrony danych.

Łowca zagrożeń

Stanowisko łowcy zagrożeń (ang. *threat hunter*) może też nosić nazwy **analityk zagrożeń** lub **badacz zagrożeń**. Praca threat hunterów jest *proaktywna*. Regularnie badają zagrożenia i ryzyko, aby być na bieżąco z najnowszymi zagrożeniami. Analizują również ewolucję i anatomię zagrożeń. Łowcy zagrożeń często opracowują reguły, które wyzwalają alerty w firmowym rozwiązaniu SIEM dla określonych cyberzagrożeń.

Threat hunterzy są biegli w konfigurowaniu oraz monitorowaniu wielu platform analizy zagrożeń (na przykład IBM X-Force, Alienvalult OTX, VirusTotal i inne) w celu proaktywnego badania cyklu życia zagrożenia. Oceniają, czy nowo powstałe zagrożenia stanowią największe zagrożenie dla firmy, na podstawie różnych parametrów, takich jak docelowe branże, wykorzystywane podatności i ataki TTP. Łowcy zagrożeń często wprowadzają zmiany w konfiguracji systemu, aby zareagować na wykryte zagrożenia cybernetyczne. Analiza cyberzagrożeń i ryzyka w czasie rzeczywistym może być przytłaczająca, gdy otrzymywanych informacji o zagrożeniach jest więcej, niż zespół HR jest w stanie przetworzyć. Dlatego threat hunterzy wykorzystują automatyzację w technologiach bezpieczeństwa do automatycznego wykrywania zachowań typowych dla określonych zagrożeń. Uwrażliwiają i wzmacniają organizacyjną infrastrukturę sieciową, aby powstrzymać potencjalny cyberatak.

Załóżmy, że niedawno pojawiło się nowe cyberzagrożenie ransomware (takie jak **Lockbit 2.0** lub **BlackMatter**). Threat hunter zbada to zagrożenie i, korzystając z automatyzacji w celu zapobieżenia jego przeniknięciu do firmy, zidentyfikuje je, jeśli wystąpi.

Aby zostać zatrudnionym na stanowisku łowcy zagrożeń, od kandydata wymagane jest doświadczenie w pracy na stanowiskach analityka SOC i IR, a także biegłość w sieciach komputerowych i systemach oraz administracji. Dobrze jest również znać różne źródła informacji o zagrożeniach w sieci, nie wyłączając dark webu. Dogłębne zrozumienie cyberzagrożeń charakterystycznych dla sektora biznesowego często zapewnia kandydatowi przewagę konkurencyjną na rynku pracy w zakresie analizy zagrożeń i threat huntingu. Dobry łowca zagrożeń lub specjalista ds. analizy zagrożeń (ang. *Threat Intelligence Analyst*, **TIA**) jest biegły w uzyskiwaniu proaktywnych i praktycznych informacji o zagrożeniach (ang. *Threat Intelligence*, **TI**) za pośrednictwem dowolnej liczby źródeł z sieci i dark webu, w tym różnych kanałów IRC (ang. *Internet Relay Chat*, **IRC**) i for internetowych. Dobry threat hunter musi być w stanie dobrać odpowiednie techniczne i nietechniczne metodologie, a także posiadać wiedzę z każdej dziedziny w zakresie korzystania z różnych platform TI.

Konsultant do spraw bezpieczeństwa

Konsultanci ds. bezpieczeństwa są często zatrudniani na podstawie umowy i wykonują zadania przez cały cykl życia projektu, zgodnie z wymaganiami. Mogą to być również osoby spoza organizacji, które są wiarygodnymi źródłami wiedzy lub mogą się wykazać doświadczeniem w zakresie określonego narzędzia lub obszaru bezpieczeństwa. Często są ekspertami w swojej dziedzinie. Innym terminem używanym do określania konsultantów ds. bezpieczeństwa jest **Subject Matter Expert** (**SME**). Konsultant ds. strategii bezpieczeństwa i konsultant ds. operacji bezpieczeństwa to przykłady wyspecjalizowanych ról.

