سامانه تحلیلگر لاگ آریادژ (ALA)

سامانه تحلیلگر لاگ آریادژ (Ariyadezh Log Analyzer) بر اساس وقایع و رویدادها ثبت شده و همچنین بر اساس دانش افراد خبره با کمک آنالیز و تحلیل های آماری و برقراری ارتباط بین رویدادها به نمایش بصری وقایع پرداخته و سعی در درک بهتر از وضعیت سایبری سازمان می نماید.

قابلیت های اساسی:

- بررسی سابقه اتفاقات و نگهداری درازمدت رویدادها به منظور رجوع در آینده بر اساس حجم ذخیره سازی در اختیار
- نگهداری اطلاعات بصورت فشرده به منظور کاهش نیاز به منبع ذخیرساز
- نرمالسازی و نمایش جزئیات رویدادهای UTM
- امکان جستجو از طریق کلیه فیلدهای مهم رویداد
- آنالیز آماری و بصیری سازی رویدادهای فایروال
- تحلیل محتوای حجمی و امنیتی رویدادهای بازدید کاربران وب
- نمایش وضعیت اتصالات VPN در گذر زمان
- مشاهده فعالیت کاربران بر اساس رویدادهای مرتبط به کاربر
- نمایش حملات و دسترسی های غیرمجاز به صورت بصری بر اساس ماژول IDS
- امکان اتصال به سامانه های هوش تهدید و کشف خودکار حوادث بر مبنای IOC