استراتژی‌های تیم آبی

تالیف : میلاد چراغی

استراتژی‌های تیم آبی

میلاد چراغی

https://t.me/CheraghiMilad

www.linkedin.com/in/miladcheraghi

سخن مترجم

بمانَد سال‌ها این نظم و ترتیب
ز ما هر ذرّه خاک افتاده جایی

غرض نقشیست کز ما باز ماند
که هستی را نمی‌بینم بقایی

مگر صاحب‌دلی روزی به رحمت
کند در کار درویشان دعایی

سعدی

مقـــدمه

این کتاب شما را با مفهوم تیم آبی و نحوه عملکرد آن‌ها آشنا می‌کند. نگاهی به تاریخچه تشکیل تیم آبی و تأثیر آن بر کسب‌وکارها صورت گرفته و به حوزه‌های مختلفی که دفاع در آن‌ها اهمیت دارد، مانند امنیت ابر و امنیت شبکه، اشاره خواهد شد. همچنین، در این کتاب یاد خواهید گرفت چگونه یک تیم آبی را ایجاد کنید.

فهرست مطالب

1

ایجاد برنامه دفاعی

همانطور که حملات سایبری در همه کشورها و صنایع افزایش می‌یابد، برخورداری از توان دفاعی برای هر سازمانی یک ضرورت مطلق است. با این حال، راه‌اندازی چنین تخصصی و دستیابی به سطح مناسبی از بلوغ، نیازمند ترکیب صحیحی از فناوری، فرآیند و افراد است.

این نقشه راه، ممکن است برای کسانی که تازه شروع کرده‌اند، کمی دلهره‌آور و طاقت‌فرسا به نظر برسد. هدف این کتاب، کمک و راهنمایی به سازمان‌ها و شرکت‌هایی است که قصد شروع این مسیر را دارند تا تمامی جنبه‌های یک برنامه دفاعی تیم آبی به‌خوبی درک شود و هیچ نقطه کوری باقی نماند.

متخصصان امنیت سایبری که تحت عنوان تیم آبی شناخته می‌شوند، آسیب‌پذیری‌های مختلف امنیتی را در زیرساخت و برنامه‌های سازمان شناسایی می‌کنند. این تلاش‌ها به پچ کردن و پیاده‌سازی رویه‌ها و کنترل‌های امنیتی مختلف کمک می‌کنند. آن ها معمولاً توانایی تفکر خلاق و پاسخ سریع به طیف گسترده‌ای از حوادث و رخدادهای سایبری را دارند. همچنین آنها مسئول حفاظت از نهادهای تجاری در برابر ریسک‌ها و تهدیدات سایبری هستند. در این فصل ما در خصوص عناوین زیر صحبت خواهیم کرد:

- سازمان ها چگونه از اجرای رویکرد تیم آبی نفع می برند؟
- ترکیب بندی تیم آبی
- تیم قرمز
- تیم بنفش
- اطلاعات تهدید سایبری
- مهارت های مورد نیاز برای حضور در یک تیم آبی
- رشد و حفظ استعدادها

سازمان ها چگونه از اجرای رویکرد تیم آبی نفع می برند؟

پیش از آنکه شروع کنیم، درک این نکته مهم است که یک سازمان از ایجاد یک تیم آبی چه منافعی می‌تواند به دست آورد. این فصل بر روی انتظاراتی که سازمان‌ها از راه‌اندازی یک تیم آبی می‌توانند داشته باشند تمرکز می‌کند و نحوه اقدامات عملی را به صورت گام به گام برای دستیابی به موفقیت توضیح می‌دهد.

ارزیابی ریسک

در گام نخست، توصیه می‌شود سازمان‌ها ریسک‌ها و تهدیداتی را که ممکن است بر دارایی‌های سازمانی آن‌ها در سطح جهانی تأثیر بگذارد، شناسایی کنند. تیم آبی با انجام ارزیابی ریسک، می‌آموزد که چگونه و در برابر چه نوع تهدیداتی باید از سازمان محافظت کند. این تیم معمولاً توصیه می‌کند که کنترل‌های امنیتی سخت‌گیرانه‌ای پیاده‌سازی شده و رویه‌های استانداردی به‌منظور ارتقای وضعیت امنیتی سازمان تدوین گردد. در بسیاری از موارد، آن‌ها ساختار برنامه‌های آموزشی برای افزایش آگاهی امنیتی کاربران نهایی را نیز طراحی می‌کنند. این اقدامات به سازمان‌ها کمک می‌کند تا دارایی‌های حیاتی خود را شناسایی کرده و نمایه تهدید مربوط به هر دارایی و همچنین کل سازمان را به‌درستی درک کنند.

پایش و نظارت

پایش و نظارت از وظایف اصلی اعضای تیم آبی است؛ آن‌ها این وظایف را به دقت برای کسب‌وکارهای خود انجام می‌دهند. سازمان‌ها از اعضای تیم آبی توصیه‌هایی برای تهیه، استقرار و راه‌اندازی ابزارهای مختلف پایش امنیتی دریافت می‌کنند. این ابزارها به سازمان‌ها امکان می‌دهند تا اطلاعات مربوط به انواع دسترسی‌ها و مجوزهایی که کاربران و کارکنان در زیرساخت شبکه دارند را ثبت کنند. تمام فعالیت‌های کاربران ثبت می‌شود و فعالیت‌های مشکوک براساس قوانینی که در ابزارهای مختلف امنیتی تنظیم شده‌اند، هشدارهایی را ایجاد می‌کنند.

بررسی‌های روزانه – بررسی تنظیمات DNS و فایروال، انجام ارزیابی‌های روزانه انطباق در داشبوردهای ابزارهای مختلف مستقر در سازمان، و موارد دیگر- از جمله وظایف کلیدی (KRA)

اعضای تیم آبی محسوب می‌شوند. این تیم همچنین انواع مختلفی از ارزیابی‌های آسیب‌پذیری داخلی و خارجی را در سطح شبکه انجام می‌دهد. در برخی موارد، اعضای تیم آبی در اولویت‌بندی آسیب‌پذیری‌های شناسایی‌شده در گزارش‌های آزمون نفوذ و ارائه راهکارهایی برای رفع آن‌ها مشارکت دارند. آن‌ها در اسکن شبکه سازمانی به‌منظور شناسایی آسیب‌پذیری‌ها و تحلیل بسته‌های ضبط‌شده شبکه برای شناسایی ترافیک مشکوک ورودی یا خروجی، دارای تخصص هستند.