Administrator bezpieczeństwa

Administrator bezpieczeństwa to nie to samo co analityk SOC. Często jednak zdarza się, że organizacje uznają administratorów bezpieczeństwa za analityków SOC **poziomu 4** (**L4**), których zadaniem jest pobieranie, instalowanie, konfigurowanie, wdrażanie i uruchamianie różnych narzędzi bezpieczeństwa w SOC. Dbają też o aktualizację tych narzędzi, gdy pojawią się aktualizacje dostawcy. To stanowisko jest podobne do roli administratora systemów, ale obejmuje zarządzanie wszystkimi narzędziami bezpieczeństwa w SOC, takimi jak SIEM, SOAR, AV-NGAV, EDR-XDR, DLP, przynęty (ang. *honeypots*), zarządzanie chmurą, WAF, zapora sieciowa, moduły równoważenia obciążenia, IAM i AD, rozwiązania do monitorowania nadużyć oraz zniesławiania marki i nie tylko. Praca obejmuje również stosowanie łatek lub poprawek wydanych przez odpowiednich dostawców narzędzi oraz konfigurowanie narzędzi bezpieczeństwa w celu zapewnienia optymalnej wydajności. Administrator bezpieczeństwa często współpracuje z łowcami zagrożeń i cyberratownikami (IR) w celu tworzenia skryptów i programów bezpieczeństwa, które automatyzują niektóre nadmiarowe zadania związane z bezpieczeństwem. Nie zajmuje się jednak badaniem zdarzeń i incydentów związanych z bezpieczeństwem, oflagowanych przez narzędzia bezpieczeństwa.

Administrator zarządzania tożsamością i dostępem

Ta rola zapewnia wsparcie w zakresie **zarządzania tożsamością i dostępem** (ang. *Identity and Access Management*, **IAM**) kilku działom w firmie. Zarządzanie uprawnieniami i uprawnieniami do aplikacji/systemu, **jednokrotne logowanie** (ang. *Single Sign-On*, **SSO**), raportowanie korzystania z aplikacji oraz współpraca z programistami w celu integracji zasad zarządzania tożsamością i dostępem dla nowych aplikacji i oprogramowania to niektóre z kluczowych obowiązków administratora IAM. Specjaliści ci mają niszowe doświadczenie w korzystaniu z różnych narzędzi IAM, a także w administrowaniu siecią.

Analityk zgodności

Analityk zgodności (ang. *compliance analyst*) często wykonuje audyt wewnętrzny korporacji lub firmy. Sprawdza i weryfikuje, czy firma przestrzega zasad bezpieczeństwa, polityki prywatności, krajowych przepisów dotyczących ochrony danych lub innych

obowiązujących praw/przepisów. Ma doświadczenie we wszystkich wyżej wymienionych rolach, ponieważ analityk zgodności jest zobowiązany do prowadzenia częstych dyskusji z przedstawicielami wszystkich innych roli zawodowych w ramach kontroli zgodności. Regularnie opracowuje raporty o stwierdzonych lub wykrytych niezgodnościach w infrastrukturze sieciowej i przekazuje je kierownictwu wyższego szczebla. Dodatkowo pomaga firmie w przygotowaniu się do audytów zewnętrznych, które mogą być obowiązkowe w niektórych sektorach biznesowych (np. służba zdrowia, bankowość, finanse, ubezpieczenia, sektor energetyczny i inne).

W tym podrozdziale podano podstawowe informacje pozwalające stworzyć zespół niebieski. Może być więcej ról do obsadzenia, w zależności od rodzaju lub złożoności organizacji, tutaj jednak omówiliśmy role typowe dla każdej organizacji. W dalszej części krótko scharakteryzujemy red teamy i purple teamy. Choć te dwa zespoły nie należą do blue teamu, to jednak ważne jest, aby zrozumieć, czym się zajmują. Ponadto opiszemy również rolę zespołu ds. analizy cyberzagrożeń. Zazwyczaj znajduje się on w zespole niebieskim, ale zdarza się, że jest z niego wydzielony.

