درباره ما

شرکت سامانه هوشمند سورنا در سال ۱۳۸۷ با اتکا به توان علمی، فنی و بیش از یک دهه فعالیت مدیران و کارشناسان خود تأسیس و به صورت تخصصی در حوزه فن آوری اطلاعات فعالیت می نماید. این شرکت، خدمات فن آوری اطلاعات را در قالب پروژه‌های طراحی و پیاده‌سازی شبکه‌های کامپیوتری، طراحی و پیاده‌سازی مراکز عملیات و مانیتورینگ شبکه(NOC)، طراحی و پیاده‌سازی مراکز عملیات امنیت شبکه(SOC)، طراحی و پیاده‌سازی گروه‌های واکنش هماهنگ رخداد(CERT) و راهکارهای جامع امنیت اطلاعات ارائه می‌دهد. رویکرد این شرکت به‌گونه‌ای است که علاوه بر ارائه مشاوره و راه‌حل‌های تخصصی، تجهیزات و ابزارهای موردنیاز مشتریان نیز را فراهم ساخته تا عملاً راهکاری یکپارچه را در اختیار آن‌ها قرار دهد.

اصول و ارزش‌های شرکت سامانه هوشمند سورنا که مأموریت شرکت را تعریف و پی‌ریزی می‌کند:

- **قابلیت اعتماد**

صداقت و اخلاق‌گرایی سرلوحه عملکرد مدیران و کارکنان سامانه هوشمند سورنا است. تلاش کارشناسان و متخصصین بر آن است که در پیشبرد اهداف و پروژه‌های مشتریان، تمام توان خود را بکار گرفته و از هیچ کوششی دریق نورزند.

- **ارج نهادن به حقوق مشتری**

تکریم و مراعات حقوق مشتریان، رویکرد شرکت سامانه هوشمند سورنا در طول دوران فعالیت خود بوده است. کارکنان شرکت با ذهنی باز و نگاهی روشن، شنوای مشکلات فنی و چالش‌های تخصصی مشتریان بوده و با شکیبایی پاسخ‌گوی آن‌ها بوده‌اند. دوستان امروز ما، مشتریان دیروز این شرکت بوده‌اند.

- **همکاری**

طراحی و پیاده‌سازی پروژه‌های نوظهور فن‌آوری اطلاعات، اغلب پیچیدگی‌های خاصی را به همراه دارند که کارشناسان را در انجام صحیح آن‌ها با چالش روبرو می‌سازند. تفکر مدیران شرکت سامانه هوشمند سورنا بر این باور استوار است که مرتفع نمودن مشکلات و ارائه راه‌حل، جز با همکاری گروهی و اشتراک مساعی تحقق نمی‌یابد.

- **نوآوری**

نوآوری در ارائه راهکار، از ویژگی‌های مهم شرکت سامانه هوشمند سورنا محسوب می‌گردد. پیشرفت سریع فن‌آوری اطلاعات و ارتباطات، طراحان و متخصصان این شرکت را بر آن می‌دارد تا همواره دانش خود را به‌روز نموده و مطابق با نیاز مشتریان، راهکار مناسب را در اختیار آن‌ها قرار دهند.

- **مسئولیت‌پذیری**

شرکت سامانه هوشمند سورنا همواره از مشتریان خود حمایت می‌کند. یکی از نکات تأثیرگذار در استمرار کسب وکار این شرکت در قالب قراردادها و تعهدات، پاسخ‌گویی و پیگیری مستمر مشکلات مشتریان بوده است. شرکت سامانه هوشمند سورنا در زمینه پشتیبانی از پروژه‌های فنی و خدمات پس از فروش محصولات نرم‌افزاری و سخت‌افزاری، تجارب درخشانی دارد.

چشم‌انداز شرکت سامانه هوشمند سورنا

چشم‌انداز شرکت سامانه هوشمند سورنا تا سال ۱۴۰۴ آن است که با اتکا بر نقاط قوت منحصربه‌فرد خود، نیازهای مشتریان را بررسی نموده و یکی از چند شرکت برتر در ارائه خدمات فنی- مهندسی و عرضه محصولات تخصصی فن‌آوری اطلاعات باشد.

SOPHOS

محافظت به سبک
SOPHOS

با توجه به اینکه هر روز از روش های جدید و متعددی جهت اجرای حملات سایبری به شبکه داخلی استفاده می شود، این نیاز احساس می شود که سازمان ها از سیستم های یکپارچه امنیتی، همانند Next Generation Firewall و Unified Threat Management استفاده کنند تا کلیه نیازهای مدیران شبکه را برای برقراری امنیت شبکه تامین نمایند .

شرکت سوفوس با تولید محصولات آنتی ویروس و رمزنگاری در سال ۱۹۸۵ شروع به فعالیت نمود و در حال حاضر، افراد زیادی از محصولات این شرکت استفاده می کنند. این شرکت امنیتی، تمرکز خود را بر روی ساده سازی و یکپارچه سازی راه کارهای امنیت شبکه گذاشته است. Sophos توانسته است در زمینه های مختلف امنیت شامل: نرم افزار، سخت افزار، ارتباطات، رمزنگاری، امنیت شبکه، امنیت پست الکترونیکی و امنیت دستگاه های همراه، محصولات مختلفی ارائه نموده و بیش از هرچیز، در زمینه سخت افزارهای UTM Sophos ، دستگاه هایی با کارایی بالا و بهینه سازی شده عرضه نماید.

در بخش سخت افزار و زیر مجموعه UTM ها ، سوفوس در دو سری مجزا SG و XG تقسیم بندی شده که شایان ذکر است، سری SG دیگر تولید نشده و جایگزین آن سری XG می باشد.

شما برای راه اندازی سخت افزارهای سوفوس (فایروال) نیاز به تهیه لایسنس دارید، لایسنس تهیه شده بنا بر نیاز سازمان و متناسب با زیرساخت شبکه تهیه شده و میبایست در پروفایل اختصاصی به نام سازمان (مشتری) تحویل گردد. در غیر اینصورت شما نه تنها صاحب لایسنس نیستید بلکه برای تمدید مجدد آن در موعد سررسید مجبور به تهیه آن از همان تامین کننده قبلی خواهید بود، زیرا که سوفوس آن شرکت را به عنوان صاحب لایسنس تلقی کرده و پروفایل به نام و در اختیار تامین کننده می باشد.

لازم به توضیح است در سری محصولات SG ، یکی از پارامترهای مهم اثبات مالکیت و همچنین تمدید مجدد، ACT Key میباشد که تامین کننده موظف به ارائه آن به خریدار نهایی است.

همچنین اگر شما از محصولات سری قدیمی SG سرویس دریافت میکنید ، میتوانید به راحتی به سری محصولات جدید XG مهاجرت نمایید. کافیست هنگام تهیه لایسنس، از لایسنس New برای سری XG بهره بگیرید. این مهاجرت در محصولات Cyberoam نیز قابل اجراست.

برای شبکه ها با n تعداد کاربر، این قابلیت فراهم شده است که امکانات امنیتی قدرتمند Sophos را با کمک یک واسط تحت web ، در اختیار داشته و به آسانی آن را مدیریت کرد.

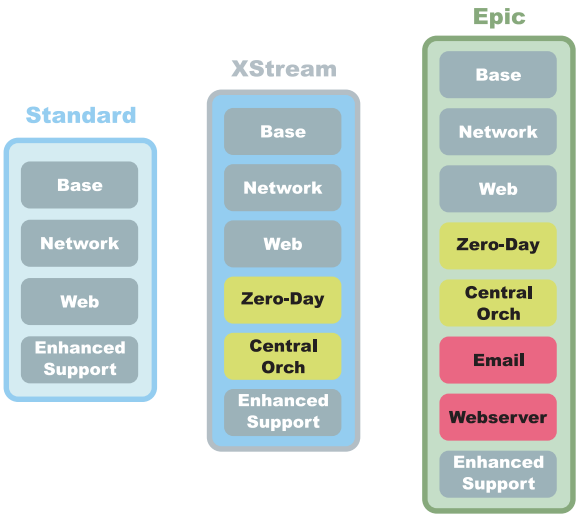
در ذیل به برخی از مزایای استفاده از فایروال های سوفوس اشاره می کنیم:

- قدرتمند و اقتصادی
- توقف تهدیدات ناشناخته توسط فایروال
- استفاده از هوش مصنوعی
- شناسایی اکسپلویت ها
- سازگاری با تجهیزات و زیرساخت شبکه سازمان
- ارائه راهکارهای عالی برای Accounting

فایـــــروال Firewall

محافظت به سبک SOPHOS

همانطـور که پیش تر اشـاره شد، برای استفـاده از محصولات سخت افزاری سوفـوس (فایروال ها) نیـاز به لایسنس دارید که در ادامـه به انواع لایسنس و کارایی آن ها اشاره میکنیم :



نکات مهمی که میبایست در خرید لایسنس مد نظر قرار دهیم :

دریافت و درخواست ثبت لایسنس در پروفایل اختصاصی

ارائه بستر مناسب از طرف تامین کننده و یا خریدار برای جلوگیری از بلاک شدن لایسنس و دستگاه

انتخاب نوع لایسنس متناسب با نیاز سازمان

بروز رسانی لایسنس از طریق سرورهای اصلی SOPHOS

FORTINET

امنیت، سرعت و اطمینان
FORTINET

فایروال ها به عنوان اولین خط دفاعی در برابر تهدیدات خارجی،بدافزارها و هکرهایی که قصد دسترسی به اطلاعات و سیستم های شما را دارند شناخته می شوند. اگر نگاهی به گذشته بیندازیم، رسالت اصلی فایـروال در واقع جداسازی داده های امن از یک ناحیه نا امن و کنترل ارتباطات بین این دو است. اما امروزه این سرویس ها کاربردهای مختلفی دارند و گستره وسیعی از امکانات و قابلیت ها را ارائه می دهند.

FortiGate از سری محصولات شرکت Fortinet می باشد که کلیه کنترل های امنیتی مورد نیاز برای تامین امنیت مبادی ورودی و خروجی ترافیک را در قالب یک ساختار یکپارچه ارائه کرده است.

ساختار فورتی گیت به نحوی طراحی شده است که فارغ از گستردگی و پیچیدگی شبکه های سازمان ها می تواند بیشینه سیاست ها و کنترل های امنیتی را در شبکه پیاده سازی و امنیت بهینه و مطلوبی را به ارمغان آورد.

شرکت فورتی نت پیشرو در ارائه راه حل های امنیتی و مبتکر ایده های نوین در زمینه شبکه،با ارائه فایروال اختصاصی خود به نـام FortiGate که به عنوان هسته اصلی محصولات این شرکت به شمـار می رود، مجموعه بی نظیری از ویژگی های امنیتی را برای مدیران فراهم آورده است. امروزه دیگر فایـروال های سنتی پاسخگوی این حجـم از تهدیدات نبوده و قـادر به تامین امنیت سازمـان ها نیستند. نسل جدید فایـروال های فورتی گیت که با عنوان Next Generation Firewall (NGFW) شناخته می شوند ، در زمینه امنیت پیشرفت قابل ملاحظه ای کرده اند، فایروال های فورتی گیت برای محافظت از سازمان ها در برابر تهدیدات داخلی و خارجی، ترافیک شبکه را فیلتر می کنند.

این محصولات در کنار برخورداری از امکاناتی از قبیل فیلتر کردن بسته ها، مانیتورینگ شبکه، پشتیبانی از IPsec و SSL VPN ، محتـوای انتقال یافته در شبکه را به صورت عمیق تر بررسی می‌کنند.این قابلیت ها توانایی شناسایی حملات، بدافزارها و سایر تهدیدات را فراهم می‌کند. فایروال های نسل جدید فورتی گیت، با ارائه چندین رابط پرسرعت، تراکم پورت بالا و توان عملیاتی بسیار زیاد، محصولی ایده آل برای استقرار در لایه امنیتی شبکه سازمان ها و مراکز داده هستند.

فایروالها در سه دسته مجزا متناسب با نوع نیاز سازمان تقسیم بندی می شوند :

High-End Firewalls

فایـروال های دسته High-end با دارا بودن نسل جدیـد پردازنده های SPU ، توان عملیـاتی بسیار بالایی دارند و از چندین درگاه پر سرعت برخوردار هستند. فایـروال های این رده توانایی برقراری حداکثـر ۱۰ میلیون ارتباط (Session) همزمان در ثانیه را دارند و به گونه ای بهینه شده اند که مناسب سازمان های بزرگ (Enterprise) ، سرویس دهنده های اینترنت (ISP) و مراکز داده هستند.

حداکثر ترافیک خروجـی در فایروال های سـری High-End فورتی گیت، ۱۵ / ۱ ترابیت بر ثانیه است. این فایروال ها بیشترین بازدهی را در سرویـس های Threat Protection (ماکزیمم ۷۵ گیگابیت بر ثانیه) و SSL Inspection (ماکزیمم ۹۴ گیگابیت بر ثانیه) ارائه می دهنـد. فایروال های سری High-end فورتینت شامل مدل های سری ۱۰۰۰ ،۲۰۰۰، ۳۰۰۰ و ۴۰۰۰ هستند.

Mid-Range Firewalls

فایروال های میان رده فورتی گیت،علاوه بر عملکرد بالا، امنیت پیشرفتـه چندلایه و دامنه دید گستـرده تری را برای محافظت در برابر حملات سایبـری فراهم می کنند. حداکثر ترافیک خروجـی در فایـروال های میان رده فورتی گیت، برابر با ۲۵ گیگابیت بر ثانیه است و امکـان برقراری ماکزیمم ۱۱ میلیون ارتباط (Session) همزمان در این فایروال ها وجود دارد.

این فایروال‌ها برای استفاده در سازمان‌های متوسط تا بزرگ بهینه شده‌اند و قادر هستند در دمای منفی۵۳ درجه تا مثبت ۷۰ درجه سانتیگراد به فعالیتشان ادامه دهند.