کنترل‌های امنیتی

اعضای تیم آبی همچنین مسئول پیاده‌سازی انواع مختلف کنترل‌های امنیتی فنی بر روی دارایی‌های حیاتی سازمان هستند. از این‌رو، لازم است ابتدا اجزای حیاتی شبکه در سازمان شناسایی و دسته‌بندی شوند. سازمان‌ها می‌توانند از پایگاه داده مدیریت پیکربندی (CMDB) برای مستندسازی تغییرات انجام‌شده در پیکربندی دارایی‌ها استفاده کنند. همچنین، CMDB نقش مهمی در متمرکزسازی اطلاعات مربوط به تمام اجزای زیرساخت شبکه ایفا می‌کند. دارایی‌هایی که در صورت وقوع حمله سایبری ممکن است منجر به توقف کامل کسب‌وکار شوند، به‌عنوان دارایی‌های حیاتی طبقه‌بندی می‌شوند. اغلب این دارایی‌ها با به‌کارگیری کنترل‌های امنیتی پیشرفته، سخت‌سازی می‌شوند.

علاوه بر ارزیابی ریسک، اعضای تیم آبی مطالعات ارزیابی تأثیر (Impact Assessment) را نیز انجام می‌دهند. این مطالعات شامل محاسبه تأثیر احتمالی انواع حملات سایبری بر دارایی‌های حیاتی مشخص و بررسی پیامدهای ناشی از از کار افتادن این دارایی‌ها در یک بازه زمانی معین بر روند کسب‌وکار است. چنین اختلالی می‌تواند به‌طور جدی عملیات تجاری را در مقیاسی وسیع تحت تأثیر قرار دهد. از این‌رو، ریسک‌ها و تهدیداتی که بر هر یک از دارایی‌های حیاتی اثر می‌گذارند، به‌طور دقیق مستندسازی می‌شوند. همچنین، اسکن‌های منظم برای ارزیابی آسیب‌پذیری‌ها، به‌ویژه آسیب‌پذیری‌های افشا شده عمومی مانند آسیب‌پذیری‌های مشترک و افشاها (CVE) و شمارش ضعف‌های مشترک (CWE)، برای این دارایی‌ها برنامه‌ریزی و اجرا می‌شوند.

اعضای تیم آبی در ارزیابی ریسک‌ها و ارائه گام‌های اصلاحی برای کاهش آن‌ها مهارت دارند. اغلب آسیب‌پذیری‌های حیاتی و سطح بالا در کوتاه‌ترین زمان ممکن وصله (Patch) می‌شوند. همچنین، برنامه‌ای از سوی تیم آبی اجرا می‌شود که هدف آن پیاده‌سازی کنترل‌های امنیتی برای کاهش تأثیر آسیب‌پذیری‌هایی است که هنوز وصله‌ای برای آن‌ها منتشر نشده است.

گزارش دهی و ارائه توصیه‌ها به مدیریت

تیم اجرایی باید تصمیم بگیرد که آیا کنترل‌های امنیتی موجود، پاسخگوی سطح مورد نیاز از محافظت هستند یا خیر. اعضای تیم آبی سندی از ریسک‌های شناسایی‌شده‌ای که کسب‌وکار با آن‌ها مواجه است تهیه می‌کنند. همچنین ممکن است تجزیه‌وتحلیل هزینه-فایده‌ای برای مدیریت انجام دهند تا تنها کنترل‌های امنیتی ای پیشنهاد شوند که از نظر فنی و اقتصادی ضروری تشخیص داده می‌شوند.

برای مثال، ممکن است تیم آبی به این نتیجه برسد که شبکه شرکت در برابر حملات توزیع‌شده منع سرویس (DDoS) آسیب‌پذیر است. حملات DDoS با ایجاد ترافیک سنگین و ارسال حجم بالایی از درخواست‌ها به سرورهای سازمان، دسترسی کاربران واقعی به خدمات را مختل می‌کنند. در چنین شرایطی، اختلال در دسترسی به سرویس‌ها می‌تواند منجر به از دست رفتن درآمد و آسیب جدی به کسب‌وکار شود. هرچه زمان بیشتری صرف شود تا تیم شبکه بتواند یک زیرشبکه خاص از آدرس‌های IP مخرب را شناسایی و مسدود کند، میزان خسارت وارده افزایش خواهد یافت. این نوع حملات می‌توانند عملکرد شبکه سازمانی را به‌شدت مختل کنند.

در چنین موقعیت‌هایی، تیم آبی نه‌تنها اقدام به تحلیل حمله و مسدودسازی آدرس‌های IP کنترل و فرمان (C2) مهاجمان می‌کند، بلکه ارزیابی تأثیر حمله را نیز انجام می‌دهد. برای پیشگیری از حملات DDoS یا سایر حملات منع سرویس (DoS)، اعضای تیم آبی پیشنهاد می‌دهند که راه‌حل‌های امنیتی پیرامونی در زیرساخت شبکه مستقر شوند. این راه‌کارها به‌طور قابل توجهی احتمال تأثیرگذاری حملات DDoS بر عملکرد سازمان را کاهش می‌دهند. اگرچه این ابزارها نمی‌توانند مانع آغاز یک حمله شوند، اما می‌توانند تأثیر آن بر شبکه کسب‌وکار را تا حد زیادی خنثی کنند.

راه‌حل‌های امنیتی مانند فایروال‌های پیرامونی، توازن‌دهنده‌های بار (Load Balancers) و فایروال‌های برنامه‌های وب (WAF)، نقش مهمی در شناسایی و جلوگیری از تأثیر حملات DoS بر شبکه سازمانی ایفا می‌کنند.
راه‌اندازی یک تیم آبی مزایای متعددی برای سازمان به همراه دارد؛ آنچه در این بخش ارائه شد، تنها مروری کلی بر مزایای رایج این تیم‌ها بود. در ادامه، تمرکز ما بر مهارت‌ها و توانمندی‌هایی خواهد بود که برای استخدام در چنین تیمی مورد نیاز هستند.

