Soc- Analyst
تحلیل گر مرکز عملیات

انور عبدالله زاده

فناوری اطلاعات و ارتباطات

پتروشیمی مهاباد

Soc- Analyst
تحلیل گر مرکز عملیات

ساختار **مرکز عملیات امنیت (SOC)**

عنوان **مرکز عملیات امنیت** یا (Security Operations Center) **SOC** به یک واحد در یک سازمان اطلاق می گردد که به صورت متمرکز، تمامی رخدادهای حادثه یی و امنیتی مربوط به زیرساختهای حوزه فناوری اطلاعات و ارتباطات در سازمان را به صورت جامع و یکپارچه، شبانه روزی و بلادرنگ نظارت و مدیریت نموده و در صورت بروز هر گونه رخداد که برای سازمان ریسک ایجاد نماید، اقدامات مناسبی را جهت کاهش اثرات و رفع آن صورت می دهد.

در حقیقت ایجاد مرکز **SOC**، راهکاری مناسب جهت جلوگیری و مقابله با حوادث فضای سایبری می باشد.

مهاباد
شرکت پتروشیمی (سهامی خاص)

سطوح SOC

- Tier1: بصورت مداوم درهمان لحظه در شبکه یا سازمان حملات سایبری/ رخدادها را شناسایی و به Tier2 می دهد.
- Tier2: تشخیص کارشناس۱ را تحلیل و بررسی می کند.
- Tier3: همان مدیر SOC است که صرفا متخصص نیست و وظیفه ی آن مدیریت فرایندهای تهدیدات و نحوه ی چیدمان شیفت کارشناسان SOC
- مدیر تکنیکال: هیچ کاری با تحلیل و هک ندارد ، وظیفه ی آن طراحی و پیاده سازی بستر لازم جهت SOC
- **توانایی های SOC:**
- ۱- در لحظه ای که سیستم فعالیت مخرب داشت بایستی ببیند و متوجه شود.
- ۲- بروز بودن در زمینه انواع حملات در جهان (چه حمله ای در حال حاضر بیشتر در جهان اتفاق می افتد)
- ۳- پاسخگویی و تحلیل حوادث
- ۴- اسکن سیستم های موجود جهت ارزیابی باگ
- ۵- تحلیل بدافزار و جرم شناسایی شده
- ۶- آگاهی سازی، مشاوره و آموزش (امنیتی) پرسنل

فرایند SOC

۱- شروع با جمع آوری لاگ ها

۲- بررسی و نشانه های حملات جدید در جهان

۳- با استفاده از دیتاهایی که داریم مدل های امنیتی جدید ساخته شود و دنبال تهدیدات سایبری باشد.

۴- تاثیری که مدل امنیتی روی سازمان می گذارد را تشخیص و به حداقل برسانیم.

۵- بصورت مستمر(۲۴ ساعته) فعالیت کند.

۶ - وقایع شناسایی شده را گزارش و مستندسازی کند.