مدل های تولید شده در این رده شامل سری ۹۰۰ ، ۸۰۰ ، ۶۰۰ ، ۵۰۰ ، ۴۰۰ ، ۳۰۰ ، ۲۰۰ و ۱۰۰ می باشد.

FORTINET

امنیت، سرعت و اطمینان

FORTINET

Entry Level Firewalls

فایروال‌های این دسته که فورتی نت از آن‌ها به عنوان Branch Office هم یاد می‌کند، از بهترین محصولات درکلاس خود به شمار می روند. این فایروال ها مقرون به صرفه بوده و از توان پردازشی نسبتا پایینی برخودار هستند.

حداکثر ترافیک خروجی قابل پشتیبانی در این محصولات به ۱۰ گیگابیت برثانیه می‌رسد و امکان برقراری ۱/۵ میلیون ارتباط (Seisson) همزمان در آن ها وجود دارد. مدل های تولید شده در این رده، شامل سری ۸۰، ۶۰، ۵۰، ۳۰ و FortiGate Rugged است. فایروال های سری Entry-level امکاناتی از قبیل Threat Protection، IPsec VPN و SSL Inspection را ارائه می‌کنند و برای سازمان های کوچک و متوسط با حداکثر تعداد ۵۰ کاربر فعال مناسب هستند.

همانطور که میدانید سخت افزارهای امنیتی برای استفاده و ارائه سرویس به لایسنس نیاز دارند و محصولات فورتی گیت نیز از این بحث مستثنی نیستند. در نظر داشته باشید که لایسنس های Off-Line یا مستقر بر روی سرورهایی به جز خود فورتی نت ، لایسنس های اورجینال نبوده و درصورت اتصال دستگاه به اینترنت، ازطرف فورتی نت شناسایی و بلافاصله بلاک خواهند شد. درضمن لایسنس‌های آفلاین قابلیت های Antispam و Web filtering را ندارند .

لایسنس ها دارای پارت نامبرهای مختلفی هستند که هر پارت نامبر، فیچرها و سطوح خدمات پشتیبانی مختلفی را دارا می باشد، گفتنی است که اکثر لایسنس ها شامل: Antispam ، Web Filtering ، IPS, IDS ، OS و Antivirus می باشند.

در جدول ذیل میتوانید انواع لایسنس ها و تفاوتهای عملکردی آنها را بررسی بفرمایید:

Service	Advanced Threat Protection (ATP)	Unified Protection (UTM)	Enterprise Protection (ENT)	A La Carte Protection
Threat Intelligence Service				✔
Industrial Security Service			✔	✔
Security Rating			✔	✔
CASB			✔	✔
Web Filtering		✔	✔	✔
Antivirus+ Sandboxing	✔	✔	✔	✔
IPS	✔	✔	✔	✔
Antispam		✔	✔	
Internet DB	✔	✔	✔	
IP Reputation	✔	✔	✔	
Application Control	✔	✔	✔	

paloalto NETWORKS

دژی محکم به نام PaloAlto

شرکت Palo Alto یک شرکت آمریکایی فعال در زمینه امنیت سایبری است که در سال ۲۰۰۵ در سانتا کلارا ایالت کالیفرنیا تاسیس شد. محصول اصلی این شرکت که در حقیقت هسته مرکزی را تشکیل می دهد و پلت فرمی برای مقابله با تهدیدات امنیتی فضای سایبری می باشد، فایروال PaloAlto است. این شرکت بیش از ۶۰.۰۰۰ سازمان را از ۱۵۰ کشور دنیا پشتیبانی می کند و نکته جالب این است که ۸۵ شرکت از ۱۰۰ شرکت برتر لیست Fortune از مشتریان این شرکت می باشند که همین موضوع نشان از کیفیت بالای خدمات و محصولات شرکت Palo Alto می باشد. شرکت Palo Alto پذیرای ۴۲ واحد تحقیقات امنیتی وهمچنین کنفرانس های امنیتی می باشد و این موضوع نشان از میزان توجه و اهمیت این شرکت نسبت به مقوله امنیت می باشد. همچنین این شرکت در رده هشتم ۱۰۰ شرکت دیجیتالی Forbes قرار دارد.

شرکت Palo Alto اولین فایروال خود را در سال ۲۰۰۷ که یک فایروال پیشرفته سازمانی بود و همچنین در حقیقت اولین Next-Generation Firewall بود را روانه بازار کرد. فایروال های نسل آینده شرکت PaloAlto قادر هستند که کنترل برنامه ها، کاربران و محتویات را با سه فناوری شناسایی منحصر به فرد Content-ID، User-ID ، App-ID انجام دهند. سه روشی که جایگزین روش های فایروال های قدیمی و UTM ها که براساس IP Address ، Port و Packet انجام می شدند. این روش های شناسایی استفاده Application ها را در استفاده های یک سازمان ایمن می نماید و جایگزین روشهای سنتی کنترل پورت ها که توسط روش های گذشته پیاده سازی می شدند، خواهند شد .

محصولات شرکت Palo Alto با محافظت از هزاران شبکه سازمانی تجاری، دولتی و ارائه دهنده خدمات، عصر نوینی در امنیت سایبری ایجاد کرده اند. پلتفرم امنیتی کاملا موثر این شرکت، تمامی تجهیزات و عملکردهای امنیتی اصلی شبکه ازجمله فایروال های نسل جدید، فیلترینگ URL ، IDS/IPS و سیستم های دفاعی پیشرفته را در کنار هم قرار می دهد. به دلیل آنکه این تجهیزات از ابتدا با هدفی مشخص در این پلتفرم قرار داده شده اند و اساسا اطلاعات مهمی را با توجه به مقررات خاص به اشتراک می گذارند :

این محصول می تواند شکاف های موجود در وضعیت امنیتی یک سازمان را از بین ببرد چرا که پروتکل های امنیتی درستی را ارئه می دهد و از آنها در مکان مناسب درشبکه استفاده می کند.

در ذیل به برخی از ویژگیهای اصلی PaloAlto اشاره میکنیم :

- امکان رمزگشایی ارتباط TLS/SSL کاربران و قابلیت نظارت عمیق بر جزئیات بسته های شبکه
- قابلیت حفاظت علیه تهدیدات امنیتی پیشرفته (ATP) و مقابله با حملات هدایت شونده سایبری
- امکان فیلترینگ پیشرفته کاربری تحت وب و کنترل دسترسی به وب سایت های مشکوک
- قابلیت امنیت DNS با تشخیص و جلوگیری از حملات
- بهره گیری از سرویس ابری پیشرفته ضدبدافزار WildFire با قابلیت تشخیص حملات zero-day
- امکان بهره گیری از اطلاعات Cortex XDR agent روی پایانه های انتهایی برای تشخیص تهدیدات درون سازمانی
- قابلیت گردآوری و تحلیل خودکار لاگ وقایع امنیتی روی سرویس ابری Cortex Data Lake جهت رسیدگی به رخدادها
- امکان ارائه به صورت VM جهت حفاظت از ارائه دهندگان خدمات ابری خصوصی، دریافت کنندگان سرویس های عمومی خدمات ابری عمده(AWS ، Azure و...) و شبکه های نرم افزار فرمان - (SDN)
- قابلیت اجرای واکنش خودکار به تهدیدات امنیتی

- IPS/App-ID/User-ID/Content-ID
- Antivirus
- Botnet Protection
- Data Filtering
- URL Filtering
- Networking & VPN
- Redundancy and Resiliency
- Centralized Management
- Application Visibility
- Decryption
- Policy Control
- Device Management

JUNIPER NETWORKS

محافظت تمام عیار JUNIPER

همانطور که میدانیم سبد محصولات Juniper بسیار گسترده و متنوع میباشد که ما در بخش امنیت شبکه ، به ارائه خدمات در زیر مجموعه UTM این برند یعنی سری SRX خواهیم پرداخت. فایروال های جدید کمپانی Juniper سری SRX، به عنوان یک راهکار جدید و کامل در حوزه ی فایروال های مجازی به شمار می رود که امنیت در سطح پیشرفته را در جهت مدیریت Policyها را برای سرویس دهندگان و سازمان ها فراهم می نماید. با استفاده از SRX متخصصان امنیتی قادر خواهند بود فایروال را برای محافظت در محیط های کاملا Dynamic پیاده سازی نموده و توسعه دهند.

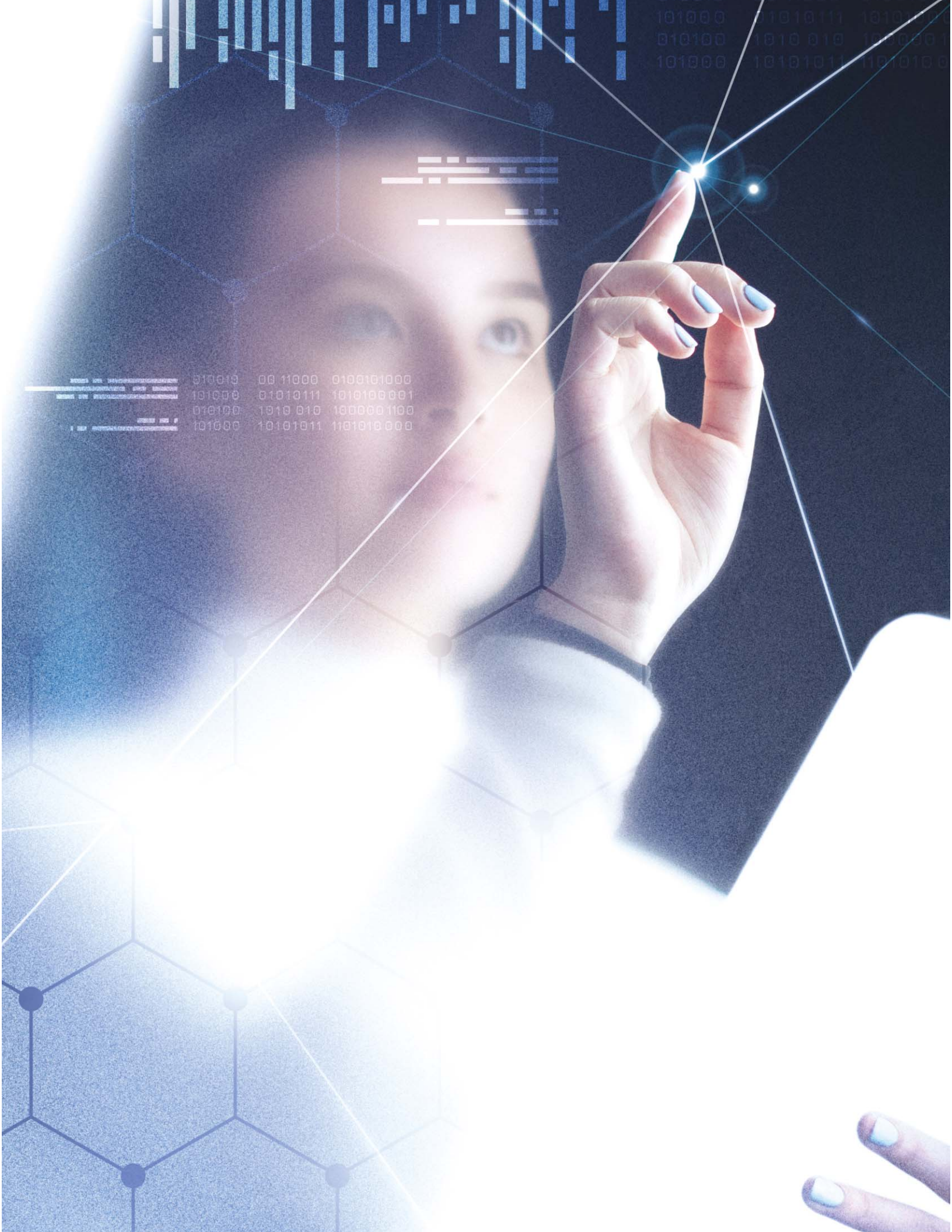
پیاده سازی Virtualized Network Function یا به اختصار VNF، به روند دستیابی به یک وضعیت امنیتی مطلوب و پایدار کمک می نماید. با این وجود اکثر VNF ها به دلیل اندازه و زمان Boot شدن خصوصا در هنگام ارائه برای سرویس های امنیتی، جهت پیاده سازی های سریع مناسب نخواهند بود. VNF در یک بازه زمانی سه دقیقه ای Boot شده و نیاز به تخصیص منابعی مانند VCPU و VRAMبه صورت Static دارد. هرچند ممکن است این موضوع برای محیط های فعلی قابل قبول باشد، اما اغلب مشتریان، به دنبال افزایش وسعت پوشش دهی امنیتی زیرساخت خود بوده و VNFهای امنیتی کوچک تر و سریع تری را ترجیح می دهند که فضای کمتری را نیز اشغال می کنند. Juniper با ارائه سرویس امنیتی VNF در یک نسخه Container شده از Networks SRX Series Services Gateways، به پوشش این نیازها می پردازد. فایروال SRX Container به سازمان ها و سرویس دهندگان اجازه می دهد تا چابکی و میزان پیاده سازی سرویس های امنیتی پیشرفته را افزایش دهد.

برخی از ویژگی های فایروال های سری SRX Juniper :

- امنیت برای هر سایز دیتاسنترها و شبکه
- محافظت جامع از تهدیدات
- حداکثر کارایی و مقیاس پذیری
- قابلیت استفاده در سیستمهای مخابراتی
- ارزش امنیتی عالی
- امکانات امنیتی مجازی

فایـــــروال Firewall


SOPHOS
FORTINET
paloalto NETWORKS
JUNIPER NETWORKS
splunk>
hp ArcSight An HP Company
KASPERSKY lab
IMPERVA Protecting the Data That Drives Business
PENETRATION TESTING
nessus Professional
CORE SECURITY
metasploit RAPID7
HCL AppScan
PRTG NETWORK MONITOR
safetica
beSTORM
solarwinds
VEEAM Modern Data Protection
forensic
Symantec
ZECURION
ESET
CANVAS



splunk>

مدیریت رخداد
splunk>

Splunk نرم افـزاری است که عمدتاً برای جستجـو، نظارت و بررسـیBig Data تولید شده توسط ماشیـن از طریق رابط کاربـری تحت وب استفاده می شود. این ابزار، ثبت، نمایه سازی (ایندکسینگ) و ارتباط داده های واقعی را در یک محیط قابل جستجو انجام می دهد که از طریق آن می تواند نمـودارها، گزارش ها، هشـدارها و داشبورد های مختلف را ایجاد کرد. این هدف برای ایجاد خوانـایی داده های تولیـد شده توسط ماشیـن در سراسر سازمـان است. اسپلانک قادر به تشخیص الگـوهای داده، تولید معیارها، تشخیص مشکلات و اسـتفاده از هوش ماشین برای اهداف عملیات تجاری است. اسپلانک یک فناوری است که برای مدیریت برنامه ها، امنیت و انطباق استفاده می شود، و همچنین برای تجزیه و تحلیل کسب وکار کاربردی است.

