Ariadezh Log Analyzer

سامانه تحلیلگر لاگ آریادژ

وجود یک محصـــــول که بتواند لاگ های حجیم و میلیونی موجود در شبکه سازمان را دریافت، تجمیع و تحلیل نماید از نیازهای ضروری هر سازمانی است. فایروال نســـل بعدی آریادژ حجم زیادی لاگ تولید می نماید که تحلیل آنها می تواند کاری بسیار سخت و عملاً ناممکن باشد.

سامانه تحلیلگر لاگ آریادژ(Ariadezh Log Analyzer) براساس وقایع و رویدادهای ثبت شـده آریادژ و همچنین براساس دانش افراد خبره با کمک آنالیز و تحلیل های آماری و برقراری ارتباط بین رویدادها به نمایش بصـــری وقایع پرداخته و سعی در درک بهتر از وضعیت سایبری سازمان می نماید.

قابلیت های اساسی سامانه تحلیلگر آریادژ

- بررسی سابقه اتفاقات و نگهداری دراز مدت رویدادها به منظور رجوع در آینده براساس حجم ذخیره سازی در اختیار
- نگهداری اطلاعات بصورت فشرده به منظور کاهش نیاز به منبع ذخیره ساز
- نرمالسازی و نمایش جزئیات رویدادهای فایروال
- امکان جستجو از طرق کلیه فیلدهای مهم رویداد
- آنالیز آماری و بصری سازی رویدادهای فایروال
- تحلیل محتوای حجمی و امنیتی رویدادهای بازدید کاربران وب
- نمایش وضعیت اتصالات VPN در گذر زمان
- مشاهده فعالیت کاربران براساس رویدادهای مرتبط به کاربر
- نمایش حملات و دسترسی های غیرمجاز به صورت بصری براساس ماژول IDS
- امکان اتصال به سامانه های هوش تهدید و کشف خودکار حوادث بر مبنای IOC
- امکان ساخت داشبوردهای اختصاصی برای سایر تجهیزات شبکه براساس سفارش مشتری