شرکت مهندسی فناوران

نقطه ایمن هوشمند

SMART SAFEPOINT TECHNOLOGY

معرفی شرکت مهندسی فناوران

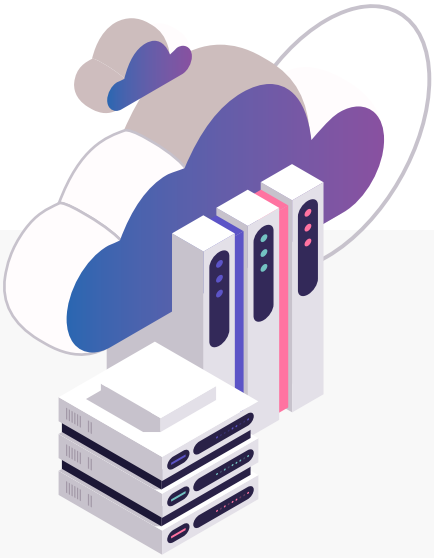
نقطه ایمن هوشمند

شرکت مهندسی فناوران نقطه ایمن، یک مجموعه پیشرو در حوزه امنیت سایبری و توسعه راهکارهای بومی در ایران است که توسط تیمی متخصص با بیش از ۱۵ سال تجربه عملیاتی در حوزه امنیت اطلاعات، تشکیل شده است. این شرکت با تمرکز بر حوزه‌های گوناگون امنیت اطلاعات از جمله امنیت شبکه، پایش و پاسخ به تهدیدات، مدیریت آسیب‌پذیری، امنیت زیرساخت ابری، توسعه محصولات امنیتی سفارشی می‌تواند نیازهای متنوع سازمان‌ها را در سطحی حرفه‌ای برآورده سازد.

حوزه‌های فعالیت:

- ارائه خدمات و زیرساخت هوش تجاری (BI) و تحلیل داده‌های امنیتی برای تصمیم‌سازی بهتر در سازمان
- مشاوره امنیتی و طراحی معماری امن در لایه سرویس و شبکه
- هاردنینگ سیستم‌ها و زیرساخت‌ها
- توسعه محصولات اختصاصی امنیت سایبری
- پیاده‌سازی و اصلاح ساختار مراکز عملیات امنیت (SOC) و ارائه خدمات مدیریت‌شده امنیتی (MSSP)
- امن‌سازی زیرساخت ابری با رویکرد Zero Trust
- تیم قرمز و شبیه‌سازی حملات پیشرفته (APT Simulation)
- اجرای تست نفوذ وب، شبکه، موبایل
- آموزش دوره‌های تخصصی در حوزه امنیت سایبری

معرفی محصولات امنیتی اختصاصی



یکسوساز داده (Data Diode)

یکسوساز داده، یک سامانه سخت‌افزاری- نرم‌افزاری است که امکان انتقال امن و یک‌طرفه داده‌ها از یک شبکه به شبکه دیگر را فراهم می‌کند. این محصول با بهره‌گیری از فناوری‌های فیزیکی و منطقی، جداسازی کامل و غیرقابل نفوذ بین شبکه‌های امن و غیرامن را تضمین می‌نماید.

ویژگی‌ها و کاربردها:

- انتقال یک‌طرفه داده، تفکیک شبکه‌های OT و IT، تجمیع امن شبکه‌های صنعتی با IT، ارائه امن سرویس‌ها و API ها در شبکه‌های ایزوله، جلوگیری از ارتباطات برگشتی ناخواسته به منابع حساس

- استفاده از تجهیز سخت افزاری بدون سیستم عامل برای تضمین فیزیکی و یک‌طرفه بودن ارتباط
- دروازه امن تبادل اطلاعات بین سرورهای عمومی و داخلی (Secure Web Service)

- جلوگیری از حملات ناشی از ارتباطات برگشتی یا کنترل‌نشده به منابع حساس
- عدم نیاز به مولفه‌های خارجی و فعال سازی کلیه مولفه ها به‌صورت جاسازی شده در تجهیز

- طراحی ماژولار برای پیاده‌سازی انواع کاربردها
- پشتیبانی از رمزنگاری داده و گواهی‌های امنیتی
- قابلیت مانیتورینگ و گزارش‌گیری بر اساس استانداردهای امنیتی

سامانه شکار تهدید مبتنی بر IOC

این سامانه به‌صورت خودکار اقدام به شناسایی تهدیدات سایبری از طریق تحلیل ترافیک شبکه و انطباق آن با اطلاعات هوش تهدید (IOC) می‌کند. اطلاعات مرتبط با تهدیدات از منابع مختلف جمع‌آوری می‌شوند و با ترافیک داخلی شبکه تطبیق داده می‌شوند.
این فرآیند نوعی بهره‌برداری از دانش امنیتی شرکت‌های امنیتی دنیا در بستر داخلی سازمان به‌شمار می‌آید.