Splunk پلت فـرمی است که در دستیابی به داده های تولیـد شده از دستگـاه ها به ما کمک می کنـد تا این داده ها مفیـد و ارزشمند شوند. پـردازش و تجزیـه و تحلیل حجم عظیمـی از داده ها یکی از بزرگتـرین چالش ها است، زیرا داده های زیادی در بخش IT و سیستـم های آن وجود دارد. در این شرایـط، اسپلانک برای مقابله با اوضـاع نقش اسـاسی دارد . به عنـوان مثـال، فرض کنیـد شما یک مدیر سیستم هستید و باید دریابید که چه اشتباهی در دستگاه و یا سیستمی که با آن کار می کنید وجود دارد.

به داده های تولید شده در دستگاه نگـاهی بیندازید تا از آنها ایده بگیرید . ساعتها طول می کشد تا بفهمید چه مشکلی در سیسـتم شما وجود دارد . اکنون، این جا زمانی است که Splunk وارد صحنه می شود. این ابزار کلیه کـارهای سنگین را برای شـما انجام می دهد، یعنی پردازش کل داده های ایجاد شده توسط دستگاه ها و سیستم های شما، و پس از به دست آوردن داده های مربوطه، پیدا کردن مشکلات بسیار ساده تر خواهد بود .

مزایای استفاده از اسپلانک :

- ایجاد گزارش های تحلیل شده همراه با نمودارها و جداول مربوطه.
- پیاده سازی آسان و منعطف.
- شناسایی داده های مخرب / مفید در بین اطلاعات شما که باعث صرفه جویی در زمان جستجو می گردد.
- سطح بالای سازگاری با داده های مختلف.
- هزینه خرید به مراتب پایین تر نسبت سایر رقبا از جمله HP ArcSight و IBM Qradar
- قابلیت پیاده سازی به صورت On-Premise ، Cloud و ترکیبی از این دو حالت.

پس از معرفی و توضیح مختصـر درباره ی ابزار اسپلانک و همچنین اشاره گذرا به برخی از ویژگـی های آن ، وقت آن است که برای استفاده از این ابزار ، لایسنس آنرا تهیه کنـیم. برای دریافت لایسنس شما نیاز به دانستن میـزان ترافیک ورودی/خروجی شبـکه خود را دارید که پارامتـر اصلی تعیین قیمت می باشد. در ادامه فرمـول محاسبه قرار داده شده است. نکته مهم این است که قیمت لایسنس این ابزار گران بوده و بیشتر برای موسسـات و مراکـز بزرگ مورد استفاده قرار می گیـرد، در نظر داشته باشیـد که این لایسنس می بایست در پروفـایل اختصاصـی بصورت کامـل تحویل گردد در غیر اینصـورت امکـان استفاده از یک لایسنس بصورت اشتـراکی Share وجود داشتـه و صدمات جبـران ناپذیری را به سازمان وارد خواهد کرد.

splunk>

مدیریت رخداد splunk>

مدیریت رخداد SIEM

Splunk Enterprise (With ES Module)

ضرورت بهره گیری از یک تکنولوژی در مرکز عملیات امنیت شبکـه با توجه به تنوع بالای تجهیزات شبکه وحجم بالای وقایع (Logs) حاصل شده از تجهیزات مشخص می شـود، به طوری که بدون بهره جستن از سیستـم های پیشرفتـه نرم افـزاری، شاهد تأثیر خطای انسانی در نتایج حاصل شده ازتحلیل و بررسی رخدادها خواهیم بود.

بالارفتن احتمال خطا موجب ایجاد سطح اطمینـان پایین و وضعیت نامناسب نسبت به پاسخگـویی صحیح در قبـال وقایع امنیتـی خواهد شد. درنتیجه، مدیریت رویدادها و تهدیدات امنیتی در چنین شبکه های گسترده از عهده نیروی انسـانی خارج می باشد، لذا استفاده از یک سیستم مکانیزه یکپـارچه با ساختاری مبتنی بر معماری توزیع شده با نام سامانه مدیریت اطلاعات و رخدادهای امنیتی یا SIEM جهت جمع آوری و مرتبط سازی رویدادهای امنیتی گزارش شده از سوی سامانه های نامتجانس و نقاط مختلف شبکه نیاز می باشد.

محصول Splunk Enterprise در کنار ماژول Enterprise Security (ES) یک SIEM قدرتمنـد را تشکیل می دهد. از این سیستـم به عنوان مغز متفکر مراکز کنترل و عملیات امنیت شبکه ی SOC یاد می شود، که قادر است هزاران رخداد از سامانـه های مختلف راجمع آوری کرده و با ذخیـره سازی طولانی مدت آنها، امکاناتـی از قبیل نمایـش و تحلیل بلادرنگ رخـداد ها، برقـراری ارتباط میـان رخدادهـای مختلف، شناسایی رفتارهای مشکوک کاربران با استفاده از الگوریتم های یادگیری ماشین، تولیدگزارش های متنوع، تحلیل وقایع و رخدادها بعد از وقوع رویدادهای امنیتی و حوادث، اعلام هشدارها درسطوح مختلف و ... را داشته باشد .

محصول Splunk پس از کسب اطمینان از جمع آوری متمرکز داده های لازم از سامانه ها و تجهیزات مختلف شبکـه، اقدام به نرمال سـازی، دسـته بندی و مرتبط سـازی داده های جمـع آوری شده نمـوده و بر اسـاس میزان ریسک اندازه گیـری شده برای هریک از رخـدادها، امکـان اولویت بندی تهدیدات شناسـایی شده را فراهـم می نماید. همچنیـن به عنوان یک سیستم نرم افزاری هوشمند قادر است تا با انجام محاسبات ریاضی پیشرفتـه بر روی سوابق رخدادهایی که در طـول زمان جمع آوری کرده، الگوهـای رفتاری نرمال و قابل پذیرش را تعیین نموده و موارد نقض این الگو ها را گزارش نماید.

[1] Security Information & Event Management

چرا هر شبکه نیازمند استفاده از SIEM است؟

- تنها راهکار جامع برای نظارت بر سیاستهای اداری سازمانها در زمینه استفاده از فناوری اطلاعات یک SIEM است .

- استفاده از تجهیزات پیشرفته شبکه و کامپیوتر به تعداد بالا، عملاً امکان نظارت از روشهای متداول بر شبکه را غیر ممکن می سازد. چرا که این تجهیزات در هر ثانیه صدها خبر از نحوه فعالیت خود ثبت می کنند و این تنها یک SIEM است که می تواند این اطلاعات را جمع آوری و پردازش نماید .

- نرم افزارهای ضد ویروس توانایی مدیریت اطلاعات از حملات ویروسی به شبکه را نداشته و به تنهایی امکان تشخیص حملات سایبری به شبکه را ندارند .

- یک SIEM مجهز به امکانات تشخیص ناهنجاری و بصری نمودن اطلاعات، می تواند به تشخیص حملات جدید که هنوز برای مدیران شبکه یا نرم افزارهای ضد ویروس آشنا نیستند، کمک بسیار نماید .

- نرم افزارهای ضد ویروس، Firewall ها، IDS ها و.... همگی به تنهایی فعالیت می کنند و امکان فعالیت گروهی، تبادل اطلاعات یا تحلیل وضعیت کار یکدیگر را ندارند و به همین علت در تشخیص حملات عموماً ضعیف عمل می کنند. در حالی که یک SIEM با دسترسی به Log های این دستگاهها، یک تحلیل عمومی و یکپارچه از وضعیت کلی شبکه به کارشناسان و مدیران ارائه می کند .

یک راهکار یکپارچه SIEM با ارائه انواع گزارشها، توانایی کمک به یافتن شواهد، علل و ریشه های حمله صورت گرفته را دارد.

splunk>

مدیریت رخداد
splunk>

قابلیت های محصول Splunk Enterprise with ES Module

محصول Splunk دارای ویژگی ها و قابلیت های فنی زیر می باشد:

- قابلیت دریافت event مربوط به انواع تجهیزات مختلف و سرویس ها
- قابلیت دریافت و نرمال سازی لاگ با فرمت های مختلف
- قابلیت دریافت و آنالیز امنیتی ترافیک Netflow از تجهیزات شبکه و امنیت شبکه
- قابلیت استخراج لاگ خام (Raw Log)
- قابلیت حفظ محرمانگی در ارسال، و دریافت و ذخیره سازی Event ها
- قابلیت توسعه پذیری به نحوی که با افزایش میزان ترافیک و رویدادهای تولیدی، خللی در عملکرد SIEM وارد نشود.
- قابلیت دریافت و ارسال رخدادهای امنیتی از انواع SIEMها
- قابلیت پیاده سازی به صورت توزیع شده (Distribute)
- قابلیت UBA (User Behavior Analytics)
- قابلیت جمع آوری داده ها و تولید انواع گزارش های آماری و ویژوالی

سرویس Splunk Enterprise with ES module به صورت On-Premise

نحوه ی ارائه سرویس Splunk Enterprise with ES module

یکی از چالش های سازمان های داخل کشور در ارتباط با سرویس های ابری، نگرانی در خصوص نشت اطلاعات و عدم حفظ محرمانگی می باشد. از آنجایی که سیاست سازمان ها در جهت حفظ محرمانگی اطلاعات ، اجازه ارسال log ها و رخداد های امنیتی تولید شده توسط تجهیزات و نرم افزار ها را به خارج از سازمان نمی دهند. در نتیجه سازمان ها، بانک ها و شرکت های دولتی و خصوصی جهت راه اندازی سرویس Splunk مجبور به خرید کامل محصول Splunk با لایسنس های مربوطه می شوند که هزینه ی آن قابل توجه می باشد. برای کاهش هزینه خرید لایسنس Splunk ، شرکت سامانه هوشمند سورنا محصول Splunk با ماژول Enterprise Security را به صورت سرویس ارایه می دهد. به این صورت که، بر اساس نیاز مشتری، نسخه و نوع لایسنس Splunk را در یک سرور فیزیکی مجزا نصب و راه اندازی کرده و همان سرور فیزیکی در Data Center مربوط به خود مشتری مستقر می شود.

splunk>

مدیریت رخداد splunk>

مزایای استفاده از سرویس Splunk Enterprise with ES module

- محرمانگی اطلاعات سازمان به طور کامل حفظ می شود به این صورت که تمامی لاگ ها و رخدادهای تولید شده تو سط تجهیزات امنیتی و نرم افزارها، در داخل خود سازمـان و به صورت local در سرور اختصاصـی مربوط به Splunk ذخیره سازی و تحلیل و ارزیـابی می شوند و هیچ اطلاعاتی از سازمان مربوطه خارج نمی شود.
- هزینه ارائه سرویس Splunk نسبت به هزینه خرید لایسنس Splunk حدود ۷۵ درصد پایین تر می باشد.
- لایسنس نصب شده به راحتی قابل ارتقاء می باشد.
- سرویس مورد نظر به صورت ۱، ۳ و ۵ ساله قابل ارائه می باشد.

Splunk Enterprise	سرویس ۱ ساله	سرویس ۳ ساله	سرویس ۵ ساله
حداقل حجم قابل ارائه	۵ گیگابایت	۵ گیگابایت	۵ گیگابایت
۱ گیگا بایت	۶۵ درصد تخفیف	۷۰ درصد تخفیف	۷۵ درصد تخفیف
Security Module(ES)	**سرویس ۱ ساله**	**سرویس ۳ ساله**	**سرویس ۵ ساله**
حداقل حجم قابل ارائه	۵ گیگابایت	۵ گیگابایت	۵ گیگابایت
۱ گیگا بایت	۶۵ درصد تخفیف	۷۰ درصد تخفیف	۷۵ درصد تخفیف

نکته: درصد تخفیفات براساس قیمت اصلی لایسنس Splunk می باشد.

مدیریت رخداد
HP Arc Sight

HP ArcSight ، یکـی از پیشگامان صنعت SIEM است که این محصـول قادر به جمع آوری، مجتمـع سـازی و همبسته سازی رویدادهـای امنیتی سرتاسر سـازمان یا شـرکت و همچنین مدیریت لاگ های آن می باشد. این محصـول از محصولات بخش Micro Focus شرکت HP می باشد. ArcSight به عنوان قلب مرکز SOC عمل کـرده و از فناوری هایی که برای تشخیص و پایش و پویش شبکه سازمان مورد استفاده قرار میگیرند (سیستم های تشخیص نفوذ شبکـه و میزبـان، دیـواره آتش، دیـواره آتش برنامه های کاربـردی وب، بررسی کننـده صحت فایـل، سیستم های جلوگیری از نشت اطلاعات، ضد بدافزارها، ابزارهای تشخیص کلاه برداری، ابزارهای تولید رویداد سیستم عامل ویندوز و لینوکس، پویشگـران آسیب پذیر)، رویـدادها و داده های متنـی را دریافت می کنـد و پردازش هایی را (بررسی و تائیـد رویدادها، همسان سـازی، پایش، تحلیل) روی آنها انجام داده و نتایج تحلیل های خود را به سایر فنـاوری ها (سیستم واکنش و پاسخ)، درصـورتی که برای ارائـه خدمات مرکـز SOC مورد نیاز باشد، ارسال می کند.

