۰۲۱ ۹۱۰۰۴۱۵۱
تهران، فلکه دوم صادقیه، بلوار آیت الله کاشانی، خ نجف زاده فروتن، خ اعتمادیان، پلاک ۴۲، واحد ۲
www.liangroup.net

splunk>

با افزایش روز افزون حملات سایبری و اتفاقات و رویدادهای داخل شبکه ها، نیاز به نرم افزارهای تجزیه و تحلیل داده Splunk که به اختصار SIEM نامیده می شوند، بطور چشمگیری افزایش یافته است. Splunk Inc یک شرکت چند ملیتی آمریکایی است که در سال ۲۰۰۳ در ایالت کالیفرنیا آمریکا تاسیس شد. محصول نرم افزاری این شرکت که به همان نام عرضه شده است، برای جست و جو، مانیتورینگ و تجزیه و تحلیل داده های سازمان ها تولید شده است. در حقیقت نرم افزار Splunk پلتفرمی قدرتمند جهت جمع آوری داده ها به منظور آنالیز و تحلیل آن ها می باشد. این پلتفرم با جمع آوری تمام لاگ های تولید شده در سطح شبکه توسط نرم افزارها، تجهیزات امنیتی و ...، اطلاعات ارزشمندی را در اختیار مدیران شبکه قرار می دهد. در انتهای سال ۲۰۱۶ بالغ بر بیش از ۱۰۰۰۰ مشتری از این نرم افزار استفاده می کردند. ماموریت این نرم افزار این است که اطلاعات سیستم ها را در یک سازمان با شناسایی الگوهای داده، ارائه معیارها، تشخیص مشکلات و ارائه اطلاعات برای عملیات تجاری، در دسترس قرار دهد.

splunk>

Splunk Enterprise چیست؟

یک نرم افزار است که داده‌های فرستاده شده از تمام برنامه‌های کاربردی، سرویس دهنده‌ها و تمام دستگاه‌های تشکیل دهنده‌ی ساختار شبکه را نمایش می‌دهد. این نرم افزاریک موتور جست و جو و تحلیل قدرتمند است که امکان نظارت، خطایابی، هشداردهی و گزارش دهی بر روی داده‌های در حال انتقال بر روی شبکه را بصورت بلادرنگ به شما می‌دهد. اسپلانک همچنین نسبت به مقیاس بسیار انعطاف پذیر است. می‌توان از Splunk به منظور حل مسائل جزئی استفاده کرد و یا آن را تبدیل به ستون اصلی تحلیل یک سازمان وسیع کرد.

Real-Time >

Splunk بصورت بلادرنگ تهدیدات را شناسایی کرده و اطلاعات مهم را برای شما و مشتریانتان فراهم می‌کند.

Machine Data >

از Splunk برای اتصال داده‌های دستگاه‌ها استفاده کنید و یک دید کلی از خطرات کسب و کار خود بدست آورید.

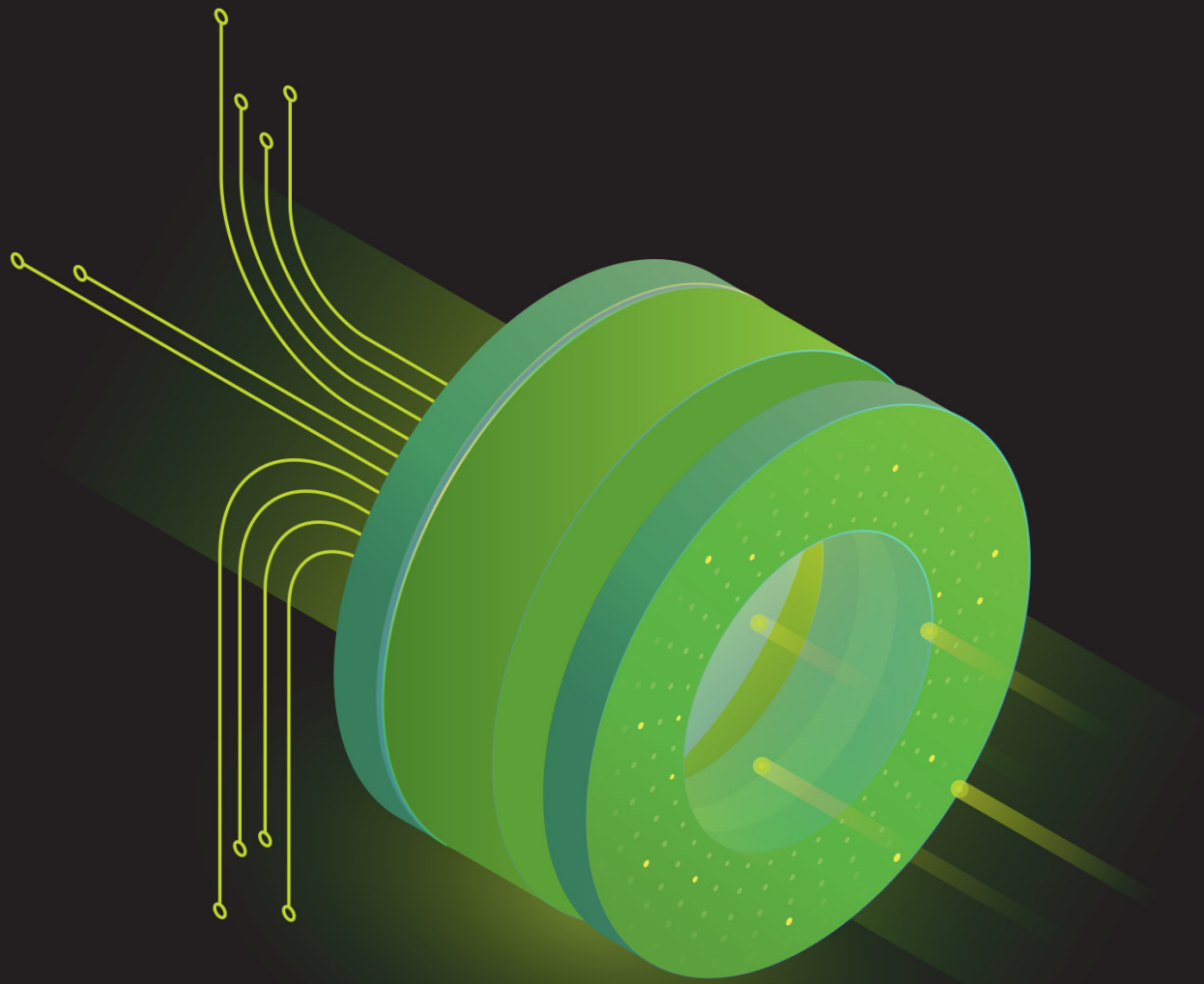
Scale >

مقیاس‌های Splunk برای نیازهای مدرن نیاز به درک پیچیدگی دارند، پس باید پاسخ‌ها را دریافت می‌کنند.

AI and Machine Learning >

اهرم هوش مصنوعی (AI) توسط یادگیری ماشین برای بینش‌های عملی و پیش بینی شده است.

www.liangroup.net >



مزایای استفاده از Splunk :

- قابلیت‌های پیشرفته در جستجو
- گراف‌های متنوع
- قابلیت‌های Parsing خودکار
- تعریف Index های متنوع
- قابلیت Data modeling
- امکان شخصی‌سازی داشبورد ها
- سرعت بالای جستجو
- قابلیت Data Mining
- قابلیت Machine Learning
- پلاگین‌ها و App های متعدد
- داشتن knowledge base بسیار قدرتمند

splunk>

www.liangroup.net