Zespół czerwony

Członkowie red teamu zachowują się jak hakerzy, którzy próbują znaleźć i wykorzystać wszelkie potencjalne luki w sieci firmowej. Są znani z używania wielu konwencjonalnych i niekonwencjonalnych technik w celu wykrycia wad w technologii i procesach oraz czynnika ludzkiego. Dlatego zwykle taki zespół istnieje poza blue teamem. Jednak, dla lepszego zrozumienia, omówmy pokrótce tę rolę.

Misja zespołu czerwonego polega na wyszukiwaniu znanych podatności, które zostały już ujawnione i mają identyfikator **Common Vulnerabilities and Exposures** (**CVE**). Specjaliści z tego zespołu przeprowadzają także testy penetracyjne infrastruktury sieci firmy w celu wykrycia nieznanych luk w zabezpieczeniach. Zespoły te mogą również testować sieci bezprzewodowe i IoT, a także urządzenia końcowe (ang. *endpoint devices*), takie jak laptopy, komputery PC, telefony komórkowe, tablety i inne. Testy penetracji sprzętu są przeprowadzane na urządzeniach ubieralnych IoT i urządzeniach wykorzystujących Bluetooth. Hakerzy w red teamach mogą testować socjotechniki na pracownikach swojej organizacji. Tego rodzaju hakerzy często otrzymują fałszywe tożsamości do działania na terenie firmy. Odgrywają kluczową rolę w identyfikowaniu oraz sugerowaniu niezbędnych środków bezpieczeństwa w celu naprawy naruszeń bezpieczeństwa, które wynikają z braku odpowiednich zabezpieczeń fizycznych. Endpointy i urządzenia mobilne również są objęte zakresem ich testów penetracyjnych lub włamań.

Omówienie szczegółowo obowiązków członków zespołu czerwonego wykracza poza zakres tego rozdziału. Należy jednak zauważyć, że red team i blue team zazwyczaj pracują w tandemie. Oto niektóre obszary, w których zespoły te ze sobą współpracują:

- tworzenie mapy topologii/hierarchii sieci w infrastrukturze sieciowej firmy w celu ustalenia liczby uruchomionych hostów, a także ich statusów;
- ocena uruchomionych usług i otwartych portów w tych systemach;
- identyfikacja dostawcy, firmware'u i szczegółów systemu operacyjnego oraz innych istotnych parametrów sprzętu;

- identyfikacja i wykorzystywanie CVE w serwerach, hubach, zaporach sieciowych, routerach, przełącznikach L2/L3, punktach dostępowych Wi-Fi i innym sprzęcie sieciowym;
- hakowanie różnego rodzaju zabezpieczeń fizycznych, takich jak przeszklone drzwi, zamki cyfrowe, sieci CCTV, a czasem także pracownicy ochrony.

W niektórych organizacjach rozsądne może być również ustanowienie programu nagród bug bounty. Są to nagrody w formie pieniędzy lub gadżetów przekazywane etycznym hakerom. Hakerzy na całym świecie wyszukują luki i w pewnych okolicznościach zarabiają na tym. Wiele witryn internetowych, organizacji i firm programistycznych oferuje programy bug bounty, w których użytkownicy mogą być rozpoznawani i wynagradzani za zgłaszanie błędów, w szczególności tych związanych z lukami w logice biznesowej (ang. *business logic*) i lukami w zabezpieczeniach sieci. Tego typu programy są tworzone przez firmy w celu nagradzania niezależnych bug bounty hunterów, którzy znajdują luki w zabezpieczeniach i słabości w systemach. Firmy wypłacają nagrody za znajdowanie luk w zabezpieczeniach i zgłaszanie ich w sposób etyczny i odpowiedzialny, zanim cyberprzestępcy będą mogli je wykorzystać lub na nich zarobić. Programy nagród są często używane w połączeniu z regularnymi testami penetracyjnymi, aby umożliwić przedsiębiorstwom ocenę bezpieczeństwa ich aplikacji w trakcie całego cyklu ich rozwoju. Dzięki temu firmy mogą korzystać z pomocy społeczności hakerów w celu ciągłego zwiększania poziomu bezpieczeństwa ich systemów — takie programy przyciągają bowiem zróżnicowaną grupę specjalistów o różnych umiejętnościach i wiedzy, co daje firmom przewagę nad ocenami podatności, które opierają się na niedoświadczonym personelu bezpieczeństwa. Dlatego zamiast jednej osoby lub jednego zespołu pracującego nad atakowaniem obrony organizacji zbiorowa siła tłumu może być dla niej korzystniejsza.