شرکت ArcSight محصول خود را به دو صورت ارائه میدهد :

- سخت افزار از پیش آماده شده (Appliance)
- به صورت بسته نرم افزاری

به نوع نرم افزاری محصول ESM و به نوع Appliance آن ESM Express یا ESM Appliance گفته می شود. نسخهESM Express به صورت پیش فرض دارای قابلیت های بیشتـری نسبت به ESM است. البتـه این قابلیت های بیشتـر روی ESM قابل اضافـه شدن هستند.

مزایای استفاده از : ArcSight

- ✓ جمع آوری و تجمیع logها از تمامی منابع IT (سازمان شبکه، امنیت و سرورها)
- ✓ مدیریت میلیون ها رویداد و اطلاعات امنیتی به منظور کسب درک جامعی و عمیق از فعالیت های تهدیدآمیز
- ✓ نظارت بر کاربران به منظور شناسایی و جلوگیری از فعالیت های غیرمعمول و تهدیدآمیز
- ✓ مدیریت پیکربندی شبکه و اصلاح معایب آن
- ✓ شناسایی و رفع سریع آسیب پذیری های امنیتی مهم و پرخطر در سرویس ها و وب اپلیکیشن های سازمان
- ✓ ایجاد گزارشات دقیق، انعطاف پذیر و در فرمت های مختلف مد نظر سازمان
- ✓ اعمال سیاست های IT جهت تخصیص منابع شبکه و پهنای باند
- ✓ بروزرسانی و پشتیبانی توسط ماهرترین متخصصین در تیم های Fortify ، ArcSight ، DVLabs و HP Labs
- ✓ دارای مدل های Express ، Logger و ESM

تست نفوذ چیست ...
Pen Test

در خدمات« تست نفوذ » فرد یا تیم ارزیاب تلاش می کنند در مدت زمان تعیین شده، بیشترین تعداد آسیب پذیری در بخش مورد ارزیابی را شناسایی و صحت آن را بررسی و تایید کنند. بخشی از این فرآیند با استفاده از ابزارهای خودکار (مشابه ابزارهای ارزیابی آسیب پذیری)، بخشی با ابزارهای نیمه خودکار(مانندBurp Suite ، Metasploit و غیره) و بخشی دیگر که توسط این ابزارها قابل بررسی نیست به صورت دستی انجام می شود .

همچنین تیم یا فرد ارزیاب در تست نفوذ پا را از« ارزیابی آسیب پذیری ها » فراتر گذاشته و علاوه بر موارد ذکر شده، تلاش می کند تا در صورت نیازآسیب پذیری های پیدا شده را به منظور بررسی سطح مخاطره یا شناسایی گام های بعدی ارزیابی، Exploit کند.

در ادامه، تیم ارزیاب گزارش فعالیت ها و یافته های خود را با جزییات کامل به سازمان کارفرما ارایه می دهد. در نتیجه سازمان به دید عمیق تری نسبت به مخاطرات موجود در کسب وکار خود دست پیدا خواهد کرد. تست نفوذ می تواند با تمرکز بر دارایی های مختلف سازمان مانند سرویس های تحت وب، نرم افزارهای موبایل، زیرساخت شبکه و غیره اجرا شود . به طور کلی میتوان مراحل تست نفوذ را به ۵ بخش اصلی تقسیم کرد :

برنامه ریزی و شناسایی

در این مرحله هدف و محدوده تست نفوذ، از جمله مشخص کردن سیستم هایی که قرار است تحت این فرایند قرار بگیرند و روش انجام آن، تعیین می گردد.

اسکن

حال، رفتار یک برنامه نسبت به انواع تست ها مورد بررسی قرار می گیرد که خود شامل دو مرحله می باشد. در تحلیل ایستا کدهای یک اپلیکیشن بررسی می شود تا رفتار آن در حالت اجرا پیش بینی شود .

در این روش با یک اسکن تمامی کدها بررسی می شود. در تحلیل پویا کدهای برنامه زمانی که برنامه اجرا شده است مورد بررسی قرارمی گیرد. به دلیل اینکه با این روش می توان برنامه را به صورت بلادرنگ تحلیل نمود، کاربردی تر است.

ایجاد دسترسی

در این مرحله با استفاده از حملات مختلفی همچون تزریق SQL و ایجاد بک دورها، ایرادات برنامه تحت وب مشخص می گردد. سپس آزمایش کننده از این ایرادات استفاده کرده و با استفاده از روش هایی مثل دستکاری سطح دسترسی، سرقت داده ها و غیره، به اپلیکیشن نفوذ می کند. با این کار می توان میزان آسیب احتمالی این ایراد در صورت بهره جویی را مشخص کرد .

حفظ و تداوم دسترسی

در این بخش، هدف آزمایش کننده بررسی امکان حفظ و تداوم دسترسی در صورت سوءاستفاده از آسیب پذیری مورد نظر می باشد. بررسی مدت زمان حفظ این دسترسی نیز در دستور کار این مرحله قرار دارد زیرا یک بازیگر مخرب می تواند با تداوم دسترسی،سطح دسترسی خود را افزایش دهد .

در واقع هدف اصلی در این مرحله بررسی حملات APT یا تهدید های پیشرفته و مستمر می باشد که در آن مهاجم به سیستم نفوذ کرده و ماه ها در آن سیستم باقی می ماند و به جمع آوری اطلاعات حساس آن سازمان می پردازد .

تجزیه و تحلیل

در نهایت اطلاعات حاصل از تست نفوذ در یک گزارش دسته بندی می شود که شامل :

- ایرادات موجود در سیستم که قابل نفوذ و بهره جویی هستند .
- اطلاعات حساسی که می توان طی حملات به آنها دسترسی یافت .
- مدت زمانی که آزمایش کننده توانست بدون اینکه شناسایی شود، در سیستم باقی بماند .

این اطلاعات توسط تیم امنیتی بررسی شده و در نهایت ساختار و زیرساخت امنیتی سازمان دوباره تنظیم می گردد. علاوه بر این اپلیکیشن های دیگر نیز پچ می شوند تا از تهدیدات احتمالی آینده پیشگیری شود.

nessus Professional

اسکنر آسیب پذیری
NESSUS

یکی از بهترین ابزارهای ارزیابی میزان آسیب پذیری دستگاه های تحت شبکه ابزار Nessus Pro می باشد. از نقاط قوت این ابزار، راه اندازی و پیاده سازی آسان آن بوده و کاربر میتواند تسلط خوبی بر روی آن داشته باشد.گزارش های ارائه شده از طرف این ابزار بسیار سریع ، جامع و موثر بوده و نوع گزارش به نحویست که برای شناسایی و رفع آسیب بسیار موثر است.
لازم به توضیح است محصولات Nessus Pro در قالب ۱ ، ۲ و ۳ ساله عرضـه شده و در مقایسه با رقبای خود قیمتی بسیار منطقی و رقابتی دارد.پیشنهاد ما برای استفاده از این محصول مختص سازمانهای کوچک و متوسط خواهد بود.
Nessus یک انقلاب متفاوتی در ارزیابی میزان آسیب پذیری ایجاد کرده و کاملا فراتر از یک اسکنر شرکتی خودنمایی میکند. در آزمون های نفوذپذیـری، دو روش جعبه سفیـد و جعبه سیاه وجود دارد که Nessus قادر است بر پایـه ی این دو آزمـون عمل کند . Nessus از انـواع ساختـارهای مختلف به منظور اسکـن پشتیبانی می کند. این ساختارها شامل سیسـتم عامل های مختلف، انواع مجـازی سازها و پروتکل های شبکه می باشد. هستـه ی اصلی Nessus ، پلاگیـن های آن هستند. در واقع هریک پلاگیـن ها بیانگر یک آسیب پذیری است که Nessus آنها را در دسته بندی مشخصی قرار داده است.

هزینه مالکیت پایین

اسکن کامل آسیب پذیری ها با اسکن نامحدود در برابر IP های نامحدود در قبال هزینه ی پایین

تسهیل رشد و پیشرفت

مهاجرت ساده به tenable.io با استفاده از ابزارهای مهاجرت سریع و امکان انتقال از سیستم های مشابه در اختیار کاربر قرار می گیرد

سهولت در استفاده

ایجاد یک Policy بسیار ساده است و فقط نیاز به چند کلیک برای اسکن کامل کل شبکه دارد

حفاظت بی نقص

ارائه افزونه هایی که پاسخ های به موقع را برای آخرین آسیب پذیری ها ارائه می دهند

تشخیص جامع

پوشش تکنولوژی های بیشتر و در نتیجه شناسایی آسیب پذیری های بیشتر و میزان تشخیص بالا

سریع و دقیق

اسکن سریع با سرعت بالا با False Posstive کم، به شما امکان می دهد تا سریعا آسیب پذیری هایی را که برای اولین بار نیاز به پاکسازی دارند شناسایی کنید

CORE IMPACT

پویشگر امنیتی
Core Impact

نرم افزار Core Impact Pro جامع ترین نرم افزار جهت ارزیابی و تست آسیب پذیری های امنیتی سازمان . این پویشگر با بیش از ۱۵ سال سابقه ی کاری در زمینه ی امنیت وتحقیقات در بالاترین سطوح به شما این امکان را می دهد تا با آزمایش جدیدترین روش هایی که امروزه مجرمین سایبری از آن استفاده می کنند، وضعیت امنیتی سازمان خود را ارزیابی کنید .

برخی از ویژگیهای این پویشگر عبارتند از :

- بررسی محیط های چند تهدیدی
- اکسپلویت هایی با ارزش تجاری
- استفاده ی تیمی
- اعتبارسنجی اسکن آسیب پذیری
- تست نفوذ شبکه
- تست نفوذ شبکه های بیسیم
- رصد و مقابله با حملات به دوربین های مدار بسته
- تست نفوذ برنامه های کاربردی تحت وب
- تست نفوذ دستگاه های موبایل
- گزارش گیری افزونه ی ExCraft SCADA برای Core Impact Pro

پلتفرم هوشمند حمله ی Core Security از طریق مدل سازی، شبیه سازی و تست آنچه که یک مهاجم واقعی می تواند انجام دهد، به شما کمک می کند تا بر روی رفع محتمل ترین تهدیدهای سرمایه های حیاتی خود تمرکز کنید .

همچنین Core Impact می تواند نتایج به دست آمده از اسکنرهای آسیب پذیری وب و شبکه را دریافت کرده و امکان اکسپلویت شدن آنها را تایید کند.

این اسکنرها شامل موارد زیر می باشند:

™GFI LANguard	Security Scanner	eEye Retina® Network	Acunetix® Web Security Scanner
Lumension® Scan	®IBM Internet Scanner	®IBM AppScan	®HP Web Inspect
®Qualys QualysGuard	Rapid7 AppSpider	™TripWire IP360	McAfee® Vulnerability Manager
®Cenzic Enterprise	®Tenable Security Scanner	®Tenable Nessus	®SAINTscanner

metasploit®
RAPID7

اسکنر آسیب پذیری و نفوذ

Metasploit

Metasploit ابزار تست میـزان آسیب پذیری است که به صورت اختصاصـی برای تسترهای نفوذ ، هکـرها ، محققین امنیتـی و دیگـر فعالان موجود در زمینه امنیت شبـکه نوشته شده است . با استفاده از این فریم ورک می توان آسیب پـذیری های موجود در سیسـتم ها ، شبکه ها و نرم افزارهای گوناگون را شناسـایی کرده و به این سیسـتم ها نفوذ کنید . این اپلیکیشـن به صـورت پیش فرض دارای اکسپلویت های بسیاری می باشد که علاوه بر آن می توان اکسپلویت دلخواه خود را ایجاد کرده و به آن اضافه کنید .

Metasploit دارای ۲ نسخه می باشد که استفاده از هر نسخه به نیاز شما و سطح کاری که می خواهید انجام بدهید بستگی دارد .

- Metasploit Pro
- Metasploit Framework

استفاده از Metasploit برای نفوذ به یک سیستم معمولا شامل موارد زیر میشود :

۱. انتخاب یک اکسپلویت
۲. تنظیم آپشن ها و گزینه های اختیاری اکسپلویت
۳. انتخاب یک Payload
۴. تنظیم آپشن ها و گزینه های اختیاری Payload
۵. اجرا کردن اکسپلویت
۶. برقرارای ارتباط با سیستم مورد نظر Remote System
۷. اجرای فرایند نفوذ به سیستم مورد نظر

لازم به توضیح است در روش فوق برای نفوذ به سیستمها ، فقط باید در محیطهای شبکه ای مورد استفاده قرار گیرد که شما کنترل و یا مجـوز تست را دارید، زیرا ممکن است باعث آسیب و یا از دست دادن داده ها شود .

HCL AppScan

پویشگر امنیتی
HCL Appscan

HCL Security AppScan یکی از ابزارهای قدرتمند در حوزه ی ارزیابی امنیتی و آزمون نفوذ است که به افزایش امنیت برنامه های کاربردی تحت وب و برنامه های کاربردی موبایل کمک شایانی می کند. این ابزار همچنین مدیریت برنامه های امنیتی سازمان و برآورده کردن خط مشی های امنیتی را تقویت می کند . HCL Security AppScan با فراهم کردن آزمون امنیتی در چرخه ی طراحی و توسعه به پیاده سازی سیستم های امن مبتنی بر وب کمک می کند. این نرم افزار در هزینه و زمان آزمون امنیتی سیستم های مبتنی بر وب کمک به سزایی می کند و با به روزرسانی خود آخرین تهدیدات این حوزه را پوشش می دهد .لازم به توضیح است این ابزار پیش تر در سبد محصولات IBM بوده که هم اکنون توسط کمپانی HCL خریداری شده و به همین نام ارائه میگردد.