چالش های SOC

۱- کمبود نیروی ماهر

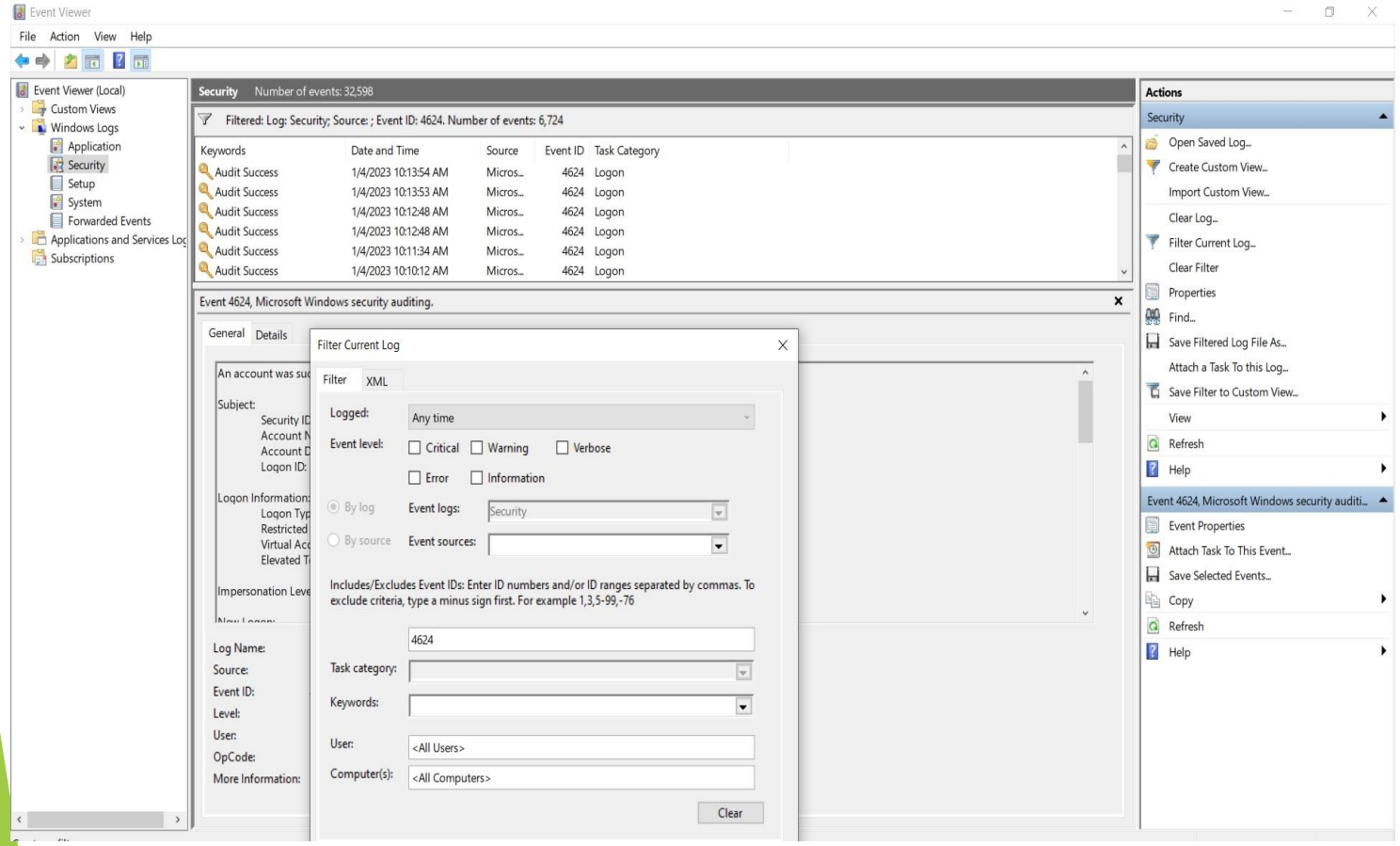
۲- ابزار خوبی در دسترس هست ولی بصورت تخصصی نمی توانند استفاده کنند.

۳- معمولا دانش خوبی در این بخش ندارند..

۴- کمبود نیروی SOC

Windows Log

- جهت بررسی در هر سیستم در قسمت Windows Log... Event Viewer قابل مشاهده می باشد.