Zespół fioletowy

Podstawowym celem współpracy red i blue teamów jest poprawa ogólnego stanu bezpieczeństwa organizacji. W tym miejscu warto wspomnieć o zespole fioletowym. Taki zespół nie zawsze jest niezależną grupą, choć może taką być. Purple team ma na celu zbliżenie red teamu i blue teamu oraz zachęcenie ich członków do współpracy i wymiany pomysłów w celu utworzenia solidnej pętli informacji zwrotnych. Jego zadaniem jest rozwijanie umiejętności zespołu niebieskiego przy jednoczesnej maksymalizacji zaangażowania zespołu czerwonego. Firma funkcjonuje najlepiej, gdy red i blue teamy współpracują w celu wzmocnienia bezpieczeństwa organizacji.

Co najważniejsze, to właśnie komunikacja jest kluczowa w tej współpracy. Aby przeprowadzić ćwiczenia, zawsze powinna istnieć komunikacja między różnymi zespołami. Pamiętaj, że celem zespołu niebieskiego jest nadążanie za najnowszą technologią i dzielenie się tą wiedzą z zespołem czerwonym. Te dane pomagają zwiększyć bezpieczeństwo organizacji. Red team musi wiedzieć o najnowszych zagrożeniach oraz taktykach hakerskich i musi poinformować o nich blue team. Od celu testu zależy, czy zespół czerwony powiadomi niebieski o zbliżającym się teście. Jeśli celem jest imitowanie rzeczywistego ataku, członkowie zespołu czerwonego mogą nie informować zespołu niebieskiego z wyprzedzeniem, aby przetestować ich mechanizmy cyberobrony.

Kierownictwo powinno zachęcać zespoły do współpracy i komunikowania się ze sobą. Aby program bezpieczeństwa mógł się rozwijać, wymagana jest dobra koordynacja między obydwoma zespołami poprzez efektywne współdzielenie zasobów, raportowanie i wymianę informacji.

Zbieranie danych o cyberzagrożeniach

Analiza zagrożeń to termin często używany przez wielu profesjonalistów, który obejmuje wywiad taktyczny, operacyjny i strategiczny. Źródła, odbiorcy i formy informacji wywiadowczych są różne. Zasadniczo wszelkie informacje o zagrożeniach otrzymywane przez SOC w dowolnej firmie muszą umożliwiać proaktywne działanie. Blue team powinien być w stanie przyswoić te informacje i wykorzystać je do proaktywnej obrony swojej organizacji.

Dane o zagrożeniach składają się ze wskaźników różnych cyberzagrożeń, takich jak adresy IP, adresy URL czy hashe plików. Są one określane jako **wskaźniki zagrożeń** (ang. *Indicators of Threats*, **IoT**) lub **wskaźniki skompromitowania** (ang. *Indicators of Compromise*, **IoC**). Z drugiej strony analiza zagrożeń jest rodzajem opartego na faktach, przetworzonego i możliwego do udowodnienia zapisu opartego na analizie, która łączy dane i informacje z wielu źródeł w celu zidentyfikowania wzorców i dostarczenia spostrzeżeń, które byłyby istotne dla organizacji. Pozwala ludziom i systemom podejmować przemyślane decyzje i skuteczne działania w celu uniknięcia naruszeń, naprawy luk w zabezpieczeniach, poprawy stanu bezpieczeństwa przedsiębiorstwa i zmniejszenia ryzyka. Wywiad strategiczny zazwyczaj koncentruje się na TTP (z ang. *tactics, techniques, procedures* — taktyki, techniki i procedury) podmiotów stanowiących zagrożenie.