ترکیب بندی تیم آبی

تیم آبی شامل افرادی با مجموعه‌ای متنوع از مهارت‌ها است. ترکیب تیم بسته به نیازهای سازمان متفاوت است. در این بخش، به بررسی چند نقش معمول که معمولاً در این تیم وجود دارند، می‌پردازیم.

تحلیلگران

یک نقش ابتدایی در امنیت سایبری که به عنوان تحلیلگر مرکز عملیات امنیت (SOC) شناخته می‌شود، یک تحلیلگر امنیت سایبری که همچنین به عنوان تحلیلگر تریاژ نیز شناخته می‌شود، به هشدارهای مربوط به حوادث با شدت خاص پاسخ می‌دهد و شواهد را بررسی می‌کند. این نقش به صورت واکنشی عمل می‌کند. سازمان‌ها معمولاً نقش‌های سطح ۱ (L1)، سطح ۲ (L2) و سطح ۳ (L3) را در SOC دارند. L1 نقش تحلیلگر مبتدی است، در حالی که L3 نقش ارشدترین تحلیلگر در SOC است. در بیشتر موارد، سطوح بالاتر شماره‌گذاری شده نشان‌دهنده افزایش سطح مسئولیت و نیازهای تجربی هستند.

مرکز عملیات امنیت ترافیک شبکه را برای رفتارهای غیرعادی یا مشکوک نظارت می‌کند. برخی فعالیت‌های مشکوک ممکن است نشان‌دهنده وجود نهادهای مخرب یا برنامه‌های مخربی مانند تروجان‌ها و باج‌افزارها در شبکه باشند. تحلیلگران ارشد، هشدارهای تولید شده توسط

راهکار مدیریت حوادث و رویدادهای امنیتی (SIEM) مانند Splunk، IBM QRadar، Logrhythm و دیگران را بررسی می‌کنند. تحلیلگران روی تریاژ و شناسایی رویدادهای مشکوک کار می‌کنند و تعیین می‌کنند که آیا هشدارها مثبت کاذب هستند یا مثبت واقعی. در صورت هشدارهای مثبت واقعی، روش عملیاتی استاندارد (SOP) طبق کتاب‌های راهنما یا دستورالعمل‌ها دنبال می‌شود. تحلیل و بررسی‌هایی که توسط تحلیلگران مبتدی انجام می‌شود، به ایجاد زمینه برای حوادث امنیتی رخ داده کمک می‌کند. آن‌ها همچنین شدت یک مشکل امنیتی را تعیین کرده و رتبه‌بندی ریسک مناسبی به آن اختصاص می‌دهند. حوادث امنیتی با شدت بحرانی و به طور کلی بالا، بلافاصله به پاسخ‌دهنده حوادث (IR) در تیم SOC ارجاع داده می‌شوند.

پاسخ‌دهنده حوادث

پاسخ‌دهنده حوادث که به عنوان تحلیلگر پاسخ‌دهی به حوادث (IR) نیز شناخته می‌شود، وظیفه ارزیابی این موضوع را دارد که آیا یک هشدار گزارش شده به حمله سازمانی یا تهدیدی پایدار برای شبکه شرکت اشاره دارد یا خیر. آن‌ها اطمینان حاصل می‌کنند که این تهدید در سریع‌ترین زمان ممکن مهار شود و سازمان بتواند طبق برنامه‌های تعریف شده به آن پاسخ دهد. پاسخ‌دهندگان حوادث معمولاً دامنه یک حمله سایبری را بررسی می‌کنند.

بر اساس گستردگی مشکل امنیت سایبری، پاسخ‌دهندگان حوادث استراتژی اصلاحی را تدوین می‌کنند. این شامل بررسی ویژگی‌های حادثه می‌شود. این بررسی شامل دارایی‌های کسب‌وکار هدف قرار گرفته شده توسط بدافزار و همچنین انواع فعالیت‌های مخرب انجام شده توسط بدافزار می‌شود. سپس، پاسخ‌دهندگان حوادث اقدام مناسب را توصیه می‌کنند. آن‌ها با تیم‌های مربوطه، اصلاحات را پیاده‌سازی می‌کنند، مانند ایجاد تیکت های IT برای بازیابی مجدد سیستم‌های آسیب‌دیده.
اغلب، پاسخ‌دهندگان حوادث با فشار برای اجباری کردن آموزش آگاهی امنیتی کاربران نهایی توسط CISO مواجه می‌شوند. آن‌ها همچنین مدیران اجرایی را به موقع از دامنه یک نقض داده مطلع می‌کنند.

شکارچی تهدید

این نقش اغلب به عنوان تحلیلگر تهدید یا محقق تهدید نیز شناخته می‌شود. کار شکارچی تهدید به صورت پیش‌دستانه است. آن‌ها به طور منظم تهدیدات و ریسک‌ها را پژوهش می‌کنند تا از جدیدترین تهدیدات آگاه باشند. همچنین آن‌ها به مطالعه تکامل و ساختار تهدیدات می‌پردازند. شکارچیان تهدید اغلب قوانین کدنویسی را طراحی می‌کنند که هشدارهایی را در راهکار مدیریت حوادث و رویدادهای امنیتی (SIEM) شرکت برای تهدیدات سایبری خاص ایجاد می‌کند.

شکارچیان تهدید در پیکربندی و نظارت بر پلتفرم‌های مختلف اطلاعات تهدید (مانند IBM X-Force، Alienvalult OTX، VirusTotal و غیره) برای انجام تحقیقات پیش‌دستانه در چرخه حیات تهدیدات مهارت دارند. آن‌ها ارزیابی می‌کنند که آیا تهدیدات جدید و نوظهور براساس پارامترهای مختلفی مانند صنایع مورد هدف، آسیب‌پذیری‌های مورد سوءاستفاده قرار گرفته و تاکتیک‌ها، تکنیک‌ها و روش‌های حمله (TTPs) بیشترین خطر را برای شرکتشان فراهم می‌کنند یا خیر. شکارچیان تهدید اغلب تنظیمات پیکربندی سیستم را برای پاسخ به ریسک‌های سایبری کشف شده پیاده‌سازی می‌کنند. تحلیل تهدیدات و ریسک‌های سایبری در زمان واقعی زمانی که اطلاعات تهدید دریافتی بیشتر از توان پردازش منابع انسانی موجود است، می‌تواند طاقت‌فرسا باشد. بنابراین، شکارچیان تهدید از اتوماسیون در فناوری‌های امنیتی برای شناسایی خودکار رفتارهای خاص برخی تهدیدات استفاده می‌کنند. آن‌ها زیرساخت شبکه سازمانی را تقویت و حساس‌سازی می‌کنند تا در برابر حملات سایبری احتمالی مقاومت کند.