ویژگی‌ها و کاربردها:

- استخراج و ذخیره‌سازی فیلدهای پروتکل‌ها پس از decode
- انطباق با طیف وسیعی از دسته‌های متنوع IOC که شامل IP، دامنه، هش فایل، URL و دسته های دیگر است؛ این سامانه قابلیت انطباق با تمامی انواع شاخص‌های شناخته‌شده تهدید را با استفاده از قوانین سفارشی دارد
- تحلیل ترافیک HTTP، DNS، TCP، SMB، Kerberos و سایر پروتکل‌ها
- مقایسه رفتار شبکه فعلی با تاریخچه ترافیکی قبلی
- داشبورد گرافیکی و سیستم هشداردهی لحظه‌ای
- امکان استفاده از اطلاعات در تحلیل‌های فارنزیکی

سامانه پویش آسیب‌پذیری توزیع یافته (DVRS)

DVRS یک سامانه برای اسکن مداوم و خودکار شبکه از نظر آسیب‌پذیری‌ها، شناسایی سرویس‌ها، پیکربندی نادرست، و تحلیل وضعیت امنیتی سازمان است. این محصول از موتورهایی نظیر Nessus استفاده می‌کند و در واقع پیاده‌سازی بومی‌شده‌ای از قابلیت‌های کلیدی سامانه Tenable SC به‌شمار می‌آید که متناسب با زیرساخت‌های داخلی و نیازمندی‌های بومی سازمان‌ها طراحی شده است.

ویژگی‌ها و کاربردها:

- شناسایی مستمر دارایی‌ها و آسیب‌پذیری‌ها
- ایجاد تاریخچه روزانه امنیت شبکه و بررسی روندهای تغییرات امنیتی در گذر زمان
- مقایسه وضعیت فعلی با داده‌های گذشته برای تشخیص تغییرات مشکوک یا ناخواسته
- ارائه داشبورد مرکزی و گزارش‌های تجمیعی با قابلیت فیلتر و اولویت‌بندی
- قابلیت ترکیب با سامانه‌های SIEM و دیگر ابزارهای امنیتی برای پوشش جامع تهدیدات
- ساختار ماژولار با اسکنرهای چندگانه و داکرایز شده برای مقیاس‌پذیری و استقرار سریع
- امکان زمان‌بندی دقیق اسکن‌ها، تعریف سیاست‌های اختصاصی و سفارشی‌سازی بر اساس گروه‌های دارایی
- استفاده از API برای اتصال به سامانه‌های مدیریت دارایی، CMDB و مدیریت تغییرات
- پشتیبانی از انواع سناریوهای اسکن (شبکه داخلی، خارجی، مجازی، ابری)
- برخورداری از قابلیت هشداردهی، امتیازدهی به آسیب‌پذیری‌ها و پیشنهاد راهکار اصلاحی بر اساس استانداردهای بین‌المللی

زیرساخت میزکار مجازی مبتنی بر Kubernetes

این زیرساخت، یک راهکار VDI مدرن و ایمن است که دسکتاپ‌های کاربران را در قالب کانتینرهای لینوکسی روی یک بستر کلاستری مبتنی بر کوبرنتیز اجرا می‌کند. کاربران از راه دور و از هر دستگاهی می‌توانند به دسکتاپ خود متصل شوند. این راهکار امکان جداسازی کامل بین شبکه‌ها و محیط‌های کاربری را فراهم می‌کند و می‌توان از آن برای سناریوهایی مانند ارائه اینترنت کنترل‌شده روی کلاینت‌های کاربری، ایزوله‌سازی مرورگرها و تفکیک سطح دسترسی کاربران در محیط‌های حساس استفاده کرد.

ویژگی‌ها و کاربردها:

- مدیریت متمرکز دسکتاپ‌ها از طریق کنسول واحد
- امنیت بالا با استفاده از WebRTC، gVisor و Seccomp به همراه ایمن‌سازی کامل زیرساخت کلاستر کوبرنتیز در برابر نفوذ، شنود و سوءاستفاده
- مقیاس‌پذیری افقی با کوبرنتیز
- پشتیبانی از احراز هویت یکپارچه با LDAP، OAuth۲ و ...
- مصرف بهینه منابع نسبت به VDI سنتی
- امکان مجازی‌سازی برنامه‌ها به صورت جداگانه
- کاربرد در سناریوهای جداسازی شبکه، BYOD ایمن، مرورگر ایزوله، و امنیت محیط کار از راه دور

خدمات امنیتی

- پیکربندی امن دارایی‌ها/ تجهیزات/ زیرساخت سازمان
- خدمات اصلاح و بهبود ساختار رویدادنگاری در سطح سرویس و ایجاد زیرساخت تحلیل داده
- پیکربندی و استقرار تجهیزات امنیتی نظیر فایروال و IPS/IDS
- پیکربندی و استقرار سامانه کنترل دسترسی و نظارت بر راهبران با بیشترین سطح دسترسی
- پیاده سازی چرخه DevSecOps و ارتقاء امنیت در فرآیند توسعه محصول
- پیاده‌سازی، امن‌سازی و نظارت بر زیرساخت‌های ابری
- خدمت تست نفوذ و تیم قرمز
- طراحی، پیاده سازی و استقرار مراکز عملیات امنیت
- استقرار و پیکربندی سرویس Vault مرکزی در سازمان
- مشاوره و ارزیابی در حوزه الزامات زیر ساخت کلید عمومی (PKI) و رمزنگاری

شرکت مهندسی فناوران

نقطه ایمن هوشمند

SMART SAFEPOINT TECHNOLOGY

info@safepoint-tech.ir

safepoint-tech.ir

تهران، آرژانتین، خیابان بخارست، کوچه مقدس (چهارم)، پلاک ۲

02188747697

02188514085