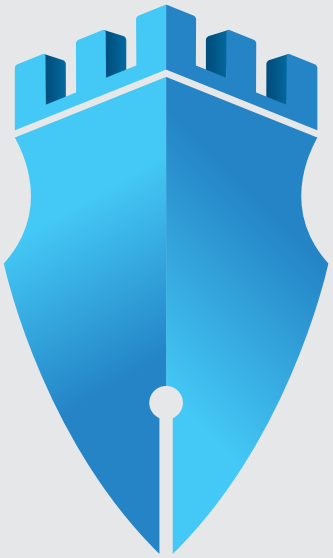


LIANGROUP

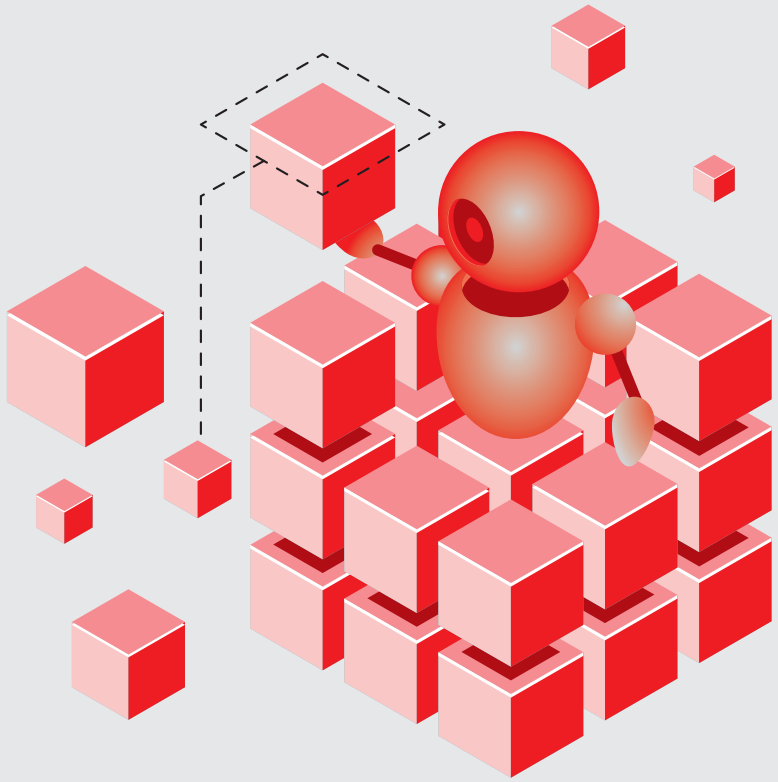
Mehrna Rayaneh Lian

۰۲۱ ۹۱۰۰۰۴۱۵۱

تهران، فلکه دوم صادقیه، بلوار آیت الله کاشانی
خ نجف زاده فروتن، خ اعتمادیان، پلاک ۴۲، واحد ۲

www.liangroup.net

ArcSight



یک مرکز SOC برای ارائه خدمات و قابلیت‌هایی که از آن انتظار می‌رود و برای آن تعیین شده است، از فناوری‌های مختلفی استفاده می‌کند. برای ارائه این خدمات و قابلیت‌ها باید میان فناوری‌های مورد استفاده در مرکز SOC همکاری و ارتباط برقرار شود. این ارتباط می‌تواند فقط برای ارسال پیغام تا درک کامل پیغام و استفاده از آن، تعریف شود. به همین دلیل نیازمند این هستیم که یک فناوری به عنوان نقطه اتصال و برقراری ارتباط میان فناوری‌های دیگر و نقطه تمرکز کانون مرکز SOC، عمل کند. از این فناوری به عنوان قلب مرکز SOC تعبیر می‌شود، که همان SIEM یا سامانه مدیریت رویداد و اطلاعات امنیتی است. ArcSight محصول SIEM خود را تحت عنوان ESM معرفی کرده است. ArcSight یک شرکت فعال در حوزه امنیت سایبری است که در سال ۲۰۰۰ میلادی در کالیفرنیای آمریکا تاسیس شد. این شرکت فعال در زمینه تولید نرم افزارهای آنالیز امنیت مراکز داده بزرگ برای امنیت اطلاعات و مدیریت رویدادها می‌باشد. این شرکت ۱۱ سال مداوم در صدر لیست ارائه شده توسط گارنتر قرار دارد که نشان دهنده کیفیت و عملکرد عالی این شرکت در این حوزه می‌باشد. شرکت ArcSight در سال ۲۰۱۰ توسط شرکت HP خریداری شد. طرح اولیه تجاری این شرکت، ساخت راه حل‌های Cache و افزایش سرعت بود اما بعد از یکسال وارد حوزه آنالیز رخدادهای امنیتی و همبستگی (Correlation) لاگ‌ها شدند که این امر با موفقیت‌های بزرگی همراه بوده است.

