سیستم مدیریت رخدادهای امنیتی

مهار (مدیریت هوشمند امنیت رایانه ای)

SIEM

Security Information and Event Management

- ذخیره سازی لاگ ها بصورت بهینه بر اساس تکنولوژی کلان داده
- قابلیت توسعه و تعریف شخصی انواع دیتا سورس توسط کاربر
- ماژول جستجو و اجرای فارنزیک بر روی لاگ خام ذخیره شده در دراز مدت

مهار نام پروژه طراحی و راه اندازی SIEM بومی شرکت فرازاندیشان سامانه گستر صبا می باشد که هدف آن ترکیب اطلاعات رخدادهای امنیتی و اجرای تحلیل‌های عمیق‌تر و شناسایی حملات پیچیده امنیتی می باشد.

MAHAR$_1$ | سامانه مدیریت رخدادهاست که وظیفهٔ جمع آوری، همسان سازی و همبسته سازی رویدادها را بر عهده دارد که نتیجهٔ آن کمک به کارشناسان **SOC** جهت پایش امنیت سازمان مبتنی بر سناریوهای امنیتی می باشد.

MAHAR$_2$ | سامانه ای است جهت تحلیل و پایش رخدادهای امنیتی هر دارایی و رفتار موجودیت ها به صورت بلادرنگ و مبتنی بر کلان داده. این سامانه علاوه بر شناسایی رخدادهای امنیتی، بررسی رفتارهای غیرنرمال در شبکه را بر اساس تاریخچه فعالیتها صورت می دهد.

- ماژول یادگیری ماشین با هدف رفتار غیرنرمال شبکه
- توسعه شخصی انواع هشدارها و ارسال ایمیل، پیامک و اخطار
- امکان پیاده سازی انواع قوانین همبسته سازی توسط کاربر

- طراحی و پیاده سازی سیستم مدیریت رخدادهای امنیتی مهار SIEM
- مشاوره، طراحی و استقرار فرآیندها، ابزار و ساختار سازمانی مرکز عملیات امنیت SOC
- شناسایی محصول مورد نیاز سازمان بر اساس قابلیتهای پروژه مهار
- برگزاری دوره آموزشی تخصصی در راستای پیاده سازی سیستم های SIEM
- ارایه خدمات مدیریت شده امنیتی (MSSP) به سازمانها با اتکا به SOC داخلی شرکت

Tel : ۰۲۱۲۲۲۷۱۵۸۳ E-mail : info@sabasamaneh.com Web :www.sabasamaneh.com