فرض کنیم که یک تهدید سایبری جدید به صورت باج‌افزار به تازگی پدیدار شده است (مانند Lockbit 2.0 یا BlackMatter). شکارچی تهدید این خطر را بررسی کرده و از اتوماسیون برای جلوگیری از نفوذ آن به شرکت و شناسایی آن در صورت نفوذ استفاده می‌کند.

یک کاندیدا برای نقش شکارچی تهدید باید در نقش‌های کاری تحلیلگر SOC و پاسخ‌دهنده حوادث (IR) تجربه داشته باشد و در شبکه و مدیریت سیستم‌ها و رایانه‌ها مهارت داشته باشد. همچنین، آشنایی با منابع مختلف اطلاعات تهدید در سطح وب و همچنین وب تاریک مفید

است. داشتن درک عمیق از تهدیدات سایبری خاص به بخش‌های کسب‌وکار اغلب به کاندیدا در بازار کار اطلاعات تهدید و شکار تهدید مزیت رقابتی می‌دهد. یک شکارچی تهدید خوب یا تحلیلگر اطلاعات تهدید (TIA) در کسب اطلاعات تهدید پیش‌دستانه و عملی از هر تعداد منبع در سطح وب و همچنین وب تاریک، از جمله سرورهای IRC و انجمن‌ها، مهارت دارد. یک شکارچی تهدید خوب باید بتواند روش‌های فنی و غیر فنی مناسب را انتخاب کند و دانش استفاده از چارچوب‌های مختلف اطلاعات تهدید را در اختیار داشته باشد.

مشاور امنیت

مشاوران امنیتی معمولاً به صورت قراردادی استخدام می‌شوند و در طول چرخه حیات پروژه وظایف مختلفی را بر عهده می‌گیرند. همچنین ممکن است از خارج از سازمان برای به ارمغان آوردن منبع قابل اعتماد از دانش یا تخصص در یک ابزار خاص یا حوزه‌ای از امنیت استخدام شوند. آن‌ها اغلب به عنوان کارشناسان در حوزه دانش خود شناخته می‌شوند. اصطلاح دیگری که معمولاً برای نام‌گذاری مشاوران امنیتی استفاده می‌شود، کارشناسان موضوعی (SMEs) است. مشاور استراتژی امنیتی و مشاور عملیات امنیتی چند مثال از نقش‌های تخصصی هستند.

مدیر امنیت

مدیر امنیت با تحلیلگر SOC یکسان نیست. با این حال، اغلب دیده شده که سازمان‌ها مدیران امنیت را به عنوان تحلیلگران SOC سطح ۴ (L4) در نظر می‌گیرند که وظیفه آن‌ها دانلود، نصب، پیکربندی، استقرار و راه‌اندازی ابزارهای مختلف امنیتی در SOC است. آن‌ها همچنین مسئول به‌روزرسانی این ابزارها هنگام وصول به‌روزرسانی‌های ارائه شده توسط فروشندگان هستند. این شغل مشابه شغل مدیر سیستم است، اما با تمامی ابزارهای امنیتی در SOC مانند SIEM، SOAR، AV-NGAV، EDR-XDR، DLP، هانی‌پات‌ها، حاکمیت ابر، WAF، فایروال، توازن‌دهنده‌های بار، IAM و AD، راه‌حل‌های نظارت بر سوءاستفاده و تخریب برند و موارد دیگر سروکار دارد. این شغل همچنین شامل اعمال پچ‌ها یا رفع اشکالات ارائه شده توسط فروشندگان ابزارهای مربوطه و پیکربندی ابزارهای امنیتی برای اطمینان از عملکرد بهینه می‌شود. آن‌ها اغلب با شکارچیان تهدید و پاسخ‌دهندگان حوادث همکاری می‌کنند تا اسکریپت‌ها و برنامه‌های امنیتی را ایجاد کنند که

برخی از وظایف امنیتی تکراری را اتوماتیک کنند. با این حال، آن‌ها مسئولیت بررسی رویدادها و حوادث امنیتی پرچم‌گذاری شده توسط ابزارهای امنیتی را ندارند.

مدیر هویت و دسترسی (IAM)

این نقش پشتیبانی مدیریت هویت و دسترسی (IAM) را به چندین بخش درون یک شرکت ارائه می‌دهد. مدیریت اختیارات و مجوزهای برنامه/سیستم، ورود یکپارچه (SSO)، گزارش‌دهی برنامه‌ها، و همکاری با توسعه‌دهندگان برای ادغام سیاست‌های مدیریت هویت و دسترسی برای برنامه‌ها و نرم‌افزارهای جدید از جمله مسئولیت‌های کلیدی یک مدیر IAM است. این حرفه‌ای‌ها تخصص ویژه‌ای در استفاده از ابزارهای مختلف IAM و همچنین مدیریت شبکه دارند.

تحلیلگر انطباق

یک تحلیلگر انطباق اغلب مسئول انجام ممیزی‌های داخلی یک شرکت یا کسب‌وکار است. آن‌ها بررسی می‌کنند و تأیید می‌کنند که آیا کسب‌وکار قوانین امنیتی، سیاست‌های حفظ حریم خصوصی، قوانین ملی حفظ حریم داده، یا هر قانون/مقررات قابل اجرا دیگر را رعایت می‌کند یا خیر. آن‌ها تجربه‌ای در تمامی نقش‌های مذکور دارند زیرا یک تحلیلگر انطباق باید به طور منظم با همه نقش‌های کاری دیگر به عنوان بخشی از بررسی‌های انطباقی گفتگو کند. آن‌ها گزارش‌های منظم از عدم انطباق‌های کشف شده در زیرساخت شبکه استخراج کرده و به مدیریت ارشد ارائه می‌کنند. علاوه بر این، آن‌ها به شرکت‌ها در آماده‌سازی برای ممیزی‌های خارجی که بسته به بخش کسب‌وکار ممکن است ضروری باشد، کمک می‌کنند (برای مثال، بهداشت و درمان، BFSI، انرژی و خدمات).

