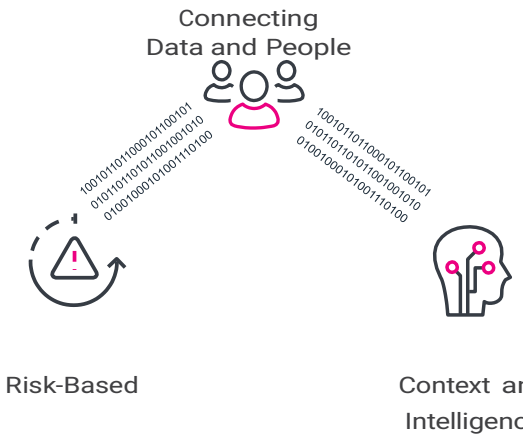
Splunk Enterprise Security

Data-driven insights for full breadth visibility, detection and investigation

Data Driven Security



- دید کامل را به دست آورید و وضعیت امنیتی را در محیط چند ابری یا multi-cloud، هیبریدی و on-premises بهبود بخشید.
- تسریع تشخیص و بررسی تهدید با استفاده از هشدار مبتنی بر ریسک ، اطلاعات تهدید یکپارچه و محتوای امنیتی خارج از چارچوب
- به سرعت محتوا را از سرمایه گذاری های فناوری با یک پلتفرم انعطاف پذیر و ادغام در ابزار ها و فناوری های multi-vendor جمع آوری کنید

تیم امنیتی شما با یک چشم انداز تهدید پویا و داینامیک ، تاکتیک های دشمن پدیدار شده و درخواست های بیزینسی در حال تحول مواجه است. اما برای رویارویی با این چالش ها ، تیم شما به قابلیت های داده محور ، دید متنی و تکنیک های دقیق تشخیص سریع تهدید نیاز دارد.این قابلیت ها می توانند به شما در کاهش میانگین زمان شناسایی و تصمیم گیری آگاهانه برای تقویت نتایج کسب و کار کمک کنند.

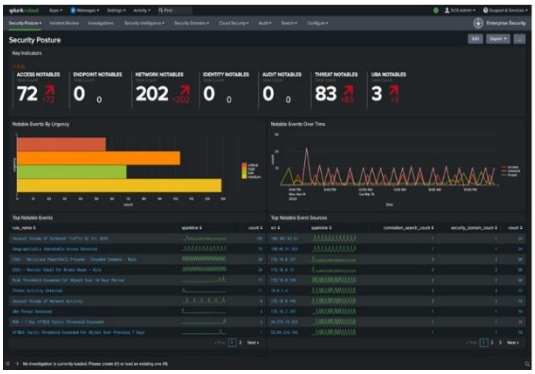
Splunk Enterprise Security (ES)یک راه حل اطلاعات امنیتی و مدیریت رویداد (SIEM) مبتنی بر داده است که یک فهم مبتنی بر داده را برای دید کامل در وضعیت امنیتی شما ارائه می دهد تا بتوانید از کسب و کار خود محافظت کنید و ریسک را در مقیاس خودتان کاهش دهید. با جستجو و گزارش بی نظیر، تجزیه و تحلیل پیشرفته، هوش یکپارچه و پیش محتوای امنیتی بسته‌بندی شده، Splunk ESشناسایی و بررسی تهدید را تسریع می‌کند و به شما امکان می‌دهد دامنه تهدیدات با اولویت بالا را برای محیط خود تعیین کنید تا بتوانید سریعاً اقدام کنید.

Splunk ESبر روی یک پلتفرم داده باز و مقیاس پذیر ساخته شده است که به شما امکان می دهد در مواجهه با تهدیدات در حال تحول و نیازهای تجاری چابک بمانید. Splunk ESبه تیم های امنیتی - با هر اندازه و سطح تخصص - کمک می کند تا عملیات امنیتی را ساده کنند. این نرم افزار موارد ذیل را فراهم می کند:

- **بیش از 1400 تشخیص خارج از چارچوب** با فریم های صنعتی مانند MITER ATT&CK ، NIST ، CIS 20 و Kill Chain
- **هوش عملی** همراه با امتیازهای ریسک نرمال شده و محتوای لازم از منابع اطلاعاتی که برای شناسایی ، اولویت بندی و بررسی رویدادهای امنیتی مورد نیاز است .
- **شناسایی در زمان واقعی** برای رفتارهای مشکوک و مخرب با استفاده از تجزیه و تحلیل جریان مبتنی بر Cloud
- **بیش از 2700 امنیت و ادغام فناوری اطلاعات** که توسط Splunk ، شرکا و اعضای انجمن ساخته شده است تا معرفی ابزارهای امنیتی و منابع داده شما به Splunkآسان شود .
- **کاهش 80 درصدی حجم هشدار** برای کاهش فرسودگی ناشی از هشدار دهی ، ارائه وضوح و اولویت بندی برای تحلیلگران و بسته شدن پرونده ها در دقایق اندک به جای هفته های متمادی
- **عملیاتی کردن چارچوب MITER ATT&CK** با یک ماتریس تجسمی که تاکتیک ها و تکنیک های مشاهده شده در رویدادهای ریسک را برجسته می کند تا در زمان بررسی رویداد ها صرفه جویی شود .
- **به سرعت دامنه یک حادثه را کشف کنید** و با دیدی جامع از عوامل اجرایی مخرب و عوامل تهدید مشاهده شده بر روی ماشین ها و کاربران به دقت پاسخ دهید.
- **پشتیبانی از هر نوع استقرار از طریق ابر** ، Multi-Cloud ، On-Premises و ترکیبی برای مطابقت با نیازهای تجاری و رشد.