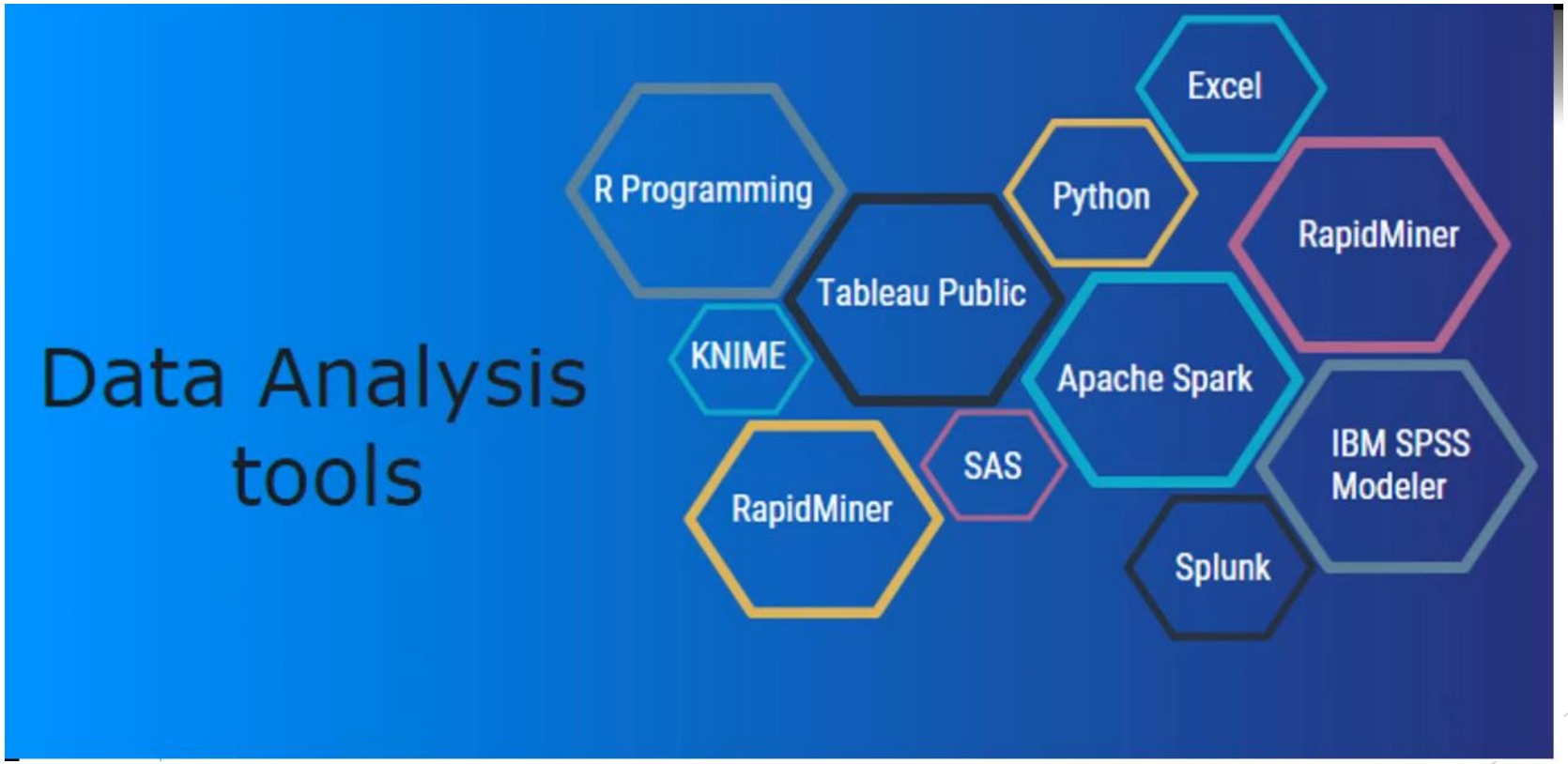


4625: Logon Field
4624: Logon Success
Logon Type:2 کیبورد
3 از طریق شبکه
4 Batch file
سرویس ویندوز5
6 unlouk
4778: remote desktop reconnected
4779:remote desktop disconnected
4647:user logoff
4634:user login
1100;system shutdown
4720:user created
1101/104:clear event

مهاباد
شرکت پتروشیمی (سهامی خاص)