این بخش پوشش داد که سازمان‌ها برای تشکیل یک تیم آبی به چه چیزهایی نیاز دارند. بسته به نوع یا پیچیدگی یک سازمان، نقش‌های بیشتری برای در نظر گرفتن وجود دارد. با این حال، در این بخش، برخی از مهارت‌هایی که به طور معمول در هر سازمانی وجود دارند را پوشش دادیم. در بخش بعدی، به طور مختصر به تیم قرمز و تیم بنفش می‌پردازیم. این دو تیم ممکن است بخشی از تیم آبی نباشند، اما مهم است که بدانیم این تیم‌ها چه کاری انجام

می‌دهند. علاوه بر این، نقش تیم اطلاعات تهدید سایبری را نیز درک خواهیم کرد. این مجموعه مهارتی، معمولاً در تیم آبی قرار دارد، اما داشتن این تیم جدا از تیم آبی نیز رایج است.

تیم قرمز

تیم قرمز مانند هکرهایی عمل می‌کند که تلاش می‌کنند هرگونه نقطه ضعف احتمالی در شبکه کسب‌وکار را پیدا کرده و بهره‌برداری کنند. اعضای تیم قرمز شناخته شده‌اند که از تکنیک‌های مرسوم و نامرسوم برای کشف نقص‌ها در فناوری، افراد و فرآیندها استفاده کنند. بنابراین، معمولاً چنین مجموعه مهارتی خارج از حوزه تیم آبی وجود دارد. با این حال، برای درک بهتر، به طور مختصر به این نقش می‌پردازیم.

مأموریت تیم قرمز شامل جستجوی آسیب‌پذیری‌های شناخته شده‌ای است که قبلاً افشا شده‌اند و دارای شناسه CVE (آسیب‌پذیری‌ها و افشاهای مشترک) هستند. آن‌ها تست نفوذ بر زیرساخت شبکه کسب‌وکار انجام می‌دهند تا نقاط ضعف امنیتی ناشناخته را کشف کنند. این تیم‌ها ممکن است شبکه‌های بی‌سیم و اینترنت اشیا (IoT) و همچنین دستگاه‌های نقطه نهایی مانند لپ‌تاپ‌ها، رایانه‌های شخصی، موبایل‌ها، تبلت‌ها و غیره را نیز تست کنند. تست نفوذ سخت‌افزاری بر دستگاه‌های پوشیدنی IoT و دستگاه‌هایی که از بلوتوث استفاده می‌کنند نیز انجام می‌شود. هکرهای تیم قرمز ممکن است تلاش کنند تا با مهندسی اجتماعی کارکنان سازمان را به دام بیاندازند. این نوع هکرها اغلب نام مستعاری دارند که در محوطه شرکت فعالیت می‌کنند. آن‌ها در تشخیص و پیشنهاد کنترل‌های امنیتی لازم برای رفع نقص‌های امنیتی که از طریق کمبود تدابیر فیزیکی رخ می‌دهد، بسیار حیاتی هستند. نقاط نهایی و دستگاه‌های موبایل نیز در دامنه تست نفوذ یا نفوذ آن‌ها قرار دارند.

مسئولیت‌های دقیق تیم قرمز فراتر از محدوده این فصل است. با این حال، مهم است بدانیم که معمولاً تیم قرمز و تیم آبی با هم همکاری می‌کنند. برخی از زمینه‌هایی که در آن‌ها با هم کار می‌کنند عبارت اند از:

- ایجاد نقشه توپولوژی/سلسله مراتب شبکه زیرساخت کسب‌وکار برای تحلیل تعداد میزبان‌های در حال اجرا و وضعیت آن‌ها
- ارزیابی خدمات در حال اجرا و پورت‌های باز در آن سیستم‌ها
- شناسایی فروشنده، سیستم‌عامل و سایر جزئیات تجهیزات مربوطه
- شناسایی و بهره‌برداری از CVEها در سرورها، هاب‌ها، فایروال‌ها، روترها، سوئیچ‌های L2/L3، نقاط دسترسی Wi-Fi و سایر تجهیزات شبکه
- هک کردن انواع مختلف کنترل‌های امنیتی فیزیکی، مانند درب‌های شیشه‌ای، قفل‌های دیجیتال، شبکه‌های CCTV و گاهی اوقات پرسنل امنیتی

در برخی سازمان‌ها، راه‌اندازی یک برنامه باگ بانتی نیز عاقلانه است. باگ بانتی‌ها پاداش‌های نقدی یا جوایزی هستند که به هکرهای اخلاقی ارائه می‌شوند. هکرهای سراسر جهان به دنبال نقص‌ها هستند و در برخی موارد، از این راه زندگی می‌کنند. بسیاری از وب‌سایت‌ها، سازمان‌ها و شرکت‌های نرم‌افزاری برنامه‌های باگ بانتی ارائه می‌دهند که در آن‌ها کاربران می‌توانند برای گزارش باگ‌ها، به ویژه آن‌هایی که مربوط به آسیب‌پذیری‌های منطق کسب‌وکار و بهره‌برداری‌های امنیتی شبکه هستند، شناسایی و جبران شوند. باگ بانتی‌ها توسط شرکت‌ها برای پاداش دادن به شکارچیان باگ مستقل که نقص‌ها و نقاط ضعف امنیتی را پیدا می‌کنند و به طور اخلاقی و مسئولانه قبل از اینکه توسط عوامل تهدید سایبری بهره‌برداری شوند، گزارش می‌دهند. برنامه‌های بانتی معمولاً به همراه تست‌های نفوذ منظم استفاده می‌شوند تا شرکت‌ها بتوانند امنیت برنامه‌های خود را در طول چرخه توسعه آن‌ها ارزیابی کنند. برنامه‌های باگ بانتی به شرکت‌ها این امکان را می‌دهند تا از جامعه هکرها برای بهبود مستمر وضعیت امنیتی سیستم‌های خود استفاده کنند. این برنامه‌ها گروه متنوعی از هکرها با مجموعه‌های مهارتی و تخصص‌های مختلف را جذب می‌کنند، که به شرکت‌ها برتری نسبت به ارزیابی‌های آسیب‌پذیری که به کارکنان امنیتی کم‌تجربه متکی هستند، می‌دهد. بنابراین، به جای اینکه یک فرد یا یک تیم به تنهایی به دفاع سازمان حمله کند، قدرت جمعی جامعه به نفع سازمان استفاده می‌شود.

