عملیات تیم آبی و دفاع سایبری

معماری و مهندسی امنیت

ارزیابی بلوغ مستقل برنامه، امنیت سایبری سازمان شما را در چهار زمینه اصلی فراهم می کند: حاکمیت امنیت، معماری امنیتی، دفاع سایبری و مدیریت ریسک امنیتی. ما پس از تجزیه و تحلیل عمیق برنامه فعلی شما، بر اساس مشخصات خطر پذیری خاص و سطح بلوغ امنیتی بهترین توصیه های عملی را برای بهبود وضعیت امنیتی شما ارائه می دهیم. نیاز سنجی و ارزیابی میدانی سازمان شما، نقشه طراحی معماری و مهندسی امنیت سایبری، طبق سطح خدمات و مراودات ارتباطی تایین خواهد شد.

مدیریت ریسک سایبری

برنامه مدیریت ریسک سایبری موجود را از نظر نقاط قوت و ضعف امنیتی ارزیابی کنید .خطرات سایبری مربوط به سازمان خود را شناسایی و رویکرد تجاری خود را برای مدیریت ریسک اینترنتی و تصمیم گیری موثر و کاهش ریسک پیش بینی کنید .دستورالعمل های مناسبی در خصوص واکنش های سریع در راستای مدیریت ریسک تعریف کرده و سعی بر سخت کردن فضای سایبری کنید. متخصصان ما این یافته ها را می گیرند تا نقایص برنامه را شناسایی کنند و به نوبه خود توصیه های عملی، فنی، استراتژیک و اولویت بندی شده را برای ایجاد یا بهبود برنامه مدیریت ریسک سایبری شما و دستیابی به یک وضعیت امنیتی بالغ و در نهایت کاهش خطرات آینده و سطح تأثیر آنها بر تجارت شما تهیه کنند.

عملیات تیم آبی

تیم آبی به ما امکان می دهد تا حملات هدفمند را که توسط ابزارهای رایج و نرم افزار امنیتی شناسایی نمی شوند، شناسایی کنیم. شکار تهدید یک روند مداوم در حال تکامل است نه یک فناوری. ما دانش کاملی در مورد حملات واقعی و تکنیک های Exfiltration داریم. ما روش های مهاجمان را تشریح می کنیم تا بتوانیم آنها را مستقل از ابزارهایی که برای انجام آنها استفاده شده اند، شناسایی کنیم .بعلاوه ما از داده های حاصله میتوان در راستای اطلاعات تهدید و CTI (اطلاعات تهدید سایبری) خود استفاده کنیم.

راه ارتباطی

تلفن:
026 368 06249

وبسایت:
unk9vvn.com

ایمیل:
info@unk9vvn.com

امنیت فضای ابری

تکنیک های امنیتی و سخت افزاری موجود خود را برای محبوب ترین دارایی های مبتنی بر فضای ابر از جم Microsoft Office 365 ، Microsoft Azure، Amazon Web Servicesو Google Cloud Platform ارزیابی کنید. تهدیدها و کنترل های امنیتی مربوط به محیط ابری خود را درک کنید. توانایی خود را در شناسایی، بررسی و پاسخ به فعالیت مهاجم در تمام مراحل چرخه حیات حمله نشان دهید .پیکربندی و کنترل های امنیتی که به طور مداوم اجرا می شوند و نقاط ضعف بالقوه را شناسایی می کنند را بررسی کنید همچنین از گزارش دهی که شامل توصیه های دقیق عملی برای سخت کردن فضای ابری، افزایش دید و شناسایی و بهبود فرایندها است، برای کاهش خطر احتمالی استفاده کنید.

اطلاعات متن باز

ما با استفاده از (Open-Source Intelligence) OSINT اطلاعات قابل توجهی درباره سازمان هدف در اینترنت جمع آوری می کنیم. از اطلاعات به دست آمده می توان برای شناسایی دارایی های آسیب پذیر و نقاط ضعفی که تهدید کنندگان هدف قرار می دهند، استفاده کرد. اطلاعات بازیابی شده با استفاده از تکنیک های OSINT، شامل جزئیاتی درباره کارمندان، ساختار سازمان، دارایی های فیزیکی، زیرساخت IT و موارد دیگر است.