ویژگی های کلیدی HCL Appscan عبارت است از:

- تست امنیت اپلیکیشن مقیاس پذیر
- گزارشات امنیتی دقیق همراه با جزییات
- پالیسی های تست، قالب های پیش فرض اسکن
- مدیریت امنیت اپلیکیشن مبتنی بر ریسک
- فهرست اپلیکیشن و طبقه بندی خودکار دارایی ها
- اولویت بندی آسیب پذیری ها در محتوای اپلیکیشن
- رتبه بندی ریسک امنیتی خودکار
- ارائه توصیه های هوشمند جهت رفع آسیب پذیری های شناسایی شده
- تست جعبه سیاه و Glass Box جهت بررسی ساختار کد برنامه

نسخه های محصول AppSan:

- AppScan Enterprise: نسخه سرویس گیرنده/سرویس دهنده جهت اندازه گیری تست امنیتی
- AppScan Standard: نرم افزار دسکتاپی برای تست خودکار امنیت وب اپلیکیشن جهت استفاده کارشناسان IT و تست نفوذ
- AppScan Source: مورد استفاده جهت پیش گیری از نقض اطلاعاتی به کمک یافتن ضعف های امنیتی در کد منبع

مخاطبین پویشگر امنیتی HCL AppScan:

- سازمان های خصوصی و دولتی
- بانک ها و موئسسات مالی و اعتباری
- آزمایشگاه های ارزیابی امنیتی نرم افزار و تست نفوذ

پویشگر امنیتی CANVAS

پویشگر امنیتی Immunity Canvas ازشرکت Immunity یک نرم افزارامنیتی جهت انجام تست نفوذ و ارزیابی آسیب پذیری است. سازمان می تواند با این نرم افزارسازمان framework خود را جهت آشکارسازی میزان رخنه پذیر بودن آن از لحاظ امنیتی بررسی کند. Canvas با استفاده از exploit های موجود، یک سیستم خودکار آشکارسازی آسیب پذیری، یک فضای کاری قابل اعتماد جهت گسترش explot های موجود ارائه می دهد.

نرم افزار Immunity Canvas دارای یک بانک اطلاعاتی جامع، کامل و به روز از آسیب پذیری های امنیتی می باشد که امکان به روزرسانی بانک اطلاعاتی و ارتقاء پایگاه دانش آسیب پذیری های آن به صورت ماهانه وجود دارد. بر اساس داده های رسمی منتشرشده به طور میانگین، ماهانه ۴ آسیب پذیری Zero-Day به بانک اطلاعاتی آسیب پذیری های این نرم افزار اضافه می شود.

برخی از ویژگی های این ابزار عبارتند از :

- دارای ویژگی multi-threating جهت اجرای چندین exploit به صورت همزمان
- نرم افزاری جهت تولید و گسترش ابزارهای امنیتی جدید
- قابلیت تولید اکسپلویت های جدید با استفاده از MOSDEF
- قابلیت مکان یابی سیستم هدف و نمایش موقعیت آن در نقشه جهان
- قابلیت جمع آوری اطلاعات و شناسایی هدف و همچنین اسکن آسیب پذیری
- D2 Exploitation Pack : این بسته باعث می شود تا بتوان نتایج اسکنرهای آسیب پذیری را به آن Import کرده و همچنین درستی آن نتایج را تایید کرد .
- قابلیت انجام حملات Client Side و Server Side
- دارای تعداد زیادی Exploit و همچنین اضافه شدن چند اکسپلویت Zero-day از طریق به روزرسانی به صورت ماهانه
- قابلیت اجرای عملیات Post Exploitation
- قابلیت انجام Privileges escalation
- قابلیت انجام عملیات DoS
- قابلیت انجام عملیات Fuzzing

پویشگر امنیتی
bestorm Fuzzer

beSTORM یک تست امنیتی پویا از محصولات در حال توسعه انجام می دهد و مدیران شبکه می توانند از این نرم افزار برای تایید امنیت اپلییکیشن های شبکه ای پیش از به کارگیری آنها استفاده کنند. بخش های QA نرم افزار که از ابزارهای مختلفی برای تست امنیت اپلیکیشن استفاده می کنند می توانند تمامی تست های پویا را در قالب یک بسته نرم افزاری انجام دهند.همچنین مدیرانی که باید قبل از به کارگیری یک اپلیکیشن امنیت آن را تایید کنند، می توانند با کمک این نرم افزار تمامی اپلیکیشن ها را با یک ابزار انجام دهند، حتی اپلیکیشن هایی که دارای پروتکل های اختصاصی هستند .

این ابزار که پیش از این تنها در سازمان های دولتی و شرکت های بزرگ کاربرد داشت، تاریخچه ای طولانی و مستند از شناسایی مسائل امنیتی در تجهیزات شبکه و نرم افزار دارد . beSTORM به دلیل کاربرد آسان و قدرت کافی برای به کارگیری در بخش نظامی، می تواند جایگزین ابزارهایی با پشتیبانی ضعیف و کاربرد پیچیده شود چرا که این نرم افزار یک فرایند تست استاندارد، قابل اطمینان و تکرارپذیر ارائه می دهد که شرکت های تجاری با هر اندازه ای می توانند آن را با فرایندهای QA نرم افزار خود همگا م سازند .

beSTORM از نظر تکنیکی یک ابزار تست فازی جعبه سیاه، هوشمند و تجاری است . این ابزار در محیط آزمایشگاهی برای تست اپلیکیشن در حین توسعه و یا برای تایید نرم افزار و سخت افزار شبکه پیش از توسعه به کار می رود.این نرم افزار دارای پشتیبانی فنی و توسعه کامل ارائه می شود و نیازی به استفاده از کد امن ندارد و با تست موقعیت هایی که احتمال خطا در آنها زیاد است و سپس بررسی دامنه نامحدود انواع حملات نتایج سریعی را ارئه می دهد .

جرم شناسی دیجیتال چیست؟

Forensic

جرم شناسی دیجیتالی یا فارنزیک (Digital Forensic) یکی از زیرشاخه های مهم امنیت سایبری می باشد که در آن متخصصین به دنبال پیدا کردن شواهد و اسنادی از یک واقعه در سیستم هستند. در اصل، هدف جرم شناسی دیجیتالی، بکارگیری تکنیک های تحقیقاتی در زمینه جرایم و حملات سایبری می باشد. بدین ترتیب، برای انجام جرم شناسی، متخصص این حوزه بعد از وقوع یک رخنه در سیستم، فراخوانده می شود و تلاش می کند تا عملیات نفوذ را تشخیص دهد، متوجه منشا آن شود و اطلاعات به خطر افتاده را احیا کند.

مدل های زیادی برای انجام جرم شناسی ارائه شده است که نشان می دهند این عملیات باید به چه صورت انجام شود تا بتوان شواهد و مدارک را به خوبی پیدا کرد. بین اکثر این مدل ها، ۴ فاز مشترک وجود دارد که در اینجا به بررسی این ۴ مورد می پردازیم :

فاز جمع آوری در فارنزیک

در فاز جمع آوری، اسناد و مدارک دیجیتالی که شواهدی برای رویداد پیش آمده هستند، جمع آوری می شوند. این فاز عموما شامل توقیف اقلام فیزیکی مثل کامپیوتر، تلفن همراه، هارددیسک و ... می باشد. بعد از توقیف این اقلام، متخصصین تلاش می کنند تا داده ها را از آسیب دیدن و یا نابود شدن نجات دهند و همچنین از شواهد دیجیتالی که نشان دهنده رویداد پیش آمده هستند محافظت کنند تا از دستکاری شدن آن ها جلوگیری شود. در این مقطع حتی ممکن است از دستگاه های ذخیره سازی یک نسخه پشتیبان تهیه شود تا همواره یک نسخه دست نخورده از شواهد و مدارک بصورت باقی بماند .

فاز بازرسی در فارنزیک

در فاز بازرسی، بازرسان تلاش می کنند تا به روش های مختلف اطلاعات و اسناد را استخراج کنند. سپس باید توجه شود که از بین سیستم های توقیف شده، چه سیستم هایی مورد بازرسی قرار گیرند. این فاز شامل چند زیربخش به نام های آماده سازی (Preparation) ، استخراج (Extraction) و تشخیص (Identification) می باشد .

فاز تحلیل در فارنزیک

در فاز تحلیل، متخصصین به کمک اطلاعات جمع آوری شده سعی می کنند یافته های بازرسان را تایید یا رد کنند. در اصل با جمع آوری تکه اطلاعات و شواهد مختلف از سیستم، سعی می کنند آن ها را در کنار یکدیگر قرار دهند و تصمیم نهایی را بگیرند .

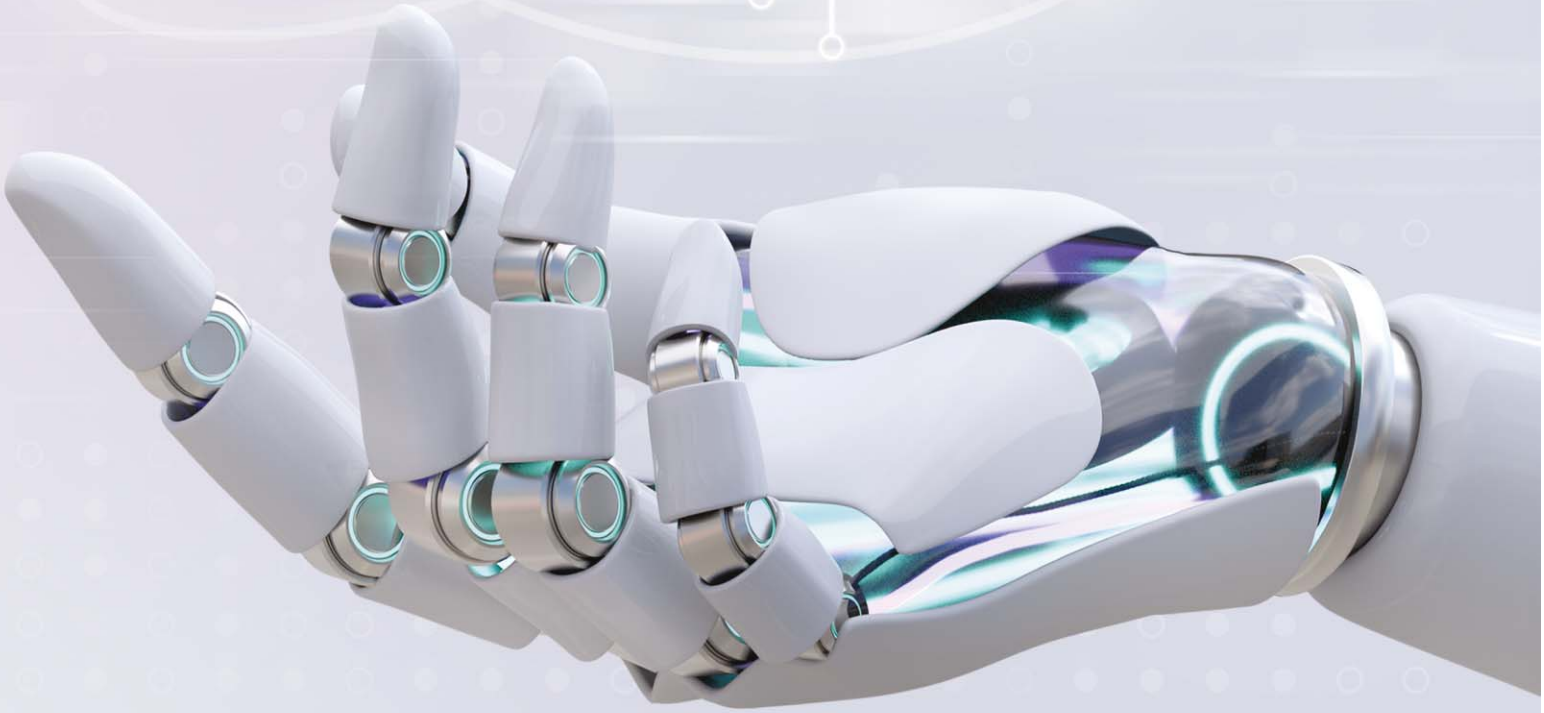
فاز گزارش در فارنزیک

در این فاز اطلاعات جمع آوری شده و نتایج تحلیل ها بطور کامل در قالب یک گزارش مستند می شود. گزارش علاوه بر دقیق بودن، باید از شفافیت و کیفیت کافی برخوردار باشد. این فاز یک گام حیاتی در انجام عملیات فارنزیک می باشد.

از معروف ترین ابزارهایی که در عملیات فارنزیک کاربردی می باشند می توان به موارد زیر اشاره کرد:

- Cellebrite
- En Case
- Digital Intelligence
- Oxygen Forensic Detective
- AXIOM
- ISEEK
- SPEKTOR
- Belkasoft
- Wireshark

سامانه هوشمند سورنا



ZECURION

مدیریت عدم نشت داده

Zecurion Dlp

Zecurion DLP
جامع ترین نرم افزار جلوگیری از نشت داده

- شناسایی و جلوگیری از نشت اطلاعات حساس سازمان
- پشتیبانی از کانالهای نشت اطلاعات شامل ایمیل، اینترنت، فایل و چاپگر
- کنترل دسترسی انعطاف پذیر و دانه ای برای دستگاه های جانبی
- تجزیه و تحلیل رفتار کارکنان و مطابقت آن با رفتار سازمانی
- ضبط و ذخیره تمامی فعالیتهای کاربران
- گزارش گیری و لاگ تمامی اتفاقات جهت پیگیری قانونی
- بایگانی کپی های سایه
- رمزگذاری فایلهای حساس
- یکپارچگی با اکتیو دایرکتوری

ویژگیها و مزایا

- ضبط میکروفون
- ضبط تصویر و صفحه کلید
- کنترل برنامه
- کنترل جامع کانال های نشت داده ها
- گزارش های قدرتمند
- تجزیه و تحلیل رفتار کاربر
- کنترل دسترسی انعطاف پذیر و دانه ای برای دستگاه های جانبی
- تلفیق با اکتیو دایرکتوری
- گزارش جامع از تهدیدات و عملکرد کاربران
- تکنیک های پیشرفته تشخیص محتوا
- کنترل ترافیک به صورت فعال یا آینه ای
- اسکن کلیه مکانهای ممکن برای ذخیره داده
- اسکن ایمیل ها و حذف اطلاعات محرمانه از داخل آن

مزایای Zecurion DLP

داده های شما بسیار مهم است و لذا بهترین محافظت را می طلبد. به همین دلیل است که باید Zecurion DLP را انتخاب کنید.
Zecurion از سال ۲۰۱۴ در Gartner Enterprise DLP Magic Quadrant رتبه بندی شده است.