SIEM
Security Information Event Management

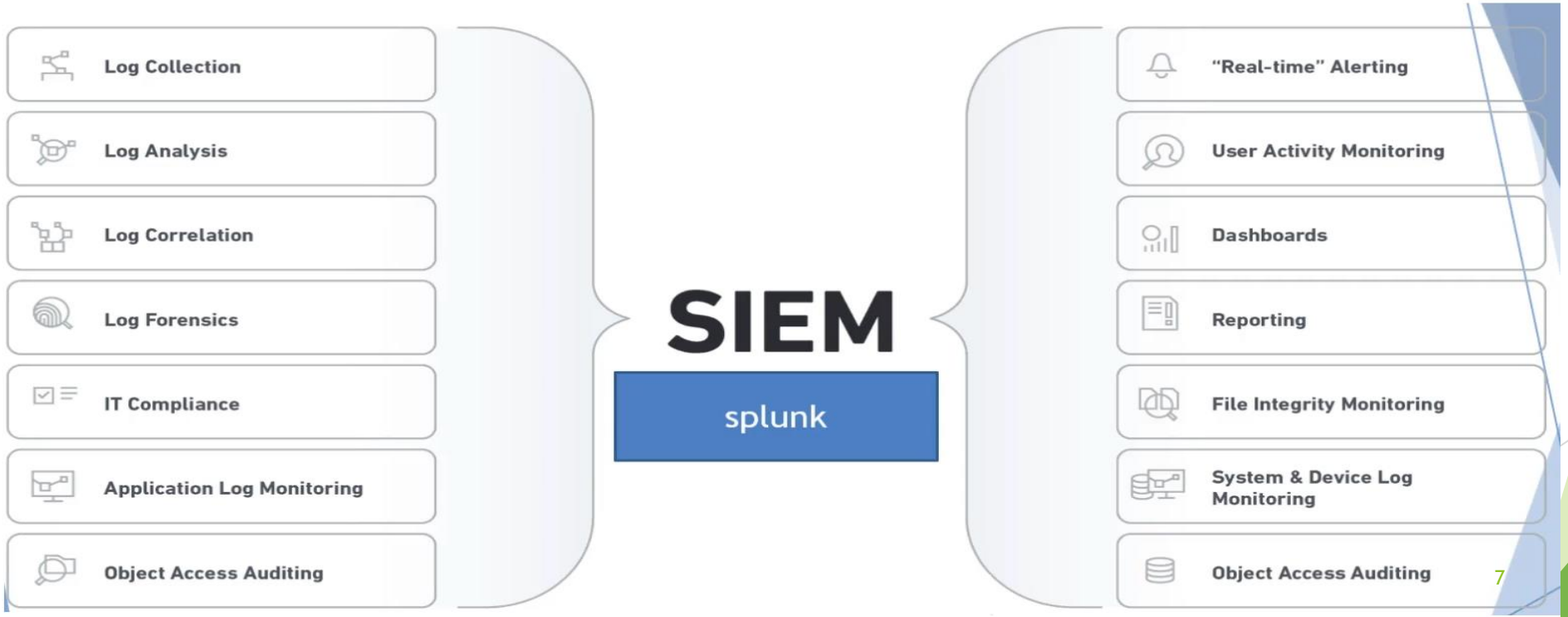
- مجموعه ابزاری است که قابلیت مدیریت رخدادها و تحلیل و بررسی لحظه ای رویداد و رخداد را به ما می دهد.



مهاباد
شرکت پتروشیمی (سهامی خاص)