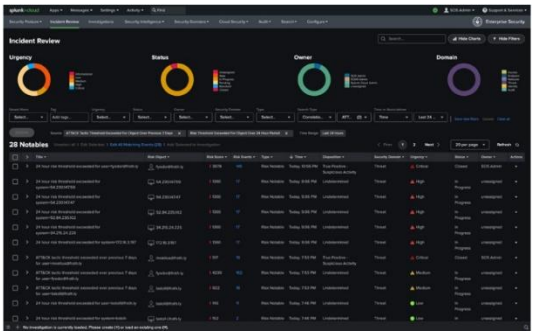
Splunk Enterprise Securityدید و بینش‌هایی را در مورد داده‌ها فراهم می‌کند که به کسب‌وکار قدرت و امنیت می‌دهد و به تحلیلگران این امکان را می‌دهد تا تصمیم‌های حیاتی را با سرعت و دقت با هدف شناسایی و دفاع یکپارچه و کامل از سازمان اتخاذ کنند.

دید کامل



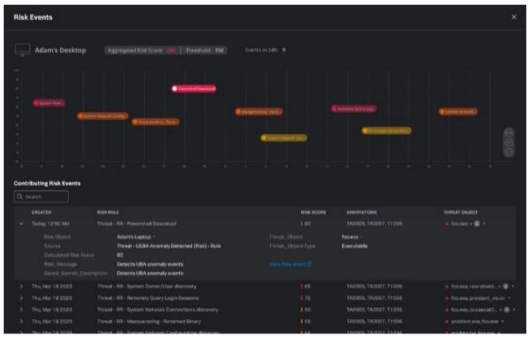
منبع های داده را تجزیه کنید و اطلاعات عملی را در وسعت کامل وضعیت امنیتی خود بدست آورید . ده ها ترابایت داده را در روز نظارت کنید – هر داده از هر کجا ، ساختار یافته یا بدون ساختار . با یک پلتفرم داده بی نظیر ، به تصمیمات مبتنی بر داده برسید که از کسب و کار شما محافظت می کند و ریسک را کاهش می دهد . امکان دستیابی به نتایج در داخل و خارج از سازمان امنیتی را فراهم میکند.

انعطاف و سازگار پذیری را افزایش دهید



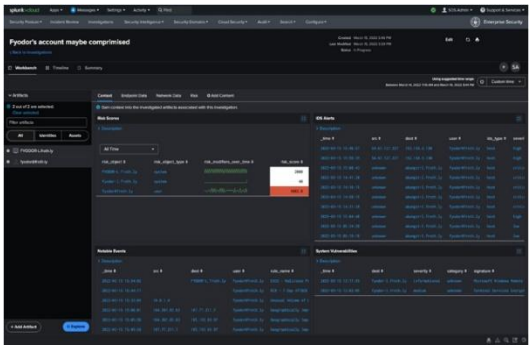
بدون توجه به اینکه سازمان در کجای مسیر ابری یا هیبریدی خود قرار دارد،در مواجهه با تهدیدها و نیازهای تجاری در حال تغییر با یک پلتفرم داده سازگار چابک بمانید . با استفاده از ادغام های فناوری ساخته شده به سرعت زمینه را در اکوسیستم امنیتی multi-vendor خود ، توسط Splunk، شرکا ، و جامعه فعال در Splunkbase که پذیرای بیش از 2500 برنامه های کاربردی و افزونه ها می باشد ، جمع آوری کنید .

تشخیص سریع تهدید



افزایش سرعت تحقیقات امنیتی تا بیش از 50 درصد با یادگیری ماشینی بدون نظارت بر شناسایی تهدیدات ناشناخته و رفتارهای غیرعادی.
با توانمند سازی و اولویت‌بندی هشدارهای با دقت بالا با هوش تهدید یکپارچه برای افزایش بهره‌وری SOC و کاهش خستگی، تحقیقات را تسریع کنید .

عملیات امنیتی خود را یکپارچه کنید



Mission Control، یک برنامه کاربردی در دسترس کاربران نرم افزار Splunk ES ، به نامنظم بودن عملیات امنیتی شما نظم می بخشد.
Splunk Mission Control .قابلیت های تشخیص، بررسی و پاسخ را در یک سطح کاری مشترک یکپارچه می کند. با کدگذاری فرآیندهای شما در قالب‌های پاسخ با قابلیت پیگیری آسان، گردش‌های کاری امنیتی را ساده می‌کند. و تیم شما را با اتوماسیون توانمند می کند تا کار تحلیلگر را کاهش دهد و سرعت پاسخگویی را افزایش دهد.