مدیریت عدم نشت داده DLP

ZECURION

مدیریت عدم نشت داده

Zecurion Dlp

Zecurion همچنین به عنوان ۷ فروشنده برتر DLP توسط IDC در سال ۲۰۱۸ معرفی شد و توسط Forrester در گزارش DLP Now Tech 2019 معرفی شد. Zecurion DLP یک راه حل مقرون به صرفه، کارآمد و جامع است. این محصول، به سرعت با زیرساخت های سازمانی یکپارچه می شود. و استقرار آن به طور متوسط چهار برابر سریعتر از سایر محصولات DLP انجام می پذیرد. پس از استقرار، زکوریون همه وقایع، پرونده ها و اسناد را بایگانی کرده و رفتار کاربران را به منظور شناسایی فعال تهدیدها تجزیه و تحلیل می کند. Zecurion DLP همچنین باعث کاهش حجم کار تیم امنیتی شده و مدیریت روزانه را با گزارش های تعاملی، نمودارها و گرافهایی که ارزیابی لحظه ای از وضعیت محافظت از داده های شما ارائه می دهند، ساده می کند .

Zecurion DLP در حال حاضر در سراسر جهان در سازمان هایی با بیش از ۱۰۰۰۰۰ کاربر در حال استفاده است. از میان مشتریان Zecurion ، به کمک شواهد جمع آوری شده برای دادخواست علیه خودی های مخرب، تاکنون بیش از ۲۱ دادخواست برنده شده است.

ساختار Zecurion DLP

سنسورها: رهگیری کانال های انتقال داده ، جمع آوری داده های رهگیری شده ، اجرای سیاست های DLP

بایگانی: کلیه داده های رهگیری شده را ذخیره میکند ، پاسخ و تحقیقات در مورد حادثه را امکان پذیر می کند ، تجزیه و تحلیل گذشته نگر یعنی سیاست جدید را برای داده های گذشته اعمال (MS SQL یا PostgreSQL) می کند.

سرورDLP: تنظیمات و خط مشی را ذخیره می کند ، آنها را به حسگرها سوق می دهد ، حسگرها را مانیتور می کند.

استقرار سرور: سنسورها و عوامل انتهایی (Endpoint Agent) را مستقر می کند.

کنسول: مدیریت انعطاف پذیر مبتنی بر وب سیاست ها و گزارشها

گزینه های استقرار

هر محیط سازمانی ترکیبی منحصر به فرد از بخش های شبکه ، انواع نقاط پایانی، سیستم عامل ها، پلتفرم ها و برنامه های مختلف است. سازمانها باید با حداقل تأثیر بر عملکرد و بهره وری بتوانند از داده ها در کل اکوسیستم محافظت کنند. در عین حال، دید جامع و جلوگیری از نشت داده ها، به توانایی نظارت و تحلیل هر فعالیتی متکی است. Zecurion طیف متنوعی از گزینه های استقرار را برای اطمینان از نظارت و محافظت از اطلاعات شما بدون توجه به آنچه در زیرساخت شبکه شما وجود دارد فراهم می کند .

ویژگیهای ممتاز

Zecurion DLP همه قابلیتهای مورد نیاز برای کنترل کانال های نشت داده، نظارت بر پردازش داده توسط کارمندان و همچنین جلوگیری از نقض داده، ارائه می دهد .

سیاست ها و قوانین انعطاف پذیر

پیکربندی خط مشی را برای چندین یا همه‌کانال‌های انتقال داده تنظیم میکند و با استفاده از انواع تکنیک‌های تشخیص محتوا و شرایط داده، تا امکان هرگونه سناریوی نقض پیش بینی و جلوگیری شود.

مدیریت عدم نشت داده DLP

Symantec

مدیریت عدم نشت داده
Symantec

معرفی محصول Symantec Data Loss Prevention

نگهداری امن اطلاعات حساس سازمـانی هیچ گاه کار سـاده ای نبوده است. ولی امـروزه سازمان ها با چالش بزرگتـری در حفاظت از اطـلاعات خود مواجه هستند. امروزه با گسترش سرویس های نگهداری اطلاعات بر روی فضای ابری،کارکنان سازمان ها از این سرویس ها جهت اشتراک گذاری فایل های حساس سازمانی استفاده می نمایند. همزمان با توسعه روش های جدیـد برای مقابله با سیستم های محافظتی سنتی، تعـداد حملات سایبری در حال افزایش می باشد. با در نظر گرفتن تمامـی این عامـل ها، محافظت از اطـلاعات در برابر گم شـدن و سرقت به صورت فزاینده ای در حال دشوار شدن است . با این تفاسیر، چگونه می توان از اطلاعات در یک محیط چالش بر انگیز حفاظت کرد؟ یک راهبرد جامع و موفق حفاظت از اطلاعات در مقابله با حملات هدف دار در حال رشد و رفتار در حال تغییر کاربران چه می تواند باشد؟

Symantec Data Loss Prevention پاسخی به پرسش های حاضر با ارائه یک رویکرد جامع جهت محافظت از اطلاعات در فضای رایانش ابری و موبایل می باشد. با استفاده از DLP شما می توانید :

- داده هایی در سراسر فضای ذخیره سازی سازمان (فضای ابری، موبایل، شبکه، کلاینت ها و سیستم های ذخیره سازی) وجود دارد،کشف کنیـد.
- نحوه استفاده از اطلاعات را پایش کنید .
- از سرقت و لو رفتن اطلاعات صرف نظر از اینکه در کجا ذخیره شده اند و چگونه استفاده می شوند.- جلوگیری کنید.

امکانات و ویژگیها

محل نگهداری داده های حساس ر ا در سازمان خود پیدا کنید

- فنـاوری (Described Content Matching DCM) داده هـا را با عبـارات با قاعـده (Regular Expressions) و الگـوهای مختـلف مطابقت می دهد. برای مثال اگر یک الگوی کارت اعتباری در یک متن دید آن را بلاک می کند .
- فنـاوری (Exact Data Matching EDM) داده های حسـاس را در پایگاه داده شناسـایی می کند.برای مثـال از استخـراج نام مشتـریان و اطلاعات آن ها از پایگاه داده جلوگیری می کند .
- فنـاوری (Indexed Document Matching IDM) با استفـاده ا ز Full File Fingerprint اطـلاعات محـرمانـه در داده هـای غیـر ساخت یافته مانند اسناد Office ، فایل های PDF ، فایل های JPEG و CAD و مالتی مدیا را شناسایی می کند .
- فنـاوری VML(Vector Machine Learning) به صورت هوشمندانـه قالب اطلاعات حسـاس به مانند اسنـاد مالـی، سورس کـد ها و ... را شناسایی می کند.
- فنـاوری (File Types Detection FTD) قابلیـت شناسایـی بیش از ۳۰۰ نوع فرمت فایـل شامل ایمیل، فایـل های گرافیکـی، فایل های سفارشی و ...را دارد .
- داده های حساس بر روی بستر ذخیره سازی سازمان و موبایل و بستر رایانش ابری را پایش و محافظت کنید.
- محافظت از داده ها با انجام اسکن محلی و پایش بلا درنگ در سیستم های ویندوزی و Mac
- پایش اطلاعات محرمانه ای که در حال انتقال از / به دسکتاپ، لپتاپ از طریق ایمیل و یا فضای ابری هستند.
- گسترش محافظت از داده ها به دستگاه های اندرویدی و iOS شخصی و سازمانی
- یافتن و محافظت از داده های غیر ساخت یافته از طریق اسکن شبکه و پایگاه داده ها و سایر انباره های داده سازمانی
- پایش و محافظت از اطلاعات در حال حرکت شامل اطلاعات ارسالی از طریق ایمیل و وب و سایر پروتکل های انتقال اطلاعات

سیاست های مختلف را به صورت سازگار در شبکه سازمان تعریف و اعمال نمایید

- استفاده از یک کنسـول واحد مبتنـی بر وب برای تعریف سیاست هـا، تجدید نظـر و اصلاح حـوادث، مدیریت کلیه کلاینت‌ها و دستگاه های موبایل و سرویس های ابری و سیستم های ذخیره سازی
- بهره گیری از بیش از ۶۰ قالب آماده برای تعریف سیاست های مورد نیاز برای راه اندازی سریع سیستم DLP
- استفاده از رویه های مطمئن و قابلیت اصلاح اتوماتیک برای خودکار کردن فرایند های اصلاحی

safetica®

مدیریت عدم نشت داده

Safetica

مدیریت عدم نشت داده DLP

نرم افزارعدم نشت داده Safetica

داده های شما مهمترین دارایی شما هستند. آن را با Safetica ایمن نگه دارید.

Safetica از نشت داد ه ها جلوگیری می کند تا داده های مشتری شما در دسترس شخص دیگری نباشد.

٪۸۰ مشاغل هر ساله یک رخداد امنیتی را تجربه می کننـد. متوسط هزینه نقض سیاست هـای امنیتی داد ه ها ۴ میلیـون دلار است. ۳ / ۲ از شرکت های کوچک در طی ۶ ماه از نقض عمده داده ها، از کسب و کار خارج می شوند.

Safetica به شما کمک می کند از خود محافظت کنید.

با Safetica ، آنچه متعلق به شماست، برای شما باقی می ماند.

Safetica یک راه حل مقرون به صرفه،آسان برای استفاده و جلوگیری کردن برای از دست رفتن داده ها(DLP) است.این کار حسابرسی های امنیتی را انجام می دهد، از خروج اطلاعات حساس از شرکت شما جلوگیـری می کند و آنچـه را که در سازمان شما می‌گذرد روشـن می کند.

Safetica می تواند در عرض چند ساعت مستقر شود به سرعت و به راحتی اطلاعات شما را ایمن می کند.

حفاظت اطلاعات

از داده های مهم خود محافظت کنید و افرادی را که می توانند به آنها دسترسی داشته باشند کنترل کنید .

تحلیل رفتار

نحوه کار، فعالیت و استفاده از نرم افزارهای گرانقیمت کارمندان خود را کشف کنید.

کنترل دستگاه

مشخص کنید کدام دستگاه ها می توانند استفاده شوند و خطرات BYOD را برطرف کنید.

درباره شرکت

مشکلات موجود در فرآیندهای داخلی را شناسایی کرده و راه حل ها را پیاده سازی کنید.

انطباق با مقررات

به راحتی با اقدامات امنیتی محافظت از اطلاعات مطابقت داشته باشید.

با Safetica می بینیم :

چه اطلاعاتی از شرکت شما خارج شده است

چه کسی داده های محرمانه را بدون مجوز دستکاری کرده است

جایی که حوادث مربوط به انطباق نظارتی اتفاق می افتد

چه اسنادی بدون نیاز چاپ شده است

کدام مجوزهای نرم افزاری استفاده نمی شوند

Safetica به شما می دهد :

حسابرسی از امنیت داخلی شرکت شما

اعلان های بلادرنگ در صورت بروز حادثه

روشی برای آموزش کاربران و جلوگیری از نشت داده های تصادفی

مرورهای ماهانه، مستقیماً به صندوق ورودی شما ارسال می شود

دسترسی آنلاین به بررسی اجمالی حادثه و جزئیات

منو اسکن کن !

محافظت هر چه بیشتر

سامانه هوشمند سورنا

www.sorena.ir

solarwinds

مانیتورینگ با مدیریت Solarwinds

نظارت و رسیدگی به حل مشکلات شبکـه به تنهایی کافـی نیست و لازم است گزارش هایی درباره عملکـرد شبکـه، مشکلات به وجـود آمده و تغییرات انجام شده با هدف حل مشکلات مکتوب شود تا فرآیند پیگیری تغییرات در آینده به سادگی امکان پذیر باشد. ابزارهای زیادی با هدف نظارت بر پهنای باند،حصول اطمینان از صحت سلامت شبکه و تجهیزات تحت شبکه طراحی شده اند.شرکت SolarWinds با سابقه درخشان در زمینه ساخت نرم افزارهای نظارتی موفق به ساخت ابزارهای مهمی شده که از آن جمله می توان به نرم افزار مانیتورینگ عملکرد شبکه، نرم افزار مانیتورینگ برنامه های کاربردی و سرور، نرم افزار تحلیل گر ترافیک جریان شبکه، نرم افزار مدیریت پیکربندی ها و ..... اشاره کرد.

این ابزار شامل ماژول هایی است که هر کدام نقش و کارایی مخصوص به خود را دارا هستند. مدیر و ناظر شبکـه برای نیاز خود ملزم به انتخاب ماژول مربوط به نیازش خواهد بود که به اختصار به شرح برخی از آنها خواهیم پرداخت.

ماژول Application Performance Monitor (APM)

امکان کنترل و مدیریت عملکرد نرم افزارهای سازمانی، سـرورهای فیزیکـی و مجـازی، سخت افزار، پردازش ها و عملکرد سیستـم عامـل را در سطح شبکه های Enterprise و با کمترین هزینه تامین می کند. این ماژول دارای قابلیت راه اندازی بسیار آسان و سریع می باشد. بطوریکـه پس از نصب نرم افزار و انتخاب نرم افزار و سرورهای مورد نظر بطورخودکار آنها را شناسایی کرده و اطلاعات، گزارشات و پیغام های مربوطـه را در یک داشبورد مجتمع نمایش می دهد .

ماژول Network Performance Monitor (NPM)

این ماژول با تامین اطلاعات حیاتی مورد نیاز، به شما کمک می‌کند تا بتوانید شبکه در حال توسعه خود را به خوبی مدیریت کنید.این نرم افزار به شما کمک می کند تا به سرعت ایرادات عملکردی شبکه را شناسایی و عیب یابی کرده و قبل از آنکه سیل تماس های تلفنی ناشی از قطعی شبکه به سوی شما روانـه شود، اقدام به برطرف کـردن آن نمایید. نـرم افـزار Orion NPM از نظر راه اندازی، استفـاده و نگهـداری آسانترین نرم افزار در مقایسه با نرم افزارهای مشابه می باشد .