تیم بنفش

هدف اصلی تمرینات تیم قرمز و تیم آبی، بهبود وضعیت کلی امنیت سازمان است. اینجاست که مفهوم تیم بنفش وارد عمل می‌شود. تیم بنفش همیشه یک گروه مستقل نیست، هرچند ممکن است باشد. هدف تیم بنفش گرد هم آوردن تیم‌های قرمز و آبی و تشویق آن‌ها به همکاری و تبادل ایده‌ها برای ایجاد یک حلقه بازخورد قوی است.

هدف تیم بنفش توسعه قابلیت‌های تیم آبی در حالی است که نتایج تعاملات تیم قرمز را به حداکثر می‌رساند. یک شرکت بهترین عملکرد را دارد وقتی که تیم‌های قرمز و آبی برای تقویت وضعیت امنیتی سازمان همکاری کنند.

اول و مهم‌تر از همه، ارتباطات در این همکاری بسیار حیاتی است. برای انجام تمرینات، باید همیشه ارتباط بین تیم‌های مختلف وجود داشته باشد. به خاطر داشته باشید که هدف تیم آبی به‌روزرسانی با جدیدترین فناوری‌ها و اشتراک‌گذاری آن دانش با تیم قرمز است. این داده‌ها به بهبود امنیت سازمان کمک می‌کند. تیم قرمز باید از جدیدترین خطرات و تاکتیک‌های هک مورد استفاده توسط هکرها مطلع شود و باید تیم آبی را در این باره راهنمایی کند. هدف آزمون سازمان تعیین می‌کند که آیا تیم قرمز، تیم آبی را از آزمون‌های آینده مطلع می‌کند یا خیر. اگر هدف تقلید از یک سناریوی حمله دنیای واقعی باشد، ممکن است تیم قرمز پیش از زمان مشخصی تیم آبی را مطلع نکند تا مکانیزم‌های دفاع سایبری آن‌ها را آزمایش کند.

مدیریت باید تیم‌ها را به همکاری و ارتباط با یکدیگر تشویق کند. برای پیشرفت مستمر برنامه امنیتی، هماهنگی بهبود یافته بین هر دو تیم از طریق اشتراک منابع مؤثر، گزارش‌دهی و تبادل اطلاعات ضروری است.

اطلاعات تهدید سایبری

اطلاعات تهدید یک اصطلاح است که اغلب توسط بسیاری از حرفه‌ای‌ها استفاده می‌شود و شامل اطلاعات تاکتیکی، عملیاتی و استراتژیک می‌شود. منابع، مخاطبان و شکل های اطلاعات همگی متفاوت هستند. در اصل، هر اطلاعات تهدیدی که توسط مرکز عملیات امنیت (SOC)

دریافت می‌شود، در هر کسب‌وکاری، باید به صورت پیش‌دستانه قابل اقدام باشد. تیم آبی باید بتواند این اطلاعات را جذب کرده و از آن برای دفاع پیش‌دستانه از سازمان خود استفاده کند.

در مورد اصول اولیه، داده‌های تهدید شامل شاخص‌های مختلف تهدیدات سایبری مانند آدرس‌های IP، URLها یا هش‌های فایل است. این‌ها به عنوان شاخص‌های تهدید (IoTs) یا شاخص‌های نفوذ (IoCs) شناخته می‌شوند. از طرف دیگر، اطلاعات تهدید نوعی سابقه واقعی، پردازش شده و قابل اثبات است که بر اساس تحلیل، داده‌ها و اطلاعات را از منابع مختلف به هم متصل می‌کند تا الگوها را شناسایی کرده و بینش‌هایی ارائه دهد که برای سازمان مرتبط باشد. این اطلاعات به افراد و سیستم‌ها اجازه می‌دهد تا تصمیمات آگاهانه بگیرند و اقدامات مؤثری برای جلوگیری از نقض‌ها، رفع آسیب‌پذیری‌ها، بهبود وضعیت امنیتی شرکت و کاهش ریسک انجام دهند. اطلاعات استراتژیک معمولاً بر تاکتیک‌ها، تکنیک‌ها و روش‌های (TTPs) عاملان تهدید تمرکز دارد.
اغلب، چنین تیم‌هایی درون تیم آبی قرار دارند. به‌طور متناوب، سازمان‌های بزرگ ممکن است ترجیح دهند که این تیم‌ها به صورت جداگانه و به عنوان یک واحد مستقل عمل کنند و با تیم‌های آبی، قرمز، بنفش، خطوط کسب‌وکار و بیشتر همکاری کنند. ما در فصل‌های بعدی به تفصیل بیشتری به این موضوع خواهیم پرداخت.

اکنون که تیم‌هایی که به‌طور نزدیک با تیم آبی کار می‌کنند را پوشش داده‌ایم، بیایید مهارت‌هایی که سازمان‌ها هنگام استخدام باید به دنبال آن باشند را بررسی کنیم. این امر به اطمینان از استخدام و قرار دادن کاندیداهای مناسب در نقش‌های مناسب کمک می‌کند.

مهارت‌های لازم برای عضویت در تیم آبی

اعضای تیم آبی با هدف از پیش تعریف‌شده‌ای برای ایمن‌سازی زیرساخت شبکه کسب‌وکار و تقویت وضعیت امنیت سایبری آن کار می‌کنند. روش‌ها و استراتژی‌هایی که آن‌ها برای دفاع از شبکه و سیستم‌ها در برابر حملات سایبری استفاده می‌کنند، با یکدیگر در هم‌تنیده‌اند. مدیریت باید درک بهتری از اهداف و وظایف اعضای تیم آبی داشته باشد.

علاقه‌مند به یادگیری و دقیق بودن

برای جلوگیری از باقی ماندن آسیب‌پذیری‌های امنیتی در زیرساخت‌های یک شرکت، نیاز است که رویکردی بسیار دقیق و جزئی‌نگر اتخاذ شود. دانستن نحوه ساخت ابزارهای سفارشی مزایای زیادی دارد. نوشتن نرم‌افزار نیازمند تمرین فراوان و یادگیری مداوم است، بنابراین مهارت‌هایی که کسب می‌شود به تیم قرمز کمک می‌کند تا بهترین استراتژی‌های حمله را به اجرا بگذارد.

