



The Agile Security Information & Event Management (SIEM) Service

Are you effectively monitoring your IT and organisation?

Recent high profile company Information Security breaches have demonstrated that attacks are now targeted and tailored to specific companies. These are not casual criminal hackers, but professionals aimed at stealing your data to gain economic or intellectual advantage. In nearly all the recent cases, subsequent investigations demonstrated that it would have been possible to pick up lead attack indicators, by inspection and correlation of security log and event information.

Individual systems are generating vast amounts of security log information, however, there is often little correlation between them and too many false positives. Enterprises spend more effort in maintaining point security monitoring solutions, than they do on acting on potential intelligence being generated. In addition, organisations find it challenging to hire and retain the required expert staff, to operate security monitoring and management solutions, often supporting multiple countries around the clock.

“Security events are being logged, but is anyone paying attention?”

To resist external attacks and internal breaches, Enterprises need an agile and adaptable Security management and monitoring service

CIPHER'S 24x7 Agile Security Information Event Management (SIEM) Service is built on leading industry solutions, with state of the art log collectors, correlation engines and investigation capabilities.

- Strong, scable and reliable log collection and retention engine
- The first MSSP worldwide to be ISO 20000 and ISO 27001 certified
- Business oriented dashboards and reports



- CRM, ERP, E-Commerce and Databases long with fraud detection intelligence
- Filtering aggregation and correlation to avoid bandwidth limitation and false positives
- More than 1 million events monitored per day!

CIPHER is the most proactive Managed Security Service Provider in the market

The service is supported by security experts trained in vertical segments, which allows them the ability to identify lead event indicators, within financial services, utilities, communications, retail, aviation and hi-tech enterprises. The benefits are:

- Fast threat assessment to reduce Enterprise risk
- Scalable, from basic monitoring (supporting compliance) through to full managed service
- Constant innovation on correlation rules and detection techniques
- Business vertical alignment to identify sector specific threats
- Reports and dashboards, which constantly evolve with the customer

Get to know about CIPHER:

-10+ years in supplying for global Enterprises in 35 countries

- More than 300,000 assets managed at 24x7 Security Operation Centres.

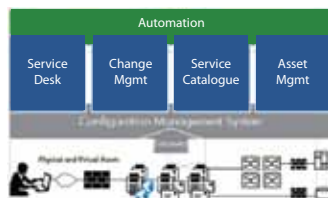


What next?

CIPHER recommends that the first step is for an Enterprise to map they key assets for event management, followed by defining abuse rules scenarios with associated incident response requirements. This will allow for the efficient transformation of the network, security and application logs into meaningful events than can be monitored by an agile security management process.

Gap Analysis	Design & Implementation	Continuous Improvement
<ul style="list-style-type: none"> ■ Critical asset identification ■ Compliance and internal security retention and reporting needs ■ Incident response and service level requirements 	<ul style="list-style-type: none"> ■ Log Repositories and Sensors ■ Connector placement and bespoke development ■ Correlation engine with CIPHER customised security use cases and rules 	<ul style="list-style-type: none"> ■ Customised Dashboard Views ■ Feedback from CIPHER Intelligence Labs ■ Security Improvements and Re-engineering based on incidents reported

On-going Management & Operations



About CIPHER

CIPHER is a multinational, specialist Information Security and Risk Management company, with over 300 employees. Our services include; Consulting and Auditing (PCI-DSS QSA, ISO 2700x and industry / country regulations), Award winning security system integration and 24x7 SOC/SIEM, with over 300,000 assets under management in 35 countries, correlating 1,000,000 events daily. In addition, we conduct Research & Development through our Intelligence Lab, supporting the CIPHER university and (ISC)² training centres. CIPHER is dedicated to delivering quality, excellence and innovation.