ماژول Network Configuration Manager (NCM)

این ماژول با تسهیل مدیریت در شبکه به ویژه در شبکه هایی که از تجهیزات با برندهای مختلف در ساختار آن استفاده شده است، ابزار جامع مانیتورینگ تحت وب را به همراه سادگی و سهولت دسترسی به اطلاعات پیکره بندی تجهیزات در شبکه را فراهم می آورد. همچنین با کنترل مستمر تنظیمات در تجهیزات موجود، هرگونـه تغییـر به وجود آمـده در آنهـا را بطور آنی به اطلاع شمـا می رساند؛ تا نسبت به رفع مشکـلات احتمالی اقدامات اولیه انجام شـود. با استفاده از این ماژول شما قادر خواهیـد بود تا اشکالات بوجود آمده در تجهیـزات را بدون نیاز به برقـراری ارتباط Telnet یا SSH ، برطرف نمایید .

ماژول Log & Event Manager (LEM)

این نرم افزار جدیدترین عضو خانواده SolarWinds می باشد که براساس تکنولوژی TriGeo تولید شده است. این محصول قدرتمند با تلفیق تحلیل بلادرنگ لاگهای تولید شده، ارتباطات بین وقایع و امکان جستجوی اختصاصی امکان‌مشاهده،کنترل و تامین امنیت را فراهم آورده است. راه انـدازی و کاربری این نرم افزار بسیـار آسان بوده ضمن تامیـن مجموعـه گزارشـات غنی و امکـان تحلیـل و مدیریت لاگها و وقایع شما را از نرم افزارهای گران قیمت و راه حل های پیچیده بی نیاز می سازد .

لازم به توضیح است که هر ماژول محدوده ی تعدادی مشخصـی دارد. به عنـوان مثـال برای مـاژول APM حداقـل سفارش بین ۱ تا ۵۰ عـدد خواهد بود که در برخی از ماژول ها علاوه بر محدوده های مشخص شده ، نوع نامحـدود نیز موجـود است. پس برای انتخاب یک ماژول، تعـداد NOD ها مهم و تاثیر گذار در قیمت نهایی آن خواهد بود.

پشتیبانـی از انواع نودهـای شبکه، تنوع گزارش، سادگـی نصب و راه انـدازی، قابلیت اطمینـان، تحمـل بـار پردازشـی در شبکـه های بـزرگ و مانیتورینگ وضعیت سلامت شبکه برخی از ویژگیهای استفاده از ابزار مانیتورینگ Solarwinds می باشند.

PRTG NETWORK MONITOR

نظارت و مانیتورینگ
PRTG

PRTG Network Monitor نرم افزاری قدرتمند برای نظارت بر شبکه و سیستم های مبتنی بر ویندوز است. این نرم افزار برای شبکه های کوچک ، متوسط و بزرگ مناسب است و قادر به نظارت بر شبکه های WLAN ، WAN ، LAN و VPN می باشد. شما همچنین می توانید وب سایت ها، ایمیل ها و پرونده های سرور، سیستم های لینوکس، ویندوز، روترها و بسیاری دیگر را تحت نظارت داشته باشید .
PRTG Network Monitor یک حالت کشف خودکار دارد که سطوح از پیش تعریف شده یک شبکه سازمانی را اسکن می نماید و یک لیست دستگاه از این داده ها را ایجاد می کند. در مرحله بعدی با استفاده از پروتکل های مختلف ارتباطی می توان در مورد دستگاه های شناسایی شده، بازیابی کرد. این نوع پروتکل ها، sFlow ، jFlow ، NetFlow ، WMI ، SNMP ، Ping هستند اما همچنین ارتباط ازطریق DICOM یا RESTful API امکان پذیر است. در زمان آموزش نصب و راه اندازی نرم افزار prtg فقط برای سیستم های Windows قابل دسترس است. همچنین این نرم افزار راه حل نظارت مبتنی بر ابر PRTG hosted by Paessler را ارائه می دهد.

معرفی بخش های مختلف نرم افزار : (در این قسمت سه بخش مهم نرم افزار PRTG توضیح داده می شود)

Network Autodiscovery

PRTG می تواند با پینگ محدوده IP مشخص شده، بخش های شبکه را اسکن می کند. به این ترتیب PRTG به طور خودکار طیف گسترده ای از دستگاه ها و سیستم ها را شناسایی می کند. این کار موجب صرفه جویی در مقدار زیادی کار پیکربندی می شود و شما می توانید شروع به مانیتورینگ شبکه خود کنید .

Maps

با PRTG Maps شما می توانید صفحات وب را با داده های حاصل از مانیتورینگ، به صورت به روز، بصورت دلخواه ایجاد کنید. شما حتی می توانید نقشه ها را با داده های حاصل از مانیتورینگ خود، در دسترس عموم قرار دهید تا کارشناسان دیگر بصورت لحظه ای آن را مشاهده کنند.

Alerts

PRTG وقتی هشدار غیرمعمولی را می بیند، به شما در جهت رفع آن هشدار می دهد. با استفاده از برنامه های رایگان موجود برای اندروید، iOS و ویندوز فون، شما می توانید این هشدارها را بصورت مستقیم بر روی تلفن همراه خود دریافت نمایید. این هشدارها به راحتی می توانند از طریق ایمیل یا SMS به شما اطلاع داده شود.

قابلیت های ابزار PRTG به اختصار عبارتند از :

- تشخیص خودکار دستگاه های موجود در شبکه پس از نصب
- رابط کاربری تعاملی و قابل تنظیم
- نظارت کامل و دقیق بر کلیه دستگاه های موجود در شبکه
- نمایش تنظیمات پیکربندی به صورت سلسله مراتبی درختی با پشتیبانی از ویژگی ارث بری تنظیمات
- معماری مدرن و عملکرد بهینه نرم افزاری
- کنترل پهنای باند مورد استفاده
- بیش از ۵۰ نوع سنسور به منظور فراهم آوردن یک نظارت جامع در شبکه های کوچک یا بزرگ
- نظارت بر کارایی و در دسترس بودن اجزای شبکه
- امکان کنترل روترها و سوئیچ های شبکه

Symantec

پشتیبان گیری به پشتوانه
Symantec Vertias

یکی از کمپانی های قدرتمند که هدف خود را بر طراحی و تولید نرم افزارهای بکاپ گیری قرار داده است، Veritas می باشد. متخصصان این شرکت توانسته اند محصولاتی نظیر Backup Exec و Net Backup را در اختیار مشتریان خود در سراسر دنیا قرار دهند. پشتوانه ی این شرکت معتبر، سابقه ی سی ساله آن در زمینه بکاپ گیری از اطلاعات موجود در شبکه ها و سیستم های موجود بوده و همین امر باعث شده است تا سازمان های بزرگ بسیاری در سراسر دنیا همکاری خود را با وریتاس آغاز کرده و ادامه دهند. Veritas Backup بر حفظ ساده، ایمن و یکپارچه سازی حفاظت از داده ها تمرکز دارد. تنها کافی ست تا انتخاب کنید که از چه اطلاعاتی بکاپ بگیرید و کجا آن ها را ذخیره کنید. تمامی داده های شما در هرجایی که باشند محافظت خواهند شد.

از آنجا که حفظ امنیت اطلاعات در کسب و کارهای امروزی حرف اول را می زند، پس گاهی بازگردانی اطلاعات ازدست رفته توسط نسخه پشتیبانی که از پیش تهیه شده است، می تواند در شرایط اضطراری بسیار مفید واقع شود. وریتاس Backup Exec توانسته است با رعایت استانداردهای بین المللی، بهترین راه کارهای ذخیره سازی و پشتیبانی اطلاعات را فراهم آورد. کنسول مدیریتی این نرم افزار بسیار ساده و منعطف طراحی شده است و مدیران بسیاری توانسته اند با اندکی آموزش، از ابزارها و ویژگی های متنوع این محصول به بهترین نحو استفاده نمایند.

امکانات و ویژگی های Veritas

استفاده آسان

- ✓ تمامی اکوسیستم داده خود را از یک کنسول واحد مدیریت کنید
- ✓ با چند کلیک کارهای پشتیبان‌گیری را انجام دهید
- ✓ به راحتی هرکار بکاپ گیری، تکثیر و یا بازیابی اطلاعات را ردیابی کنید

محافظت از اطلاعات فضای ابری

- ✓ Instant Cloud Recovery را با Azure Site Recovery ادغام کنید
- ✓ از همه ردیف های ذخیره سازی ابری AWS پشتیبانی به عمل آورید
- ✓ هزینه های ذخیره سازی و پهنای باند را با deduplication درون سازمانی بهینه کنید

بازیابی فاجعه

- ✓ بازگرداندن دانه دانه ماشین های مجازی به صورت مستقیم، ازطریق پشتیبان گیری بدون عامل
- ✓ بازیابی فوری کلیه ی ماشین های مجازی
- ✓ تست خودکار بازیابی فاجعه از پشتیبان گیری های ماشین های مجازی
- ✓ به حداقل رساندن خرابی و اختلالات با استفاده از بازیابی یکپارچه

VEEAM
Modern Data Protection

پشتیبان گیری به روش
Veeam

Veeam Backup & Replication یک برنامه پشتیبانی و محافظت از داده هاست که برای محیط های مجازی VMware vSphere و Microsoft Hyper-V hypervisors توسط شرکت Veeam ساخته شده است. این نرم افزار قابلیت پشتیبان گیری ، replication و Restore کردن ، برای ماشین های مجازی ارائه نموده است . Veeam Backup & Replication برای محیط های مجازی سازی شده طراحی گردیده است. به وسیله snapshots گرفتن از ماشین ها و استفاده از این snapshots برای گرفتن بکاپ که به دو صورت Full و Incremental است. برای بازگردانی داده ها می توان نسخه پشتیبان گرفته شده را در محل ذخیره شده قبلی یا در مکانی دیگر بازیابی نمود. گرفتن Snapshots به وسیله VMware vSphere میتواند بار سنگینی بر عملکرد ماشین های مجازی بگذارد و مدیران IT را به چالش بکشد .Veeam به طرز چشمگیری این روند را بهبود بخشیده است.با استفاده از Snapshots گرفتن در سطح استوریج حتی در ساعات کاری با کمترین تاثییر بر عملکرد می توانید از داده های خود بکاپ تهیه نمایید .Veeam می تواند با ادغام با replication در سطح استوریج در صورتی که استوریج اصلی در دسترس نباشد و دچار مشکل شده باشد به سرعت داده شما را بازیابی نماید .

برخی از ویژگی های ابزار VEEAM :

- تعریف کاربران مختلف با دسترسی های محدود و نامحدود
- معرفی برنامه زمانبندی شده برای گرفتن Backup
- قابلیت اطمینان بالا در پروسه گرفتن Backup و بازگرداندن آن
- امکان Backup گیری از ماشین ها مجازی ویندوزی و لینوکسی
- مستندسازی وضعیت سیستم ها و مدیریت گزارش ها
- اطلاع رسانی از طریق ایمیل درباره بروز مشکلات در پروسه ایجاد بکاپ
- کاربری بسیار آسان

آنتی ویروس Kaspersky

نسخه های تحت شبکه (Kaspersky Endpoint Security for Business)

محصول امنیتی اصلی کسپرسکی یعنی Kaspersky Endpoint Security for Business در میان کسب و کارها و رهبران صنعت IT به عنوان راهکاری سریع و مطمئن برای مقابله با بدافزارها شناخته شده است. این راهکار همچنین دامنه متنوعی از ابزارهای مدیریتی را در قالب یک کنسول واحد ارائه می دهد. برخی از این قابلیت های مدیریتی - امنیتی عبارتند از: تحلیل آسیب پذیری ها، مدیریت وصله ها، کنترل برنامه های کاربردی، Mobile Device Management(MDM) ، رمزنگاری جزئی (فایل ها) و کلی (هارد دیسک) و رمز گذاری (Authentication) روی هارد درایوها و دستگاه های External . شرکت کسپرسکی، محصولات Endpoint خود را از نظر امکانات به چهار دسته زیر تقسیم می نماید.

- **Kaspersky Endpoint Security for Business – Cloud**
- **Kaspersky Endpoint Security for Business - Select**
- **Kaspersky Endpoint Security for Business – Advanced**
- **Kaspersky Total Security for Business**

آنتی ویروس ESET

نسخه های تحت شبکه آنتی ویروس (ESET Endpoint Security)

محصولات امنیتی ESET قادر هستند. تمامی تهدید هایی که بر اساس وب و یا حملاتی که به سمت قربانی انجام می پذیرد را توسط پیشرفته ترین تکنولوژی اسکنر هوشمند محافظت نماید. این محصولات ۱۰۰ ٪ تمامی تهدیدات و حملات را بلاک می کنند.

