سامانه مدیریت اطلاعات و رویدادهای امنیتی باتیس (Batis SIEM)

پیشرفت‌های بی‌سابقه و مزایای بی‌شمار اینترنت و سرویسهای مبتنی بر آن باعث شده است تا مسئله تهدیدهای امنیتی بیش از پیش مطرح شود. با گسترش فناوری های فضای سایبری، حملات به طور مداوم در حال افزایش و پیچیده تر شدن هستند. 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 نسبت به دارایی های سازمان نشان دهد. سیستم‌های مدیریت اطلاعات و رویداد های امنیتی (SIEM) بخش اساسی از یک مرکز عملیات امنیت (SOC) هستند. این سیستم ها به سازمان‌ها کمک می‌کنند تا نه تنها دید جامعی از وضعیت امنیتی خود به دست آورند، بلکه زیرساخت IT خود را نیز حفاظت کنند. شرکت دژافزارنت با توجه به هزینه های گزاف محصولات خارجی و همچنین مشکلات محصولات داخلی، از جمله نیاز به منابع سخت افزاری بسیار زیاد، تصمیم به توسعه SIEM جدیدی با نام تجاری "باتیس" نموده است که به جرأت می‌تواند، رقیب محصولات خارجی موجود در بازار به شمار آید.

قابلیت های اساسی:

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 برخط کلیه اطلاعات کشف شده از شبکه سازمان با نشانگرها و کشف تهدید (دامنه، IP، نام فایل، MD5 و ...)
- **Asset Management**
  مدیریت دارایی های شبکه
- **Ticket Management**
  اتوماسیون پیگیری حوادث