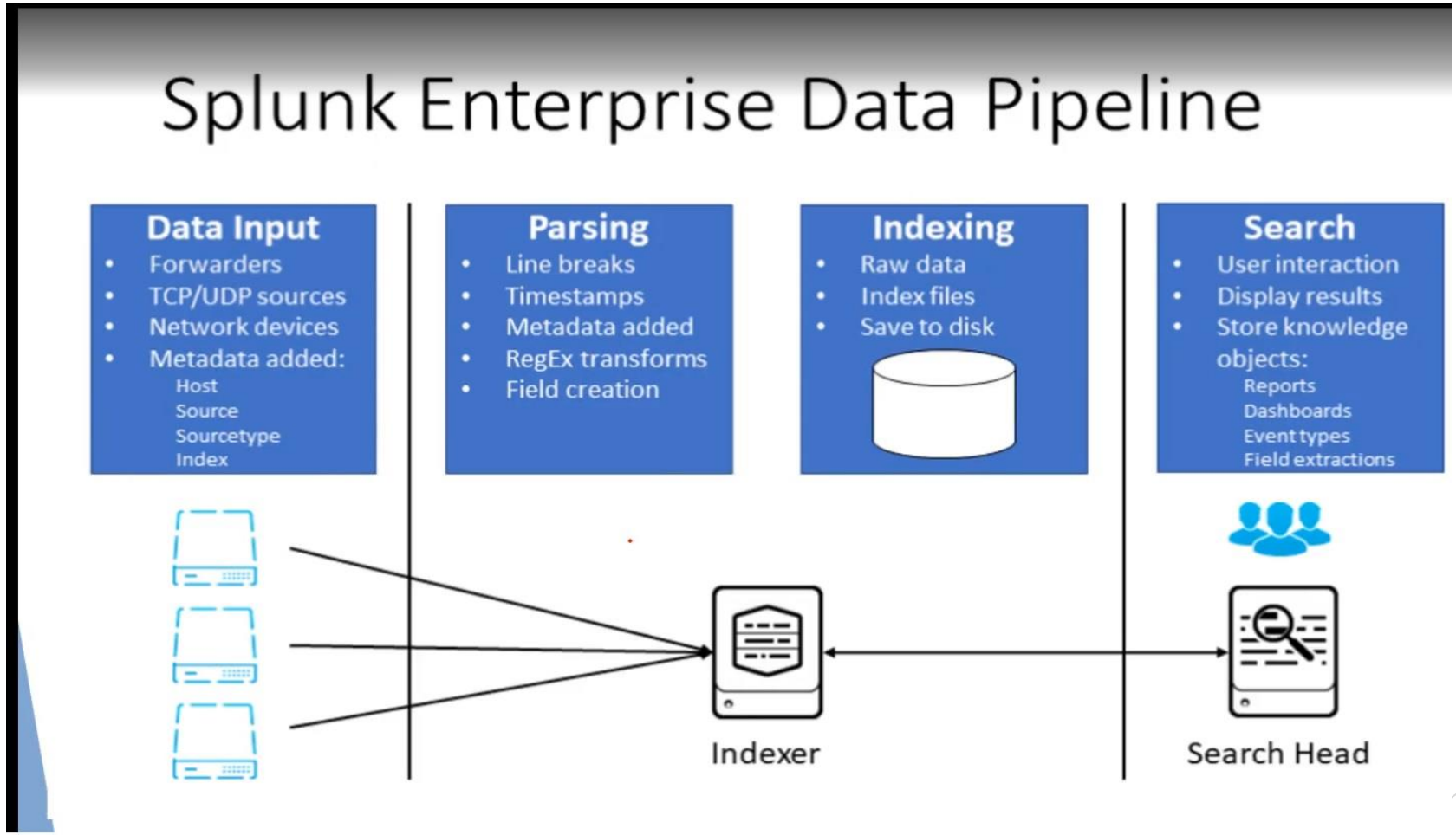
What is splunk?

- Splunk ابزاری قوی از SEIM می باشد که جهت تحلیل Big Data ها استفاده می شود.
- همیشه بروز بوده و جز ۴ ابزار اول دنیا می باشد و گزارش گیری راحت و کامل را دارا می باشد.



مهاباد
شرکت پتروشیمی (سهامی خاص)

