جرم شناسی دیجیتال و پاسخ به حادثه

پاسخ به حوادث

مهمترین جنبه خدماتSOC / CERT ، صلاحیت تیم فنی است، زیرا سطح دانش متخصصان، امنیت سایبری سازمان را تایین می کند. از طرف دیگر، شبکه مستقیماً با استفاده از نرم افزار NIDS / IDS پوشش داده می شود تا حملات انجام شده در شبکه محلی به طور منحصر به فرد تشخیص داده شود. دامنه های مخرب، آدرس های IP و اطلاعات هش (IoC) توسط سیستم اطلاعات تهدیدات سایبری یا (Cyber Threat Intelligence) ما 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 هستند که بیش از یک دهه است معرفی شده اند. از دستاوردهای آنها میتوان به شکار تهدیدات در کلاس جهانی یعنی APT ها و پاسخ به حوادث رخ داده اشاره کرد. حملات پیشرفته APT بواسطه IoC ها رصد می شوند و در تکنیک های شکار الگو رفتاری تکنیکی و تاکتیکی آنها ترسیم میشوند که به این امر TTP گفته می شود. قدرت شناسایی آسیب پذیری های روز صفر (ضعف نرم افزاری که 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)، 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، در مواقع اضطراری میتواند به سازمان ها و نهادهای دولتی کمک رسانی سایبری کند، این پاسخ به یک حادثه در زمان رخداد حمله سایبری امر بسیار مهمی بوده و میتواند تیم های جرم شناسی را در امر تحقیقات صریح کمک کند، برای مثال در صورت آلوده شدن سیستم عامل های یک سازمان به باج افزار معمولا مدت زمان کوتاهی برای رسیدن باج افزار به مرحله Impact لازم است. اگر تیم پاسخگویی جرم شناسی دیجیتال سریع وارد عمل شود واکنش مناسبی در خصوص حمله میتواند نشان دهد.

تجزیه و تحلیل بدافزار

تحلیل بدافزار از موارد بسیار کلیدی در راستای جمع آوری اطلاعات و جرم شناسی است که با استفاده از آن 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 مخرب وارد شده به سیستم، عملیات مناسبی انجام داد و داده کاوی را بعد از مهندسی معکوس منطقه مورد نظر آغاز کرد.

جرم شناسی دیجیتال

ما خدمات تخصصی جرم شناسی دیجیتال را که به آن) DFIR جرم شناسی و پاسخ به حادثه) میگویند، 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 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 عملیاتی که مهاجم انجام داده را تعیین کنید. با گذشت زمان در صورت عدم ایمن سازی صحیح شواهد، مکتوبات سیستم از بین می روند حتی اگر کاربر روی آن کار کند و سیستم به سادگی در حال اجرا باشد.

از طرف دیگر، خاموش کردن رایانه بدون محافظت قبلی لازم، منجر به از دست رفتن جبران ناپذیر داده های دیجیتالی میشود که در حافظه سیستم عامل ذخیره شده و مختص به مهاجم است. این داده ها ممکن است حاوی اطلاعات مهمی برای تجزیه و تحلیل حادثه باشند.

نظارت بر محیط IT

امروزه، امنیت دیجیتال نیاز هر شرکتی است بنابراین مهمترین مسئله سرعت واکنش است. ما در SOC از فناوری های دفاعی پویا استفاده می کنیم که برای شناسایی انواع جدیدی از تهدیدهای هرگز دیده نشده (نمونه های منحصر به فرد در حملات هدفمند) استفاده می شوند.

هر نمونه جدید به طور خودکار در یک Sandbox تجزیه و تحلیل می شود تا بتوان رفتار را شبیه سازی و روش های مخرب را شناسایی کرد. با استفاده از محصولاتی مانند Splunk و ELK تمامی رفتارهای درون شبکه جمع آوری و رفتارشناسی خواهند شد.