Analitycy cyberzagrożeń często zasiadają w zespole niebieskim. Duże organizacje mogą ich jednak wydzielić, by działali jako samodzielna jednostka współpracująca z blue, red i purple teamem, działami biznesowymi i innymi. Omówimy to bardziej szczegółowo w dalszej części tej książki.

Teraz, gdy przedstawiliśmy zespoły, które ściśle współpracują z blue teamem, przyjrzyjmy się umiejętnościom, na które organizacje powinny zwracać uwagę podczas rekrutacji. Pomoże to w zatrudnieniu właściwych kandydatów i umieszczeniu ich na odpowiednich stanowiskach.

Umiejętności wymagane do pracy w zespole niebieskim

Członkowie zespołów niebieskich pracują w określonym wcześniej celu, aby zabezpieczyć infrastrukturę sieci biznesowej i wzmocnić poziom jej zabezpieczeń cybernetycznych. Stosowane przez nich metodologie i strategie obrony sieci oraz systemów przed cyberatakami przeplatają się ze sobą. Kierownictwo musi dobrze rozumieć cele i funkcje członków zespołu niebieskiego.

Chęć do nauki i zorientowanie na szczegóły

Aby uniknąć pozostawienia luk w zabezpieczeniach infrastruktury firmy, wymagana jest dbałość o szczegóły. Równie pożądana jest wiedza na temat tworzenia niestandardowych narzędzi. Pisanie oprogramowania wymaga dużo praktyki i chęci do ciągłego uczenia się.

Dogłębna znajomość sieci i systemów

Dogłębne zrozumienie systemów komputerowych, protokołów, bibliotek i dobrze znanych TTP toruje drogę do sukcesu specjalisty cyberbezpieczeństwa. Zdolność blue teamu do zaznajomienia się ze wszystkimi systemami i nadążania za postępem technologicznym ma tutaj kluczowe znaczenie. Wiedza o tym, jak pracować z serwerami i bazami danych, zapewni dodatkowe możliwości, jeśli chodzi o odkrywanie ich wad. Równie istotna jest znajomość tego, jak korzystać z pakietów oprogramowania, które pozwalają analitykom SOC monitorować infrastrukturę sieciową pod kątem nieoczekiwanych lub potencjalnie wrogich działań. SIEM to rozwiązanie analizujące incydenty bezpieczeństwa w czasie rzeczywistym. Otrzymuje dane z wielu źródeł i analizuje je według zadanego zestawu kryteriów. Blue teamy, podobnie jak red i purple, wykorzystują różnorodne technologie bezpieczeństwa, w tym honeypoty, sandboksy, XDR i NGAV, frameworki wykrywania zagrożeń i rozwiązania SIEM. Poniżej znajduje się lista niektórych najpopularniejszych narzędzi z dziedziny cyberbezpieczeństwa, które są często używane przez te zespoły do pracy operacyjnej:

- Splunk,
- Haktrails,
- Cuckoo Sandbox,
- SecurityTrails API.

Nieszablonowe i innowacyjne myślenie

Główną cechą zespołu ds. cyberbezpieczeństwa jest umiejętność nieszablonowego myślenia oraz ciągłe opracowywanie nowych narzędzi i podejść w celu poprawy bezpieczeństwa organizacji. Aby nadążyć za atakującymi, specjaliści ds. bezpieczeństwa cybernetycznego muszą stale myśleć nieszablonowo i odkrywać nowe narzędzia i podejścia. Zespoły ds. bezpieczeństwa cybernetycznego wdrażają różnorodne narzędzia w ramach swoich działań, w tym narzędzia do rekonesansu, eskalacji uprawnień i zagrożeń ze strony kanałów bocznych oraz eksfiltracji.