دانش عمیق درباره شبکه‌ها و سیستم‌ها

درک کامل سیستم‌های کامپیوتری، پروتکل‌ها، کتابخانه‌ها و تکنیک‌ها، تاکتیک‌ها و روش‌های شناخته‌شده (TTPs) زمینه موفقیت کارکنان امنیتی را فراهم می‌کند. توانایی تیم قرمز در درک تمام سیستم‌ها و همگام بودن با پیشرفت‌های فناوری بسیار حیاتی است. دانستن چگونگی کار با سرورها و پایگاه‌های داده، گزینه‌های بیشتری برای کشف ضعف‌ها فراهم می‌کند. همچنین آشنایی با بسته‌های نرم‌افزاری که به تحلیلگران SOC اجازه می‌دهد زیرساخت شبکه را برای فعالیت‌های غیرمنتظره یا بالقوه مخرب رصد کنند، بسیار مهم است.

SIEM یک راهکار است که حوادث امنیتی را به صورت لحظه‌ای تحلیل می‌کند. این سیستم داده‌ها را از منابع متعدد دریافت کرده و بر اساس مجموعه‌ای از معیارها آن‌ها را تحلیل می‌کند. تیم‌های آبی، مشابه تیم‌های قرمز و بنفش، از فناوری‌های متنوع امنیتی مانند هانی‌پات‌ها، سندباکس‌ها، XDRها، NGAVها، چارچوب‌های تشخیص تهدید و راهکارهای SIEM استفاده می‌کنند.

در ادامه فهرستی از برخی ابزارهای محبوب امنیت سایبری که این تیم‌ها معمولاً برای کارهای عملیاتی خود به کار می‌برند آمده است:

- Splunk
- Haktrails
- Cuckoo Sandbox
- SecurityTrails API

تفکر نوآورانه و خارج از چارچوب

ویژگی اصلی تیم‌های امنیت سایبری، توانایی آن‌ها در تفکر خارج از چارچوب است؛ آن‌ها همیشه در حال توسعه ابزارها و روش‌های جدید برای بهبود امنیت سازمان هستند. برای همگام شدن با مهاجمان، متخصصان امنیت سایبری باید به طور مستمر خارج از چارچوب فکر کنند و ابزارها و روش‌های جدیدی کشف کنند. تیم‌های امنیت سایبری در طول عملیات خود از ابزارهای مختلفی استفاده می‌کنند که شامل ابزارهای شناسایی، افزایش امتیاز دسترسی، حرکت جانبی و استخراج داده‌ها می‌شود.

توانایی عبور از موانع مرسوم برای انجام وظایف

تحلیلگران SOC همیشه تعداد قابل توجهی هشدار مثبت کاذب (False Positives) را شناسایی می‌کنند. برای کاهش تعداد هشدارهای مثبت کاذب در ابزارهای SOC، گاهی تحلیلگران ارشد باید از چندین مانع مرسوم عبور کنند. آن‌ها باید قوانینی با چندین معیار فیلتر تنظیم کنند که گاهی پیچیده و سنگین می‌شود. ترسیم نقشه ذهنی از تمام موارد کاربرد به این متخصصان کمک می‌کند چون باید ارتباط بین موارد مختلف پیکربندی شده در ابزارهای SOC را برقرار کنند. آن‌ها همچنین باید بررسی کنند که آیا قوانین خاصی که برای یک مورد کاربردی تنظیم شده‌اند، قوانین دیگر را نقض نمی‌کنند. حل تعارض‌ها در کمترین زمان ممکن و بدون تأثیر روی SLAها بسیار مهم است. در بسیاری از موارد، این کار شبیه به پیدا کردن سوزن در انبار کاه است.

تحصیلات، مدارک دانشگاهی و گواهینامه‌ها

برای فعالیت در نقش‌های تیم آبی، داشتن مدارک دانشگاهی یا گواهینامه‌های خاص الزامی نیست. مهارت‌های عملی و استعدادهای فنی مهم‌ترین عامل برای موفقیت در این نقش‌ها هستند، زیرا این توانمندی‌ها باعث می‌شود افراد در هر سازمانی عملکرد بهتری داشته باشند. البته داشتن مدارک تحصیلی یا گواهینامه‌های مناسب ممکن است در برخی آگهی‌های شغلی به عنوان یک مزیت در نظر گرفته شود.

بسیاری از اعضای تیم آبی به‌صورت خودآموز یاد گرفته‌اند و دانش آن‌ها حاصل تلاش شخصی است نه آموزش رسمی. با این حال، برخی سازمان‌ها ممکن است به دنبال مهارت‌های خاصی در رزومه فرد باشند و این مدارک تحصیلی بیشتر به عنوان ابزار غربال‌گری برای دعوت به مصاحبه در نظر گرفته می‌شوند، نه الزامی برای استخدام.

برخی گواهینامه‌های محبوب در حوزه تیم آبی توسط نهادهایی مانند CompTIA، SANS، EC-Council، ISC2، ISACA و سایر مؤسسات صادر می‌شوند. همچنین، دوره‌های آموزشی تخصصی مرتبط با محصولات امنیتی خاص نیز وجود دارد که به تقویت مهارت‌های عملی اعضای تیم آبی کمک می‌کند.

توسعه و نگهداشت استعدادها

یکی از چالش‌برانگیزترین وظایف مدیران امنیتی، یافتن فردی متعهد، پرشور و باهوش برای تیم امنیت است. کمبود مهارت‌های تخصصی امنیت سایبری در سراسر جهان یک واقعیت شناخته‌شده است؛ بنابراین جذب استعدادهای مناسب اهمیت زیادی دارد. هیچ راه‌حل واحدی برای این چالش وجود ندارد، اما در ادامه چند راهکار پیشنهادی برای مدیریت بیان می‌شود:

آزمایشگاه‌های سایبری

تشویق کارکنان به راه‌اندازی آزمایشگاه شخصی در خانه یا استفاده از آزمایشگاه‌های شرکت، یک روش مؤثر برای یادگیری عملی است. در این فضا می‌توان سناریوهای واقعی را شبیه‌سازی کرد و مهارت‌های جدید را تمرین و تقویت نمود. یادگیری عملی برای بسیاری از افراد بهترین روش یادگیری است و استفاده از آزمایشگاه، ریسک آسیب به محیط عملیاتی را حذف می‌کند.