ArcSight

با استفاده از ArcSight ESM 7.0 ، برای مراکز SOC خود چابکی و سرعت بیشتری به منظور گسترش امنیت سایبری و همچنین سرعت سریع تری به منظور کشف تهدیدات امنیتی به ارمغان بیاورید بطوری که امکان جمع آوری ۱۰۰۰۰۰ لاگ در ثانیه را خواهید داشت. در حقیقت این محصول با ارائه Visibility کامل و جامع از کلیه فعالیت های انجام گرفته در زیرساخت IT سازمان ها، قادر به کشف و جلوگیری از مشکلات امنیتی خارجی (هکرها و بدافزارها) و داخلی (نشت اطلاعات و کلاهبرداری)، خواهد بود. ArcSight ESM یک راه حل نرم افزاری جامع است که پایش رویدادهای امنیتی سنتی را با هوش شبکه ای، همبسته سازی زمینه ای، تشخیص ناهنجاری، ابزارهای تحلیل تاریخچه ای و اصلاح خودکار ترکیب کرده است. یک راه حل چندسطحی است که ابزارهایی را برای تحلیل گران امنیت شبکه، مدیران سیستم و کاربران تجاری ارائه کرده است.این محصول به عنوان قلب مرکز SOC عمل کرده و از فناوری هایی که برای تشخیص و پایش و پویش شبکه سازمان مورد استفاده قرار می گیرند (سیستم های تشخیص نفوذ شبکه و میزبان، فایروال، فایروال برنامه های کاربردی وب، بررسی کننده صحت فایل، سیستم های جلوگیری از نشت اطلاعات، ضدبدافزارها، ابزارهای تشخیص کلاه برداری، ابزارهای تولید رویداد سیستم عامل ویندوز و لینوکس، پویشگران آسیب پذیری)، رویدادها و داده های متنی را دریافت می کند و پردازش هایی را (بررسی و تائید رویدادها، همبسته سازی، پایش، تحلیل) روی آن ها انجام داده و نتایج تحلیل های خود را به سایر فناوری ها (سیستم واکنش و پاسخ)، درصورتی که برای ارائه خدمات مرکز SOC مورد نیاز باشد، ارسال می کند.

ArcSight

قابلیت های کلیدی ArcSight

ArcSight Data Platform

ArcSight ESM که برای مقیاس های بسیار بزرگ و سرعت بسیار بالا طراحی شده است بطور کامل با ADP Event Broker، که یک راهکار تحویل و جذب هوشمندانه داده برای مراکز SOC مدرن است و بیش از ۴۰۰ محصول را پشتیبانی می کند یکپارچه می شود.

Real-Time Data Correlation

جمع آوری داده ها و اطلاعات و Correlate کردن رویدادها و ایونت ها در زمان بلادرنگ، به منظور افزایش جلوگیری از تهدیدات سایبری که قوانین داخلی را نقض کرده و بستر شبکه را به خطر می‌اندازند. به راحتی SIEM را با اضافه کردن گره های Correlate با موتور منعطف منحصر به فرد خود، مقیاس پذیر می کند.

Workflow Automation

مرکز مانیتورینگ SOC خود را با شناسایی هشدارهای امنیتی توسط ArcSight ESM قدرتمندتر سازید. قابلیت ادغام با اجرای دستورات روی دستگاه های خارجی به وسیله ArcSight Action Connectors نیز برای شما فراهم شده است. این عمل به ترسیم حملاتی که روی بستر شبکه اتفاق می‌افتد کمک بزرگی می کند.

ArcSight Investigate Integration

یکپارچه سازی SIEM خود با ArcSight Investigate، نسل بعدی شکار و تحقیق راه حل های کاربردی، به منظور ایجاد بسیار سریع و بصری جستجو و تجسم داده ها در محیط عملیات امنیتی است. این ویژگی به شما درک بسیار بالایی از وضعیت شبکه ارائه خواهد داد.

Multi-Tenancy And Unified Permissions Matrix

ArcSight توانمندی های مدیریتی متمرکز را تقویت می کند که شامل آستانه های نقش محور و قوانین دسترسی یکپارچه، ماتریس اجازه ها و مسئولیت های توزیع و انتشار تمام داده ها و هشدارها در سطح مشتری می باشد.

Community

بهره مندی از قوانین امنیتی، داشبورد ها و گزارش هایی که توسط متخصصان SOC از Micro Focus و ArcSight Community تهیه شده است. ArcSight Activate شامل صدها راه حل مورد استفاده و بسته های ESM برای حل نیازهای امنیتی مدیریت رویداد شما است.