Umiejętność przekraczania barier w wykonywaniu zadań

Analitycy SOC zawsze wykrywają dużą liczbę **fałszywie pozytywnych alarmów** (ang. *False Positives*, **FP**). Aby zmniejszyć ich liczbę, starsi analitycy SOC muszą czasami przekroczyć kilka barier. Muszą skonfigurować reguły obejmujące wiele kryteriów filtrowania,

co czasami staje się przytłaczające. Pomocna może tu być mapa myśli (ang. *mind map*) wszystkich przypadków użycia, która umożliwi specjalistom połączenie różnych przypadków użycia skonfigurowanych w narzędziach SOC. Muszą oni bowiem sprawdzić, czy pewne reguły, które zostały skonfigurowane do obsługi przypadku użycia, nie zastępują innych reguł. Bardzo ważne jest także rozwiązywanie konfliktów w możliwie najkrótszym czasie bez wpływu na SLA (ang. *Service Level Agreement* — umowa o gwarantowanym poziomie świadczenia usług). W wielu przypadkach jest to jak szukanie igły w stogu siana.

Wykształcenie, kwalifikacje i certyfikaty

Role członków blue teamu nie wymagają żadnych drogich certyfikatów ani stopnia naukowego. Dla każdego zespołu niebieskiego w organizacji najważniejsze są praktyczne umiejętności i predyspozycje profesjonalistów. Jednak posiadanie odpowiednich kwalifikacji akademickich i/lub certyfikatów może być w trakcie rekrutacji wskazywane jako pożądane na różnych stanowiskach. Wielu członków zespołów niebieskich jest samoukami i nie wymaga prowadzenia za rękę. Jednak niektóre organizacje mogą szukać pewnych konkretnych umiejętności w CV kandydatów do blue teamu przed zaproszeniem ich na rozmowę kwalifikacyjną. W związku z tym stopnie akademickie — choć nie są wymogiem — mogą jednak pomóc dostać się na krótką listę zaproszonych na rozmowę wstępną w danej organizacji. Organizacje takie jak CompTIA, SANS, EC-Council, ISC2, ISACA i inne wydają popularne certyfikaty w zakresie kompetencji zespołu niebieskiego. Istnieje też wiele innych programów szkoleniowych i certyfikatów specyficznych dla technologii/dostawcy, które pomagają zespołom niebieskim doskonalić praktyczne umiejętności w zakresie danego produktu zabezpieczającego.

W tej części wyjaśniliśmy, jakie umiejętności są potrzebne i jakie osoby zatrudnić. To jednak nie wystarczy. W dalszej kolejności powiemy, w jaki sposób zadbać o rozwój i utrzymanie talentów.

Rozwój i utrzymanie talentów

Jednym z najtrudniejszych zadań w życiu każdego kierownika ds. bezpieczeństwa jest znalezienie oddanego, entuzjastycznego i myślącego członka zespołu. Powszechnie wiadomo, że na całym świecie brakuje specjalistów. Dlatego przyciągnięcie i utrzymanie odpowiednich osób w swojej organizacji jest jeszcze ważniejsze. Nie ma w tym zakresie jednego słusznego rozwiązania. Przyjrzyjmy się kilku pomysłom, które może wdrożyć kierownictwo.

Laboratoria cybernetyczne

Przede wszystkim można zachęcić pracowników do założenia domowego laboratorium lub skorzystania z laboratorium udostępnionego przez firmę. Laboratoria mogą służyć do testowania sytuacji, które mogłyby się rzeczywiście przydarzyć, a także do ćwiczenia

i doskonalenia nowych umiejętności. Dla zdecydowanej większości osób nauka praktyczna jest najlepszym sposobem zdobywania doświadczenia, a w laboratorium nie ma szans na wprowadzenie ryzyka do środowiska produkcyjnego.