ساختار کار Spulank Enterprise

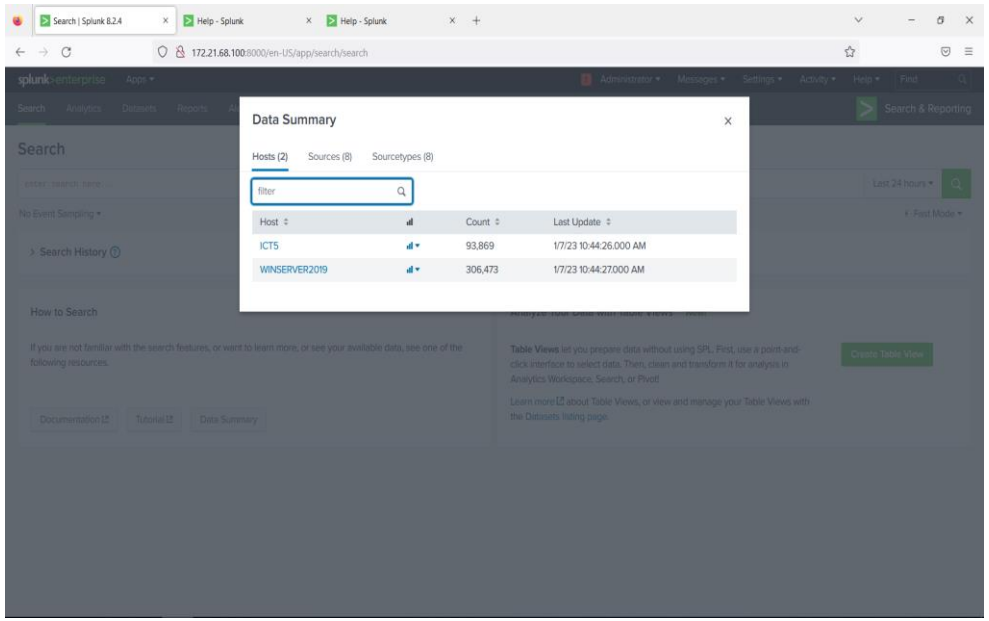


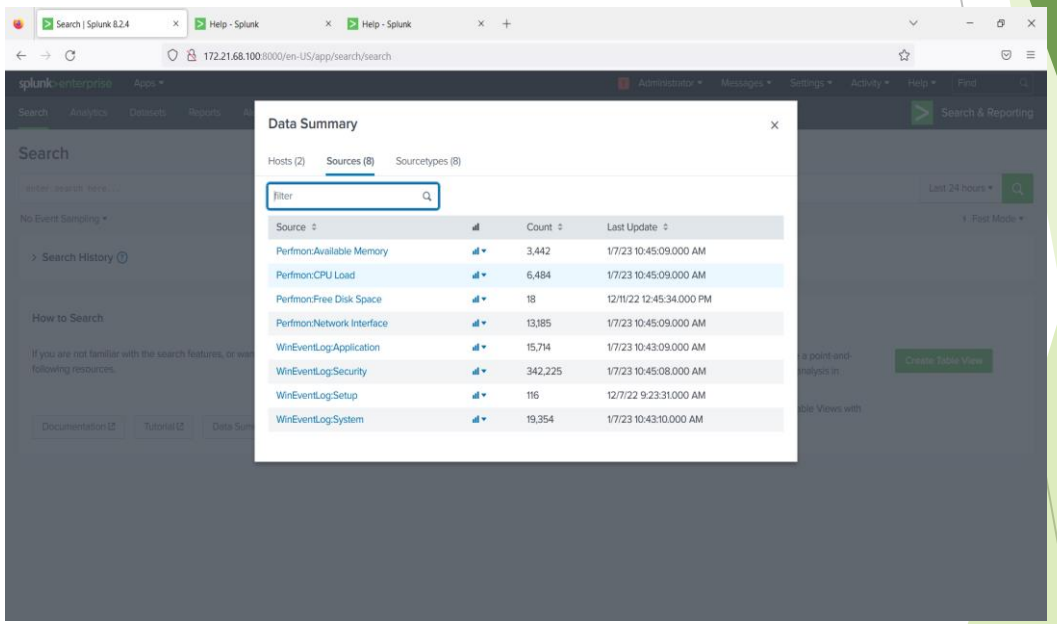
مهاباد
شرکت پتروشیمی (سهامی خاص)

نحوه کار با Splunk

- ۱- روی سیستمی که می خواهیم Log هایش را داشته باشیم ابزاری مانند Log Forwoder یا Sysmon نصب می کنیم.
- ۲- یک سرور جدا با حجم دلخواه (حجم بر حسب نیاز سازمان) راه اندازی می کنیم و Splunk را روی آن نصب می کنیم که Log های سیستم ها روی آن ارسال و ذخیره شوند.(Indexer)
- ۳- با استفاده از Splunk به تجزیه و تحلیل Log های ارسالی می پردازیم.

