Batis SIEM

سامانه مدیریت اطلاعات و رویداد های امنیتی باتیس

پیشـــــرفت های بی سابقه و مزایای بی شمار اینترنت و سرویس های مبتنی بر آن باعث شده است تا مســـــئله تهدیدهای امنیتی بیش از پیش مطرح شود. با گســترش فناوری های فضـــای سایبری، حملات به طور مداوم در حال افزایش و پیچیده تر شدن هســـــــتند. بنابراین، یک سازمان باید به طور مداوم در حال نظارت بر وضعیت امنیتی خود باشد تا بتواند واکنش های مناسب و فوری در قبال هر گونه تهدید نســـــبت به دارایی های سازمان نشـــان دهد. سیســـــتم های مدیریت اطلاعات و رویداد های امنیتی (SIEM) بخش اساسی از یک مرکز عملیات امنیت (SOC) هستند. این سیستم ها به سازمان ها کمک می کنند تا نه تنها دید جامعی از وضعیت امنیتی خود به دســـت آورند، بلکه زیرســـــاخت IT خود را نیز حفاظت کنند. شـــــرکت دژافزارنت با توجه به هزینه های گزاف محصـــولات خارجی و همچنین مشـــکلات محصـــولات داخلی، از جمله نیاز به منابع سخت افزاری بســـیار زیاد، تصـــمیم به توسعه SIEM جدیدی با نام تجاری "باتیس" نموده است که به جرأت می تواند، رقیب محصـــولات خارجی موجود در بازار به شمار آید.

قابلیت های اساسی سامانه باتیس

این سامانه با طراحی ماژولار خود از ماژول های اساسی زیر تشکیل شده است:

- **Big Data Framework** یک چارچوب برای پشتیبانی از لاگ ها با EPS بسیار بالا و گزارش گیری سریع از میلیارد لاگ موجود
- **Log Aggregator** تجمیع ساز لاگ
- **Correlation Engine** موتور همبسته ساز برای تشخیص حملات
- **Chain Correlation** همبسته سازی روی لاگ ها برای تشخیص حملات چند گامی آهسته
- **Threat Intelligence** هوش تهدید برای جمع آوری اطلاعات تهدیدات از منابع معتبر جهانی
- **VMS(Vulnerability Management System)** سیستم متمرکز اسکنر آسیب پذیری و داشبورد مرکزی تحلیل اطلاعات آسیب پذیری
- **SIGMA Engine** موتور قوانین سیگما برای پشتیبانی از قوانین سایر SIEM های مشهور
- **Threat Intelligence based on IOC** به منظور انطباق بر خط کلیه اطلاعات کشف شده از شبکه سازمان با نشانگرها و کشف تهدید
- **Asset Management** مدیریت دارایی های شبکه
- **Ticket Management** اتوماسیون پیگیری حوادث