Capture-the-Flag i hackathony

Zawody **Capture-the-Flag** (**CTF**) mogą być organizowane w miejscu pracy. Takie wyzwania pomagają w treningu pozwalającym na rozwinięcie kompleksowych umiejętności w wielu zakresach oraz w budowaniu zespołu i komunikacji. CTF i hackathony są najlepszymi wydarzeniami w trakcie większości młodych i tętniących życiem konferencji poświęconych bezpieczeństwu cybernetycznemu. Oferują również każdej firmie jeden z najlepszych sposobów na znalezienie nowych talentów, jeśli chce ona zatrudnić lub rozszerzyć zespół ds. bezpieczeństwa. Uczestnicy demonstrują nie tylko swoją wiedzę, ale także komunikatywność, umiejętność pracy w zespole oraz chęć pomocy i edukacji innych.

Projekty badawczo-rozwojowe

Inną możliwością jest opracowanie własnego projektu lub znalezienie odpowiednich projektów ze społeczności open source. Większość projektów open source wymaga dokumentacji lub innej pomocy w różnych obszarach bezpieczeństwa. Specjaliści cyberbezpieczeństwa mogą uznać, że motywuje ich to do zaprezentowania swoich umiejętności na arenie publicznej. Tak więc organizacja, która pozwala swoim pracownikom spędzać czas na takich projektach społecznościowych, może być postrzegana jako magnes przyciągający talenty.

Zasięg społeczności

Umożliwienie pracownikom wzięcia udziału w spotkaniach branżowych, a nawet lokalnych spotkaniach oraz zachęcanie ich do tego to świetny sposób na zaszczepienie nawyku ciągłego uczenia się. Sam udział w konferencji ma swoje zalety, ale pracownicy mogą pójść dalej, przygotowując przemówienia i prezentacje, a nawet zgłaszając się jako wolontariusze do pomocy przy wydarzeniach. Co więcej, daje to pracownikom możliwości nawiązywania kontaktów i budowania relacji. Jest to kluczowa umiejętność, zwłaszcza dla personelu **Cyber Threat Intelligence** (**CTI**).

Mentoring

Kierownictwo firmy może pomóc, udzielając wsparcia młodym i nowym talentom. Mentoring może być wspaniałym doświadczeniem edukacyjnym zarówno w pracy, jak i poza nią. Dzięki niemu zespół ds. bezpieczeństwa dowiaduje się więcej o organizacji i odczuwa większą więź z kierownictwem wyższego szczebla. Co więcej, motywuje to pracowników do budowania ścieżki kariery i sieci kontaktów w całej organizacji i liniach biznesowych.

Ciągła, nieograniczana nauka

Umiejętności wymagane do ochrony sieci firmowej stale ewoluują, ponieważ branża cyberbezpieczeństwa dostosowuje się do zarządzania pojawiającymi się zagrożeniami za pomocą nowych taktyk, technik i procedur. Niektóre badania pokazują, że w ciągu zaledwie trzech miesięcy cyberprofesjonaliści, którzy nie kontynuują nauki, pozostają w tyle i odnoszą znacznie mniejsze sukcesy. Taktyki stosowane przez nieetycznych hakerów cały czas ewoluują; czy blue team nie powinien zatem również się zmieniać?

Pomaganie pracownikom w ciągłym uczeniu się ma kluczowe znaczenie dla zapewnienia bezpieczeństwa organizacji w dzisiejszej szybko zmieniającej się cyberprzestrzeni. Udziałowcom zaleca się ciągłe szkolenia w zakresie cyberbezpieczeństwa, podkreślając wysoki **zwrot z inwestycji** (ang. *Return on Ivestment*, **RIO**) w zakresie bezpieczeństwa i efektywności pracy. Ciągłe i nieograniczane szkolenia w zakresie cyberbezpieczeństwa pozwalają zespołom niebieskim rozwijać się oraz odświeżać swoją wiedzę podczas pracy i być na bieżąco z trendami w branży. Co więcej, cyberprofesjonaliści, którzy przeszli szkolenie w miejscu pracy, najlepiej radzą sobie z obroną przed atakami w czasie rzeczywistym. Częste szkolenia i certyfikaty umożliwiają zespołowi niebieskiemu szybkie wykrywanie przypadków reagowania na incydenty i skuteczne radzenie sobie z nimi. Wiele firm inwestuje w nowe, zaawansowane rozwiązania zabezpieczające, aby wyprzedzać cyberzagrożenia. Jednak ze względu na brak czasu lub zasobów, aby zrozumieć, jak ich używać, cyberprofesjonaliści niekiedy nie są w stanie w pełni ich docenić lub zastosować technologii, przez co nie mają przewagi nad cyberprzestępcami. Aby korzystać z nowych technologii, cybereksperci muszą się stale uczyć nowych podejść i być na bieżąco.

