



# Mindtree

*Welcome to possible*

## Real time security monitoring and management service.

### Business challenges

- How do I ensure proactive management to ensure protection against all information security threats?
- How do I make sure I comply with all relevant regulatory and compliance requirements?
- Do I know the threats and malicious activities that are targeting my operations on a daily basis?
- Is it possible to get alerts only for genuine information security threats and not waste time on false positives?


Enterprises face both external and internal threats to their data, network and IT assets. The attacks on data (like IP spoofing attack) are now sophisticated enough to catch enterprises off-guard. This can lead to financial loss, civil liabilities due to customer lawsuits, serious disruption of day-to-day operations and loss of image with customers and regulatory agencies. It is important for enterprises to have a proactive system that keeps track of activities in their network, servers and other IT assets on a 24/7 basis. This helps track down malicious activities and stop them before they cause damage.

### Our offering

Mindtree's real time security monitoring and management service helps you keep track of all traffic that passes through your IT infrastructure – your network, your data centre, your servers, your routers / switches and your security devices like firewalls, UTM devices, IDS devices. Using advanced event correlation technology, we help you with real time alerts when we sense genuine threats and help you take appropriate action to stop the malicious activity from progressing, thereby protecting your data and IT assets from getting compromised. Our event correlation technology also helps prevent wastage of time due to false positives i.e. genuine activities which can be mistaken for malicious activities.

### Key features

- State-of-art event correlation and trend analysis
- Pattern discovery and behavioural analysis
- Integrated with early warning global threat advisory
- Customized reports through Secure Service Portal providing real time alerts and tailor-made reports
- Action taken based on your decision after seeing the alert



Mindtree delivers this service through our ISO 27001 certified ArcSight deployed Global Security Operations Centre (GSOC). This GSOC is staffed with certified and experienced security professionals (with certifications like CISA, CISM, CEH, AESA and technical certifications across various security technologies), who monitor and manage your services 24x7x365. GSOC is a global operations centre and a single point of contact for all your support needs. Our tools deployed in GSOC identify real threats in IT infrastructure and eliminate false positives leveraging the advanced event correlation capabilities of ArcSight. Client-specific delivery models (in-premise, shared services and hybrid) and SLAs are executed.

### Key benefits

- World leading ArcSight SIEM tool-based real time 24x7x365 security alert service
- Can meet all compliance requirements including log storage
- Build and monitor customer-specific use cases thereby customizing the service to your organization's needs
- SLA based service plus hybrid delivery models to minimize your security risks and reduce overheads
- Real time report and actionable insights from MWatch Secure Service Portal
- Trusted advisory services to keep your organization up-to-date on latest security threats
- Predictable management of costs and protection delivered by experts, so you can concentrate on your core business

### About Mindtree

Mindtree is a global information technology solutions company with revenues of over USD 400 million. Our team of 11,000 experts engineer meaningful technology solutions to help businesses and societies flourish. We enable our customers achieve competitive advantage through flexible and global delivery models, agile methodologies and expert frameworks.