اطلاعات امنیتی و مدیریت رویدادها

از CTI برای بروزرسانی مداوم اطلاعات از منبع خارجی در مورد یک سازمان معین استفاده می شود. این خدمات از دو قسمت اصلی تشکیل شده است: اطلاعات مربوط به تیم های امنیتی و IOC (شاخص سازش) که بیشتر برای داده کاوی خودکار داده ها به منظور نظارت داخلی با سیستم های SIEM ، IPSاسیستم پیشگیری از نفوذ (یا IDS / NIDS / HIDS (سیستم تشخیص نفوذ ، شبکه) انجام میشود. ساده ترین مثال برای چنین داده کاوی ای، میتواند کسب اطلاعات آدرس های IP از شبکه honeypotمورد استفاده توسط مهاجمان یا تشخیص تغییرات پورت های باز در زیرساخت های شرکت باشد. ما از یک نرم افزار اختصاصی استفاده می کنیم که بسته به نیاز مشتری به طور خودکار به دنبال تهدیدات احتمالی است. ما از نظارت بر زیرساخت با داده های CTI که به ما امکان شناسایی حملات هدفمند به طور مداوم میدهد پشتیبانی می کنیم.

تهدید فعال

ما می دانیم که چگونه علائم حمله و حضور متجاوز در زیرساخت های سازمان را به طور موثر شناسایی کنیم. اینکار برای یک شکارچی تهدید، اجرای یک نرم افزار اختصاصی) به عنوان مثال یک (HoneyPot یا نظارت بر ترافیک DNS و لاگ های ورودی در داخل یک شبکه است که به دنبال فعالیت های مخرب می گردد.

بررسی آنتروپی انواع درخواست های DNS و مقایسه دامنه ها با شاخصه های حمله یا (IoCs) دریافت شده از اطلاعات تهدید و غیره است. از طرف دیگر تجزیه و تحلیل ورود به سیستم در این مورد فقط محدود به نظارت بر وقایع سیستم نیست، بلکه به معنی تجزیه و تحلیل عمیق در پردازش ها و با بررسی اتصال پردازش ها بسیاری از منابع است که می تواند نشان دهنده به خطر افتادن یکپارچگی باشد.

محافظت فعال

برای محافظت فعال میبایست از آزمایشات و اقدامات امنیتی موجود برای تشخیص نقاط ضعف استفاده و ممیزی های امنیتی را کاملا برقرار نمود، همچنین آسیب پذیری های موجود را بواسطه خدمات تست نفوذ به عنوان یک مکمل ارزیابی کرد. موارد جدید تری مانند: بررسی امنیت فضای ابری و مهندسی اجتماعی و شبیه سازی های تیم قرمز از موارد خاص تری در خصوص برقراری محافظت فعال خواهند بود.

ارزیابی های امنیتی بر پایه کشف آسیب پذیری فعال هم یکی دیگر از موارد محافظت فعال میباشد، یعنی تیم آبی در خصوص آسیب پذیری های انتشار یافته همواره باید گزارشات سامانه ها را بروز رسانی نماید.

شناسایی فعال

شناسایی فعال بدین معنی است که کارشناس تیم آبی بر اساس اکتشافات مخازن رویدادها بصورت دستی اقدام به طراحی امضا های فعال در خصوص فایل های مخرب کرده و مخازن امضای مکانیزم های شناسایی کننده را همواره بروز رسانی نماید.

شناسایی فعال به ارتباطات و بهره برداری هایی که از پروتکل ها می شود هم نظارت دارد و اگر تکنیک های Exfiltrationموجود در مستندات MITRE ATT&CK توسط کارشناسان مشاهده شود سریعا اقدام به رهگیری و داده کاوی ارتباط کرده و در صورت نا معتبر بودن ارتباط را از بین خواهند برد. این امر همواره یکی از موثر ترین روش های شکار تهدیدات بوده و داده های تراکنش شده مبهم را براحتی نمایان میسازد.