Podsumowanie

Ustanowienie programu ochrony nie jest prostym zadaniem. Wiele projektów jest dysfunkcyjnych lub nie istnieje, co wpływa na obecny stan bezpieczeństwa biznesu. Ten rozdział powinien pomóc Ci zrozumieć, czym są blue, red i purple teamy. Skuteczny program cyberbezpieczeństwa wymaga umiejętności organizacyjnych, kompetentnego, pracowitego personelu, silnego przywództwa i dogłębnego zrozumienia niszy cyberbezpieczeństwa.

W tym rozdziale omówiliśmy potrzebne umiejętności i wskazaliśmy rodzaje specjalistów, których należy rekrutować, a co ważniejsze, podpowiedzieliśmy, jak rozwijać i zachowywać te talenty. W następnym rozdziale omówimy, jak zarządzać takim zespołem, a także jakie wskaźniki i metryki należy ustawić, aby mieć pewność, że zespół dobrze sobie radzi i zapewnia organizacji jak największą wartość.

Idealny system i strategia obronna? Zaprojektuj i zbuduj!

W obecnych czasach praktycznie każda organizacja przechowuje dane w miejscu, które połączone jest z jakąś siecią. Zapewnia to ich dostępność, równocześnie jednak naraża je na zagrożenia. Niepożądany dostęp do danych może oznaczać katastrofę dla organizacji, stąd tak ważna jest praca zespołu niebieskiego. Blue team identyfikuje podatności w infrastrukturze oraz aplikacjach i wdraża procedury bezpieczeństwa.

Ta książka zapewni Ci wiedzę, dzięki której z powodzeniem utworzysz blue team w swojej organizacji. Dowiesz się, z jakich defensywnych środków cyberbezpieczeństwa warto skorzystać i jakimi metodami ocenić skuteczność aktualnego stanu zabezpieczeń, dogłębnie zrozumiesz także sposoby działania cyberprzestępców. Lekturę rozpoczniesz od krótkiego przeglądu znaczenia, zadań i składu zespołu niebieskiego, poznasz też ważne techniki i najlepsze praktyki w defensywnej ochronie cyberbezpieczeństwa. Nauczysz się korzystać z metodologii NIST w celu utworzenia planów reagowania na incydenty i dowiesz się, jak je testować. Znajdziesz tutaj również wskazówki, dzięki którym dopasujesz swoje działania ściśle do potrzeb organizacji.

Dzięki tej książce:

- zrozumiesz rolę blue teamu w organizacji i sposób jego działania
- dowiesz się, jak wygląda zarządzanie ryzykiem z perspektywy zespołu niebieskiego
- nauczysz się tworzenia skutecznych strategii obronnych
- dowiesz się, jak ułożyć dobry program nadzoru
- przekonasz się, jak kontrole wewnętrzne przyczyniają się do zminimalizowania ryzyka

Kunal Sehgal od ponad 15 lat zajmuje się cyberbezpieczeństwem, współpracuje z organami ścigania na całym świecie. Specjalizuje się w doradztwie dotyczącym poprawy poziomu bezpieczeństwa.

Nikolaos Thymianis zajmuje się bezpieczeństwem informacji w szpitalach i dużych firmach farmaceutycznych. Jest doradcą na Uniwersytecie w Pireusie i uznanym prelegentem.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-0456-9
9 788328 904569
Cena: 59,00 zł