مسابقات Capture-the-Flag و هکاتون‌ها

برگزاری مسابقات CTF در محل شرکت می‌تواند باعث تقویت آموزش بین‌بخشی، افزایش همدلی در تیم و بهبود ارتباطات شود. CTFها و هکاتون‌ها جزء اصلی بیشتر کنفرانس‌های پرانرژی امنیت سایبری هستند. این رویدادها همچنین فرصت خوبی برای شناسایی استعدادهای جدید

برای استخدام یا گسترش تیم امنیتی فراهم می‌کنند. شرکت‌کنندگان در این رقابت‌ها نه‌تنها دانش فنی خود را نشان می‌دهند، بلکه مهارت‌های ارتباطی، توانایی کار تیمی و تمایل به کمک و آموزش دیگران را نیز به نمایش می‌گذارند.

پروژه‌های تحقیق و توسعه

توسعه پروژه‌های داخلی یا مشارکت در پروژه‌های متن‌باز نیز راهی دیگر برای جذب و نگهداشت استعدادهاست. بسیاری از پروژه‌های متن‌باز نیازمند مستندسازی یا همکاری در حوزه‌های امنیتی مختلف هستند. این فرصت‌ها می‌توانند انگیزه‌ای برای کارکنان فراهم کنند تا مهارت‌های خود را در سطح عمومی به نمایش بگذارند. بنابراین، اگر سازمان به کارمندان خود اجازه دهد زمان خود را صرف چنین پروژه‌هایی کنند، این می‌تواند به عنوان عاملی برای جذب استعداد محسوب شود.

تعامل با جامعه تخصصی

حمایت از حضور کارکنان در همایش‌ها، کنفرانس‌ها یا حتی نشست‌های محلی، باعث تقویت فرهنگ یادگیری مستمر در سازمان می‌شود. حضور در یک همایش به‌تنهایی مفید است، اما کارکنان امنیتی می‌توانند یک گام فراتر رفته و در این رویدادها سخنرانی کنند یا داوطلبانه کمک برسانند. این فعالیت‌ها امکان برقراری ارتباط و ایجاد شبکه‌های حرفه‌ای را فراهم می‌کنند که برای کارکنان اطلاعات تهدید (CTI) اهمیت حیاتی دارد.

منتورینگ (مربی‌گری)

رهبران سازمان می‌توانند با مربی‌گری به رشد استعدادهای جوان کمک کنند. این کار، هم درون محیط کار و هم خارج از آن، تجربه‌ای مفید برای یادگیری محسوب می‌شود. منتورینگ باعث می‌شود اعضای تیم امنیتی شناخت بیشتری از سازمان پیدا کرده و احساس ارتباط بیشتری با مدیران ارشد داشته باشند. این موضوع آن‌ها را به توسعه مسیر شغلی و شبکه‌سازی بین واحدها و خطوط کسب‌وکار تشویق می‌کند.

یادگیری مستمر و بدون مانع

مهارت‌هایی که برای محافظت از شبکه‌های سازمانی مورد نیاز هستند، همواره در حال تغییر هستند، زیرا صنعت امنیت سایبری برای مقابله با تهدیدات نوظهور و TTPهای جدید در حال تکامل است. تحقیقات نشان داده‌اند که کارشناسان سایبری در صورت توقف یادگیری، ممکن است در عرض تنها سه ماه از روند روز عقب بمانند و بهره‌وری آن‌ها کاهش یابد.

تکنیک‌های مهاجمان سایبری به‌طور مداوم تغییر می‌کند، پس چرا تیم آبی نیز رشد نکند؟ کمک به یادگیری پیوسته کارکنان برای حفظ امنیت سازمان در فضای سایبری پرشتاب امروز حیاتی است. توصیه می‌شود ذی‌نفعان، آموزش مداوم سایبری را اتخاذ کنند تا بهره‌وری و امنیت را افزایش دهند. آموزش مداوم، به اعضای تیم آبی کمک می‌کند تا دانش خود را به‌روز نگه دارند و با روندهای صنعت همگام شوند.

کارکنانی که آموزش‌های لازم را حین کار دیده‌اند، عملکرد بسیار بهتری در مقابله با حملات دارند. آموزش‌های مکرر و دریافت گواهینامه‌ها باعث می‌شود تیم آبی بتواند به‌سرعت تهدیدها را شناسایی کرده و به‌صورت مؤثر پاسخ دهد.

اگرچه بسیاری از شرکت‌ها روی فناوری‌های امنیتی جدید سرمایه‌گذاری می‌کنند، اما به دلیل کمبود زمان یا منابع لازم برای یادگیری این ابزارها، کارشناسان امنیتی نمی‌توانند حداکثر استفاده را از آن‌ها ببرند. برای بهره‌برداری کامل از فناوری‌های نوین، کارشناسان امنیت باید دائماً در حال یادگیری و به‌روز نگه‌داشتن خود باشند.

خلاصه

راه‌اندازی یک برنامه امنیت اطلاعات کار ساده‌ای نیست. بسیاری از برنامه‌ها ناکارآمد هستند یا اصلاً وجود ندارند، و همین موضوع یکی از دلایل وضعیت نامطلوب امنیت در کسب‌وکارهاست. این فصل باید به شما کمک کرده باشد تا تیم‌های آبی (Blue Team)، قرمز (Red Team)، بنفش (Purple Team) و تیم اطلاعات تهدیدات سایبری (CTI) را بهتر بشناسید.

یک برنامه امنیت سایبری مؤثر نیازمند مهارت‌های سازمانی، کارکنان آگاه و پرتلاش، رهبری قوی و درک عمیق از حوزه امنیت سایبری است.

در این فصل، درباره مهارت‌های مورد نیاز، نوع استعدادهایی که باید جذب شوند، و از همه مهم‌تر، روش‌های توسعه و حفظ آن استعدادها صحبت کردیم. در فصل بعدی، درباره نحوه مدیریت چنین تیمی صحبت خواهیم کرد و همچنین بررسی خواهیم کرد که چه شاخص‌ها و معیارهایی باید تعریف شوند تا اطمینان حاصل شود که تیم به‌خوبی عمل می‌کند و بیشترین ارزش را برای سازمان ایجاد می‌کند.

2 فصل دوم به زودی ...