splunk

اسپلانک یک فناوری پیشرفته و مقیاس‌ پذیر است که کلیه فایل‌های موجود در سیستم را فهرست بندی می‌کند و شما می‌توانید به راحتی در آن‌ها جستجو کنید. اسپلانک تمامی‌داده‌های موجود در شبکه و سیستم‌های شما را تجزیه و تحلیل می‌کند و سپس با استفاده از هوش ماشین، آن‌ها را مورد بررسی قرار می‌دهد. به صورت کلی از این نرم افزار برای جستجو، نظارت و بررسی بیگ دیتا توسط ماشین استفاده می‌شود و این کار از طریق رابط کاربری تحت وب انجام می‌شود. ثبت و بررسی داده‌ها در این نرم افزار در یک محیط قابل جستجو انجام خواهد شد و شما می‌توانید از داده‌های موجود نمودار، گزارش، هشدار و… بگیرید و یا برای خودتان یک داشبورد ایجاد کنید. به این ترتیب نرم افزار اسپلانک قادر به بررسی الگوهای داده، تولید معیارها، تشخیص مشکلات و… خواهد بود و می‌تواند با استفاده از هوش ماشین، آن‌ها را تحلیل نماید

بدون بررسی و تحلیل لاگ‌های ثبت شده شما هیچوقت نمی‌توانید حملات احتمالی شبکه را پیش‌بینی کنید. این لاگ‌ها تنها روشی هستند که با استفاده از آن می‌توانید مهاجمین شبکه را تشخیص دهید. حتی در صورتی که بتوانید حملات را تشخیص دهید، وقتی که به لاگ‌های ثبت شده دسترسی نداشته باشید، نمی‌توانید متوجه جزئیات حمله شوید و با آن مقابله کنید. اما اسپلانک می‌تواند با دریافت، جمع آوری و ساختار دادن به تاریخچه وقایع مختلفی که در سطح سیستم رخ می‌دهد کمک زیادی به تحلیل سریع و برقراری ارتباط بین این وقایع نماید..

اسپلانک در واقع به عنوان یک موتور جستجو برای فایل‌های لاگ موجود در شبکه عمل می‌کند. شما می‌توانید با استفاده از نرم افزار اسپلانک هر نوع لاگ متنی را با هر نوع فرمتی مورد بررسی قرار دهید. در واقع اسپلانک هیچگونه وابستگی به فرمت لاگ ندارد و فقط متنی بودن آن‌ها مهم است.

برای مثال شما با استفاده از اسپلانک می‌توانید داده‌های زیر را مورد بررسی قرار دهید:

* لاگ‌هایی که توسط تجهیزات امنیتی مثل **آنتی ویروس**، **فایروال** و **IPS** ایجاد شده‌اند.
* لاگ‌هایی که توسط تجهیزات زیرساخت شبکه مثل مودم، روتر و سوییچ تولید شده‌اند.
* لاگ‌های مربوط به نرم افزارهای داخلی مثل نرم افزار انبار، حسابداری و…
* لاگ‌هایی که توسط سیستم عامل ایجاد می‌شوند.
* لاگ‌هایی که تجهیزات الکترونیکی ساختمان مثل سنسورها، آسانسور و پله برقی ایجاد می‌کنند.
* لاگ‌های مرتبط با تجهیزات هوشمندی مثل موبایل و تبلت
* لاگ‌هایی که توسط سیستم‌های داخلی مربوط به شبکه مانند DHCP، Apache و… ایجاد خواهند شد.

نرم افزار اسپلانک تمامی‌این لاگ‌ها را به صورت یکجا ذخیره و دسته بندی می‌کند و شما می‌توانید ارتباط بین تغییرات بخش‌های مختلف را به راحتی مشاهده و در صورت لزوم آن‌ها را اصلاح کنید. همچنین می‌توانید بدون استفاده از تجهیزاتی مثل SNMP، از اسپلانک به عنوان یک نرم افزار مانیتورینگ 360 نیز استفاده کنید. (مانیتورینگ کامل)