ArcSight

ویژگی های اصلی و مزایا

جمع آوری
و تجمیع log ها از
تمامی منابع IT سازمان
(شبکه، امنیت
و سرورها)

مدیریت
میلیون ها رویداد
و اطلاعات امنیتی به
منظور کسب درکی جامع
و عمیق از فعالیت های
مخاطره آمیز

نظارت
بر کاربران به
منظور شناسایی و
جلوگیری از فعالیت های
غیرمعمول و
مخاطره آمیز

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

دارای مدل های
Logger
Express
و ESM

بروزرسانی
و پشتیبانی توسط
ماهرترین متخصصین در
تیم های DVLabs
ArcSight، Fortify
و HP Labs

اعمال
سیاست های IT جهت
تخصیص منابع شبکه و
پهنای باند

ایجاد
گزارشات دقیق،
انعطاف پذیر و در
فرمت های مختلف
مدنظر سازمان

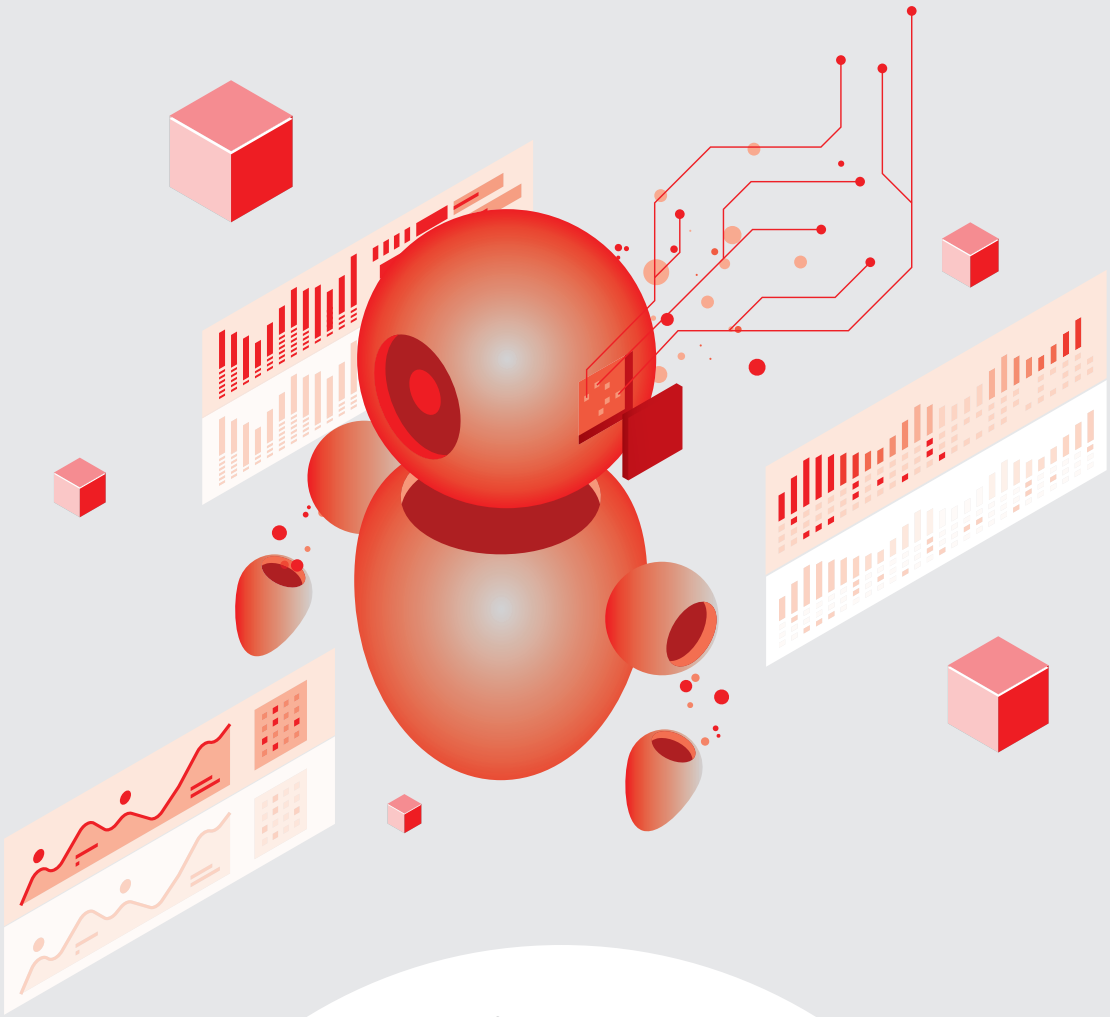
ArcSight

ArchSight بهترین راهکار SIEM

ArcSight به عنوان یک رهبر در جمع آوری و مدیریت رویداد امنیتی، قادر به ارائه راه حل‌های بهترین در کلاس برای مشتریان خود است. Obrela با استفاده از ArcSight به دنبال ارتقای امنیت سایبری و قابلیت‌ها و پیشنهادات SecOps می‌باشد. پلت فرم ArcSight با مقیاس پذیری و موثر بودن، به Obrela اجازه می‌دهد تا SecOps های سطح بالا را به مشتریان خود برای نیازهای امنیتی سایبری ارائه دهد. ArcSight چگونه می‌تواند SOC شما را بهبود بخشد و نیازهای امنیتی شما را برآورده کند؟

شرکت ArcSight محصول خود را به دو صورت ارائه می دهد

- 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 می‌شود. نسخه ESM Express به صورت پیش‌فرض دارای قابلیت‌های بیشتری نسبت به ESM است. البته این قابلیت‌های بیشتر روی ESM قابل اضافه شدن هستند.