جرم شناسی دیجیتال و پاسخ به حادثه

Digital Forensics and Incident Response

پاسخ به حوادث

مهمترین جنبه خدمات SOC / CERT صلاحیت تیم فنی است، زیرا سطح دانش متخصصان است که امنیت سایبری سازمان را تعیین می کند. از طرف دیگر، شبکه مستقیماً با استفاده از نرم افزار IDS / NIDS (Network Intrusion Detection System) پوشش داده می شود که حملات انجام شده در شبکه محلی را به طور منحصر به فرد تشخیص می دهد. دامنه های مخرب، آدرس های IP و اطلاعات هش (IOC) توسط سیستم CTI ما (Cyber Threat Intelligence) ارائه می شود، که اطلاعات را با همکاری سایر تیم های بین المللی پاسخ به حوادث دریافت می کند.

شکار تهدیدات

شکار تهدید و اطلاعات تهدید موضوعاتی است که بیش از یک دهه است معرفی شده است.یکی از دستاوردهای مربوط به شکار تهدید پیشگیرانه و همچنین پاسخ به حوادث پیشرفته، از جمله APT کلاس جهانی (تهدید مداوم پیشرفته) موضوعی است که بشدت در حال گسترش است و بواسطه IOC ها حملات پیشرفته APT رصد می شوند .قدرت شناسایی آسیب پذیری های روز صفر (ضعف نرم افزاری که هنوز هیچ گونه اصلاحیه امنیتی برای آنها وجود ندارد) یکی از ویژگی های شکار تهدیدات است.

جرم شناسی دیجیتال

شناسایی زودهنگام و تحقیقات سریع برای دفع مهاجمان و پاسخگویی به تهدیدها بسیار مهم است .اما تعداد بیشماری هشدار، اطلاعات ناکافی و عدم دید می تواند شما را از انجام این کارهای مهم باز دارد .اینجاست که ما وارد می شویم .ما هم از نظر امنیت سایبری (اطلاعات تهدید و شکار تهدید) و هم پاسخ سریع به حوادث (DFIR)هم یک نظارت مستمر 24 ساعته بر منابع IT را ارائه می دهیم .ما از شما دعوت می کنیم تا با سرویس SOC به عنوان سرویس ارائه شده توسط تیم مرکز عملیات امنیتی (SOC) آشنا شوید.

راه ارتباطی

تلفن:
026 368 06249

وبسایت:
unk9vvn.com

ایمیل:
info@unk9vvn.com

مرکز عملیات امنیت

کارشناسان SOC (شکارچی تهدید) و تیم CERT همواره میکوشند تا در زمینه های دفاعی (تیم آبی) و تهاجمی (تیم قرمز) در امنیت سایبری و همچنین یک آزمایشگاه حرفه ای جرم شناسی رایانه ای را پیاده سازی کرده تا در موقعیت های مختلف بتوانند کنش های مناسبی را از خود نشان دهند، در مرکز عملیات امنیت همواره متخصصین شکار و پاسخ سریع به حادثه مامور داده کاوی از پایگاه های گردآوری اطلاعات خواهد بود.

تیم پاسخگوی حوادث امنیت رایانه

یک تیم پاسخ دهنده به حوادث شناخته شده که در مواقع اضطراری میتواند به سازمان ها و نهادهای دولتی کمک رسانی سایبری کند، این پاسخ به یک حادثه در زمان رخداد یک حمله سایبری بسیار امر مهمی بوده و تیم های جرم شناسی را میتواند در امر تحقیقات صریح بسیار کمک کند، برای مثال اگر یک باج افزار سوار بر سیستم عامل های یک سازمان شود معمولا یک مدت زمان کوتاهی برای رسیدن باج افزار به مرحله Impact تعیین می شود که اگر تیم پاسخگویی جرم شناسی دیجیتال سریع وارد عمل شود میتواند واکنش مناسبی در خصوص حمله اتخاذ کند.

تجزیه و تحلیل بدافزار

تحلیل بدافزار از موارد بسیار کلیدی در راستای جمع آوری اطلاعات و جرم شناسی خواهد داشت و در این حوزه میتوان روش های ضد مهندسی معکوس و ضد بازیابی کدنویسی را خنثی کرد، همچنین میتوان در راستای رفتار شناسی و ایجاد امضاء در خصوص فایل فرمت های مخربی که وارد سیستم شده است عملیات مناسبی را انجام داده و داده کاوی را بعد از مهندسی معکوس منطقه مورد نظر آغاز نمایند.

جرم شناسی دیجیتال

ما خدمات تخصصی در پزشکی قانونی رایانه به ویژه مربوط به امنیت سایبری به معنای DFIR (جرم شناسی و پاسخ به حادثه) را ارائه می دهیم. ما برای انجام تجزیه و تحلیل در جرم شناسی از تجهیزات و ابزارهای تجاری بسیار تخصصی استفاده می کنیم.

آزمایشگاه جرم شناسی دیجیتال ما که ماهانه ده ها مورد داده کاوی و استخراج اطلاعات در آن انجام می شود متشکل از تعدادی نرم افزار حرفه ای و معتبر از جمله FTK Forensic Toolkit و X-Ways Forensics است که به شما امکان می دهد شواهد را از طریق چندین مستندات تجزیه و تحلیل کنید.

حادثه امنیتی

ایمن سازی صحیح ردیابی های دیجیتال امکان تجزیه و تحلیل عمیق حادثه را فراهم می کند و به شما امکان می دهد جزئیات چگونگی وقوع و عملیاتی که مهاجم انجام داده را تعیین کنید. در صورت عدم امنیت صحیح شواهد، با گذشت زمان مکتوبات سیستم از بین می رود حتی اگر کاربر روی آن کار نکند و سیستم به سادگی در حال اجرا باشد.

از طرف دیگر، خاموش کردن رایانه بدون محافظت قبلی لازم منجر به از دست رفتن غیرقابل جبران ناپذیر داده های دیجیتالی مختص به مهاجم می شود که در حافظه سیستم عامل ذخیره می شوند و ممکن است حاوی اطلاعات مهمی برای تجزیه و تحلیل حادثه باشد.

نظارت بر محیط IT

محصولات امنیتی که برای شناسایی حملات شبکه، ارتباطات را رصد می کنند و از صدها قانون از پیش تعیین شده برای تشخیص استفاده می کنند و همواره یک عیب اصلی را دارا هستند این عیب را میتوان عدم درک بیشتر هشدارهای گزارش شده دانست .

مهاجمان اغلب از روش های مبهم سازی در خصوص کانال های ارتباطی با مرکز فرمان خود استفاده میکنند که رصد آنها برای محصولات سطح شبکه امکان پذیر نیست و بدین ترتیب همواره نیازه به تیم های بنفش حس خواهد شد که با رفتارشناسی های مشکوک در سطح شبکه حملات و ارتباطات را شکار کنند.