# عملیات تیم آبی و دفاع سایبری

## Blue Teaming and Cyber Defense

## 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. پس از تجزیه و تحلیل عمیق و مشترک برنامه فعلی شما، ما بهترین توصیه های عملی را برای بهبود وضعیت امنیتی شما بر اساس مشخصات خطر پذیری خاص و سطح بلوغ امنیتی ارائه می دهیم. نیاز سنجی و ارزیابی میدانی سازمان شما نقشه طراحی معماری و مهندسی امنیت سایبری طبق سطح خدمات و مراودات ارتباطی تعیین خواهد شد.

## مدیریت ریسک سایبری

برنامه مدیریت ریسک سایبری موجود خود را از نظر نقاط قوت و ضعف امنیتی ارزیابی کنید. خطرات سایبری را که مربوط به سازمان شما هستند شناسایی کنید و رویکرد تجاری خود را برای مدیریت ریسک اینترنتی برای تصمیم گیری موثر و کاهش ریسک پیشبینی کنید و دستورالمل های مناسبی در خصوص واکنش های سریع در راستای مدیریت ریسک تعریف کرده و سعی بر سخت کردن فضاء 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 – 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 جمله Microsoft Office 365 ، Microsoft Azure ، Amazon Web Services و 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 نظارت و شکار انجام شود. با بررسی پیکربندی، کنترل های امنیتی به طور مداوم اجرا می شوند و نقاط ضعف بالقوه را شناسایی می کنند همچنین گزارش دهی شامل توصیه های دقیق عملی برای سخت کردن فضای ابری، افزایش دید و شناسایی و بهبود فرایندها برای کاهش خطر احتمالی است.

## اطلاعات متن باز

ما مشارکتهای (Open-Source Intelligence) OSINT را در جایی انجام می دهیم که اطلاعات قابل توجهی را درباره سازمان هدف در اینترنت جمع آوری می کنیم. از اطلاعات به دست آمده می توان برای شناسایی دارایی های بالقوه آسیب پذیر و نقاط ضعف استفاده کرد که تهدیدکنندگان ممکن است هدف قرار دهند . 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

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 برای نظارت داخلی با سیستم های SIEM ، IPS (سیستم پیشگیری از نفوذ) یا IDS / NIDS / HIDS (سیستم تشخیص نفوذ ، شبکه) ساده ترین مثال برای چنین داده کاوی می تواند کسب اطلاعات آدرس های IP از شبکه honeypot مورد 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 پشتیبانی می کنیم که به ما امکان می دهد حملات هدفمند را به طور مداوم شناسایی 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 هانی پات) یا نظارت بر ترافیک DNS در داخل یک شبکه است که به دنبال فعالیت بالقوه مخرب است.

بررسی آنتروپی انواع درخواست های DNS و مقایسه دامنه ها با IOC (شاخص سازش) دریافت شده از اطلاعات تهدید و غیره. 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 با اتصال 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 ارزیابی آسیب پذیری ها که امنیت برنامه ها را تعمیین و عملیات تست نفوذ مکمل این جریان خواهد بود. همچنین 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.

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

## شناسایی فعال

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

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