- **ESET Protec Entry**
- **ESET Protec Advanced**
- **ESET Protec Complete**

Symantec KASPERSKY lab safetica ESET

IMPERVA®
Protecting the Data That Drives Business®

امنیت بانک اطلاعاتی
DataBase Security by IMPERVA

در حال حاضر سیستم های اطلاعاتی در بخش های مختلف سازمان ها مورد استفاده قرار می گیرند که اغلب آنها مبتنی بر پایگاه داده های آسیب پذیر هستند. همچنین، مهاجمان از طریق برنامه های کاربردی می توانند به پایگاه داده سازمان ها حمله کنند. استفاده از Database Firewall (DBF) و Web Application Firewall (WAF) یکی از راه های دفاع در عمق است که از این حملات جلوگیری می کند. شرکت Imperva یکی از شرکت های پیش رو در تولید محصولات امنیتی به خصوص DBF و WAF می باشد. شرکت Imperva با عرضه محصول Secure Sphere DBF از اطلاعات مربوط به پایگاه داده های مستقر در سازمان ها محافظت می کند. از آنجایی که بخش قابل توجهی از حملات پایگاه داده ها از طریق برنامه های کاربردی صورت می گیرد لذا یکی دیگر از محصولات شرکت Imperva محصول امنیتی Secure Sphere WAF می باشد. DBF مربوط به شرکت Imperva محصولی است که از بانک های اطلاعاتی در مقابل حملات خراب کارانه، از بین رفتن و سرقت اطلاعات محافظت می کند. این محصول، نظارت همیشگی بر روی بانک اطلاعاتی را بر عهده گرفته و در صورت بروز مشکل از مکانیزم های همانند پیام هشدار و یا مسدود کردن ترافیک استفاده می کند. این محصول با ایجاد سیاست های امنیتی و قوانین حسابرسی از اطلاعات و منابع اطلاعاتی محافظت می کند. WAF یک پروتکل دفاعی لایه ۷ محسوب می شود و معمولا در برابر حملاتی مانند File Inclusion ، XSS ، CSRF و SQL injection از اپلیکیشن تحت وب محافظت می کند .

فایروال Imperva ، با فیلتر کردن ترافیک مخرب، از برنامه تحت وب، در برابر آسیب پذیری های موجود در آن، محافظت می کند. این فایروال، یک راهکار امنیتی همه جانبه است که از سطح جدیدی از دفاع عمیق، رونمایی می کند. یکی از قابلیت های این فایروال، این است که به هر شکلی که بخواهید، می توانید آن را مستقر کنید. WAF ایمپروا قابلیت استقرار در محل، Azure ، AWS را دارد و یا حتی خود این فایروال را می توانید به عنوان یک سرویس ابری، به کار بگیرید.

WAF ایمپروا چگونه از برنامه های شما محافظت می کند؟

شناسایی حمله

WAF به دقت حملات را شناسایی می کند و false positive ها را به حداقل می رساند و برای این کار، از پروفایلینگ پویا و اعتبارسنجی همبسته استفاده می کند.

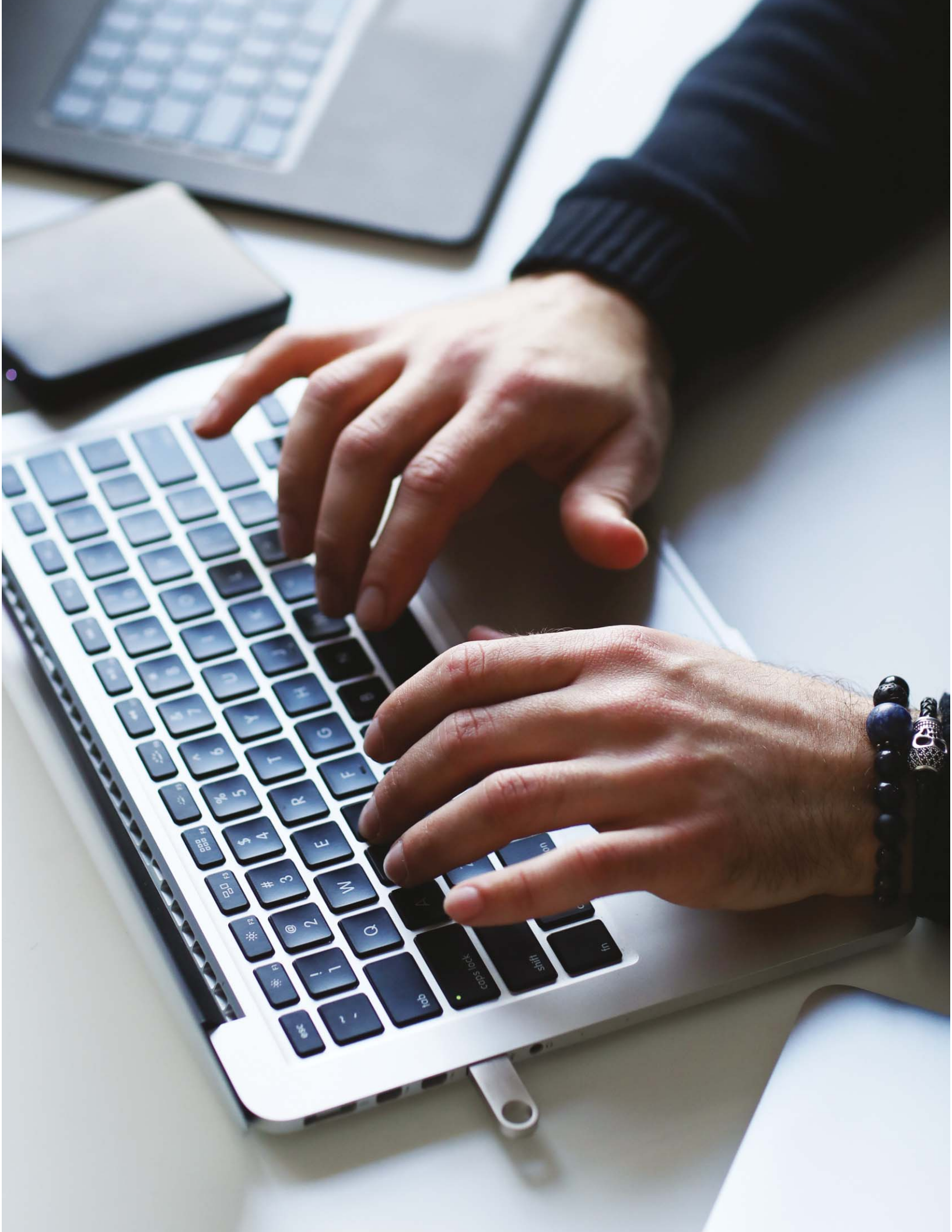
همان طور که در مورد گیت وی WAF گفتیم، پروفایلینگ داینامیک،تمام زوایای اپلیکیشن های تحت وب را بررسی می کند. اعتبارسنجی همبسته حملات هم، تمام جرایم و تخلفات مستقل را جمع آوری و تجزیه و تحلیل می کند. ترکیب این دو قابلیت، باعث می شود فایروال WAF ، حملات را با دقت استثنایی تشخیص دهد و ترافیک بد را مسدود کند.

ادغام SIEM

فایروال Imperva، با بسیاری از اکثر سیستم های پیشرو در زمینه ی امنیت اطلاعات و مدیریت رویداد (SIEM) ، مانند Splunk ، ArcSight و غیره ، ادغام می شود. این فایروال، روید اها را در فرمت پیام های CEF ، syslog و JSON انتقال می دهد.رویداد هایی که توسط فایروال WAF ایمپروا ایجاد می شوند، مستقیماً ایندکس شده و به راحتی قابل جستجو هستند. این ویژگی در پاسخگویی سریع به حادثه،بسیار مهم و کارآمد می باشد.

گزارش های جامع

فایروال WAF Imperva،گزارش های گرافیکی با کیفیتی ارائه می کند که باعث می شود به راحتی بفهمید وضعیت امنیتی وب اپلیکیشن شما در چه وضعیتی است و اوضاع بر طبق دستورالعمل های مدیریتی پیش می رود یاخیر. همچنین می توانید گزارش های از پیش تعریف شده با قابلیت سفارشی سازی تدوین کنید، به سرعت وضعیت امنیتی و میزان انطباق با PCI، FISMA، HIPAA ، SOX و سایر استانداردها را ارزیابی کنید. از مزایای فایروال Imperva ، می توان به تحلیل حملات و داشبورد های مدیریتی اشاره کرد .



توانایی های قابل ارائه در سامانه هوشمند سورنا

یکی دیگر از توانایی های تولیدی سامانه هوشمند سورنا ، طراحی پاور دیتا سنتر ،تامین انواع UPS ، باتری و تابلو برق و امور پسیو و PDU جهت ارائه به بخشهای مختلف IT-ICT و صنعتی کشور، درکنار ارائه مشاوره فنی بوده است. با توجه به تنوع محصولات،که شامل انواع UPS ، باتری های اسیدی/ بازی و همچنین امکان ارائه محصولات مذکور از کارخانه های مختلف داخلی و خارجی می باشد.

برخی از توانایی های قابل ارائه در این بخش عبارتند از:

✓ ارائه انواع UPS :

عرضه انواع مولد برق بدون وقفه (UPS) به صورتهای تک فاز و سه فاز با برند های معتبر اروپایی ، آمریکایی و آسیایی .

✓ ارائه انواع Battery

ارائه باتری های اروپایی Fiamm ، Hoppecke و Varta(Enersys) و همچنین برندهای کره ای Rocket و Global و Yuasa نیز مهیا می باشد. دربخش باتری های نیکل کادمیوم نیز امکان ارائه باتری های اروپایی - SAFT و ALCAD تحویل در داخل کشور وجود دارد.

✓ تابلو برق (Power Distribution Panel) PDP

تولید تابلوهای مادر - تابلو اصلی و ساخت تابلوهای تقسیم ، ارائه نقشه های اولیه و مشاوره طبق استاندارد های بین المللی .

PDP MAIN
PDP UPS
PDP CHARGER DC
PDP BATTERY
CHANGEOVER AUTOPDP
PDP Automation

✓ پاور دیتا سنتر

ارائه طرح و اجرا پروژ ه های دیتا سنتر
تابلو برق
لدر و سینی
کابل کشی

✓ پاور ماژول (PDU)

طراحی و ساخت
BISIC PDU RACK
METER PDU
SMART PDU

انواع خروجی های برق به شرح ذیل می باشد:

- پریزهای ساده DIN49440
- پریزهای IEC 60320/C13 Back to Back
- پریزهای IEC60320/C19 Back to Back







منو اسکن کن !

طراحی ، ساخت و عرضه
سامانه هوشمند سورنا
www.sorena.ir

ماژول توزیع برق(PDU)
(ZERO UNIT)

ویژگی ها

✓ **قابلیت نصب در رک های APC بدون نیاز به ابزار**

این امکان باعث می گردد مصرف کننده خیلی سریع و به راحتی دستگاه را در پشت رک نصب و یا جدا نماید.

✓ **قابلیت Reset کردن کلید محافظ**

در هنگام وقوع اضافه بار یا اتصال کوتاه در برخی از مدل ها

✓ **قابلیت نصب عمومی**

این امکان باعث می ـگردد تا هیچ فضایی از فضای مفید رک اشغال نگردد و امکان نصب تعداد تجهیزات بیشتری در داخل رک مهیا گردد، همچنین فاصله سرور و کانکتور برق به حداقل رسیده و آرایش زیباتر و ایمن تری برای تجهیزات ایجاد می‌گردد.

✓ **کانکتورهای خروجی متنوع**

در هر دستگاه دو نوع کانکتور خروجی IEC-C13 و IEC-C19 تعبیه شده است و این باعث می گردد تا انواع تجهیزات کامپیوتری و سرورها با قدرت 10A و 16A را بتوان تغذیه نمود.

✓ **قابلیت نصب از دو جهت**

امکان نصب PDU به صورتی که کابل ورودی از بالا و پایین رک قابل هدایت باشد.

✓ **کابل ورودی از نوع فلکسی لاستیکی NYMHY**

موجب می گردد آرایش کابل مخصوصا در محل خمها بسیار مناسب و زیبا اجرا گردد. روکش این نوع کابل ها در مقابل صدمات فیزیکی و سایش مقاوم تر از کابل های افشان معمولی می باشد.

✓ **کانکتور ورودی از نوع صنعتی**

کانکتور مورد استفاده از کیفیت بسیار خوب و دارای استاندارد CE میباشد. از آنجا که عموما اختلالات مربوط به سیستم توزیع برق از محل اتصالات و کانکتورها حادث می گردد، کیفیت این کانکتور بسیار مهم و حیاتی می باشد.

ماژول توزیع برق(PDU)
(ZERO UNIT)

✓ساپورتهای نگهدارنده کابل برق

جهت مهار کابل های برق سرورها و تجهیزات کامپیوتری و جلوگیری از جدا شدن آنها از کانکتور پاور ماژول ، ساپورت هایی برای این منظور تعبیه شده است

✓کیفیت رنگ

عموما ماژول توزیع برق رک در مراکز داده و دیتا سنترها نصب میگردند و از آنجا که در این نوع مراکز رطوبت هوا بین ۴۵ ٪ تا ۵۵ ٪ تنظیم می گردد ، لذا جهت جلوگیری از زنگ زدن بدنه تجهیزات بایستی دارای کیفیت و ضخامت رنگ مناسب باشند . در این دستگاه کلیه مراحل جرم گیری تا مرحله رنگ به شدت کنترل و در نهایت محصول خروجی دارای چسبندگی و ضخامت رنگ بسیار مناسب می باشد.

✓چاپ راهنما

کلیه کانکتورها و المان های د ستگاه دارای چاپ راهنما به صورت سیلک می با شند. این چاپ با رنگ سفید روی زمینه سیاه اجرا می گردد و دارای کیفیت بسیار مناسب است.

✓کانکتورهای خروجی

در ماژول های توزیع برق عمودی مذکور از دو مدل کانکتور IEC-C13 و کانکتور IEC-C19 از برندهای معتبر مورد استفاده قرار گرفته اند تا انواع تجهیزات با توانهای 10A و 16A قابل اتصال باشند. اهمیت کیفیت کانکتورهای خروجی با توجه به اینکه نقطه اصلی بروز حادثه است، بسیار مهم می باشد.

✓تست دی الکتریک

به منظور اطمینان از مقاومت عایقی حامل های جریان و بدنه دستگاه تست دی الکتریک انجام می گیرد.

✓قابلیت مانیتورینگ

در مدلهای Metered و IP پارامترهای ولتاژ، جریان، توان و انرژی مانیتور می گردند. همچنین امکان نصب سنسور دما و نمایش آن در مدل های IP وجود دارد.

✓قابلیت اتصال به شبکه

در مدلهای IP امکان اتصال PDU به شبکه از طریق درگاه SNMP یا Modbus فراهم بوده و پارامترهای قابل اندازه گیری توسط تجهیز از طریق شبکه قابل نمایش و مدیریت می باشد.