

Mindtree security log review and analysis service

Business challenges

- How do I get to know the different types of attacks my organization is subjected to?
- Can I proactively keep track of compliance violations my employees are committing?
- How do I use my security logs to significantly reduce security and data loss incidents?
- Is there a data-based intelligent way to take decisions on my future security investments and initiatives?


Enterprises face both external and internal threats to their data, network and IT assets. These days the attacks are so sophisticated (like IP spoofing and DDOS attacks) very often the enterprises become aware of the threat only after they have been compromised. This can lead to financial loss, civil liabilities due to customer law suits, serious disruption of day-to-day operations and loss of image with customers and regulatory agencies. So it is important for enterprises to have a proactive system to keep track of activities in their network and other IT assets by analyzing the logs of activities on their servers, routers, switches, firewalls, intrusion detection systems etc.

Our offering

Mindtree's security log review and analysis service is based on industry-best practices in analysis and reporting. It is multi-faceted and extremely customizable to suit your requirements. Our log analysis can be done on a daily basis to help you take immediate measures against threats or on a weekly basis to analyze trends and change policies or on a monthly basis to analyze weekly trends, analyze dormant anomalies and take action based on accumulated data and thereby improve your security posture step by step.

Key benefits

- World leading ArcSight SIEM tool-based service
- Significant reduction in security incidents and data loss incidents
- Decrease in downtime due to security incidents
- Reduced number of malware incidents
- Can successfully navigate through third party security audits
- Can plan your security investments and initiatives based on real data from your IT infrastructure
- Peace of mind due to 100% compliance



Mindtree's security log review and analysis service will involve understanding of your – network topography and security policies, classification of IT assets, operating systems and applications and the setting up of criteria to classify severity of security events to identify incidents to take action on. The process of log analysis will include prioritization of log entries by using parameters such as source and destination IP address, identifying the log source, finding out the frequency of entry, identifying the device on which the event has occurred, identifying the attack signature, evaluating the initiator and target IPs and calculating duration of the event. Our report will give both strategic and tactical recommendations and some of the key areas covered in our report would be – key problems needing management attention, top attacks your organization has faced during a particular period, compliance violations noticed, immediate action steps the management needs to take, top user account privilege changes during a particular period, changes required in firewall rules etc.

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 (they have 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.

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.