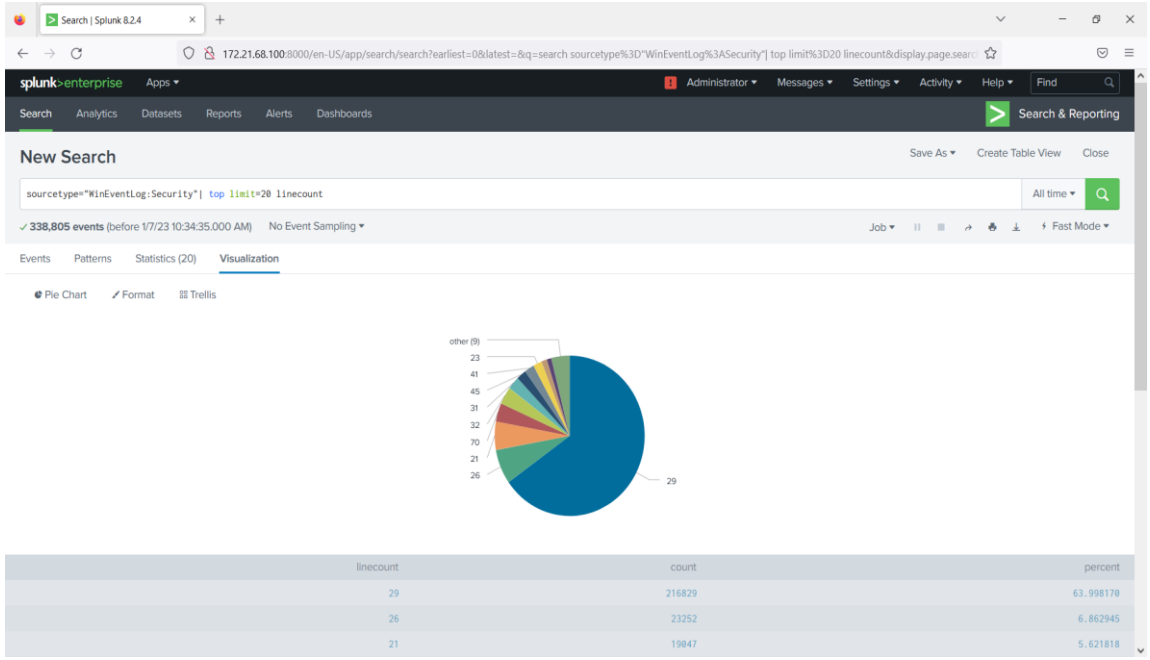
نمونه از فایل Splunk

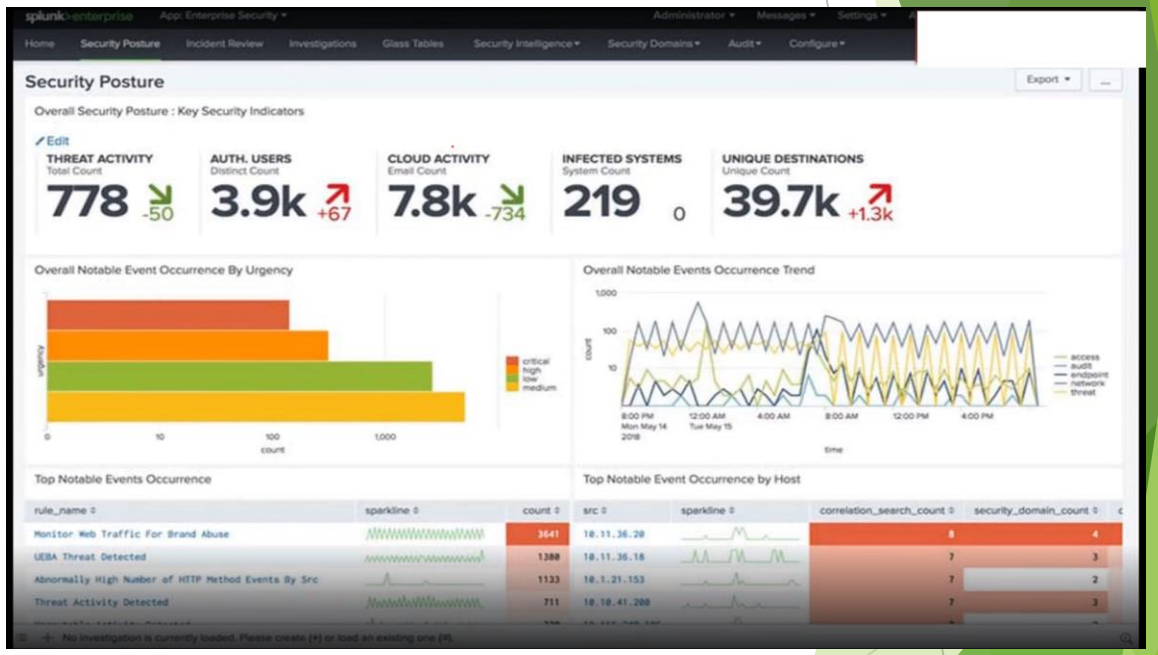




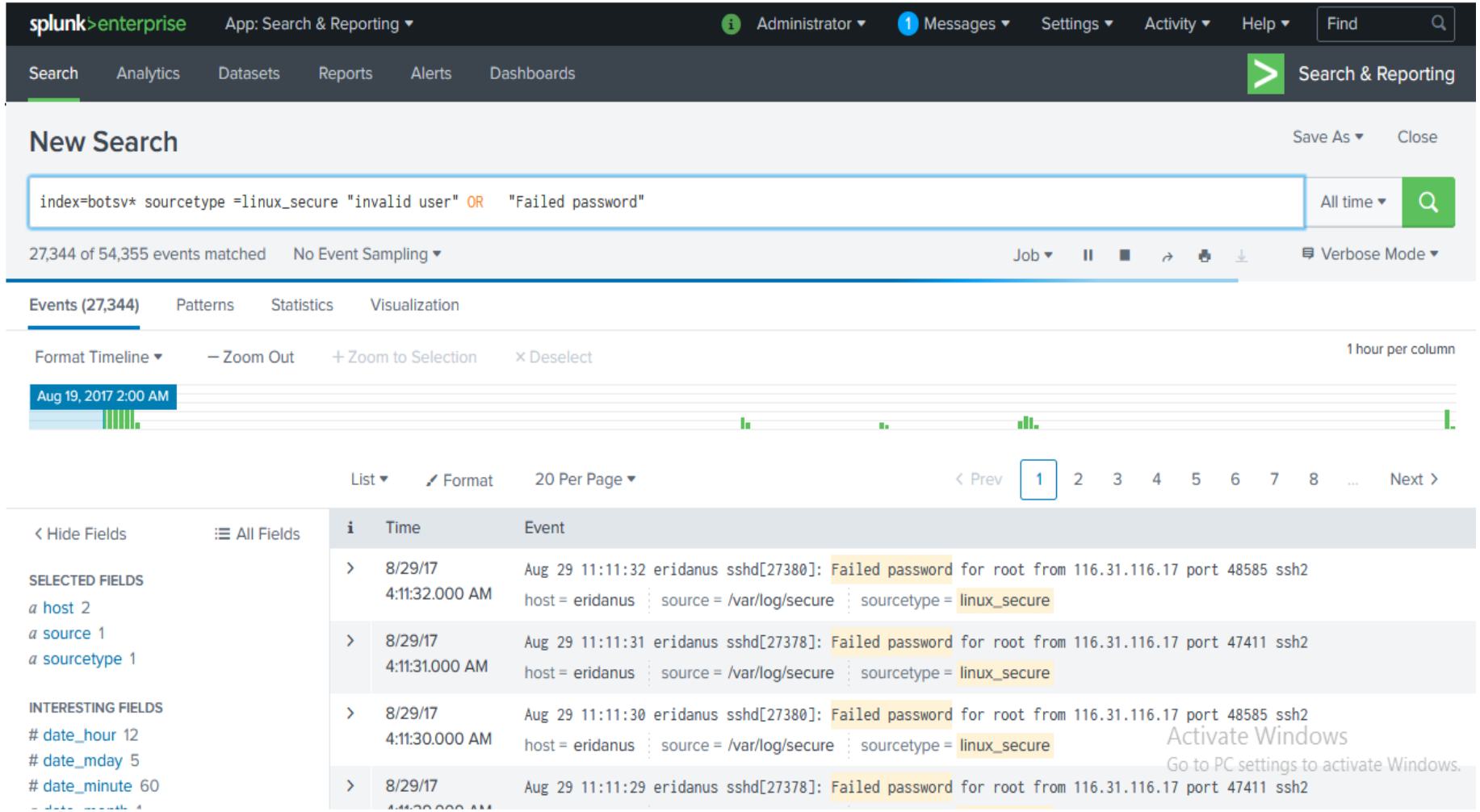
مهاباد
شرکت پتروشیمی (سهامی خاص)

گزارش گیری و داشبوردسازی





مهاباد
شرکت پتروشیمی (سهامی خاص)



مهاباد
شرکت پتروشیمی (سهامی خاص)

مهاباد
شرکت پتروشیمی (سهامی خاص)

ممنون از اینکه همراه ما بودید
لطفاً نظرات خود را با ما در میان بگذارید.

04431931256

aabdollahzadeh@mapc.ir

مهاباد
شرکت پتروشیمی (سهامی خاص)