Mindtree

*Welcome to possible*

# Managed IDS and IPS services.

## Business challenges

- How do I get the best value from the security devices I have invested in?
- Is it possible to identify and stop attacks and security breaches in progress?
- What are the best practices in managing policies and monitoring of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)?
- How do I reduce operational expenses in maintaining my security infrastructure and also ensure best in class management?

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) play a crucial role in preventing harmful traffic from entering trusted areas of your network and systems. A defense in depth information security strategy demands that you implement IDS and IPS in your network and servers. However, maintaining an IT team to manage and monitor these systems 24/7 and respond to alerts and warnings is very time-consuming and cost prohibitive. As a result, many leading enterprises are outsourcing the monitoring and management of their IDS and IPS to reduce the burden on their in-house staff, to get best-in-class service from experts and to reduce operating expenses over time.

## Our offering

Mindtree's managed IDS and IPS Service has been carefully designed to fit the diverse requirements of today's connected enterprises. It provides a more effective early warning system for threats and attacks through 24x7x365 monitoring by our team of experienced security engineers. Mindtree has a managed IDS and IPS service designed to align with each individual organization's security initiatives and budgetary requirements. Our service supports a wide range of IDS and IPS platforms – Cisco, Juniper, ISS, McAfee, Tipping Point etc.

## Key features

- Customized planning, design and configuration of contracted IDS and IPS
- Distinct and tailor-made SLA terms to handle your unique requirements
- Handle routine as well as emergency policy changes within a well-defined time frame
- Monthly vulnerability scanning and patching of the IDS and IPS operating systems
- 24/7 monitoring of IDS and IPS security event data using ArcSight SIEM tool
- Provide extended log archival capabilities for regulatory compliance
- Access the real time alerts as well as routine reports from our MWatch – Secure Service Portal

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, who have technical certifications for leading IDS and IPS platforms such as Cisco, Juniper, ISS, McAfee, Tipping Point etc. as well as professional services certifications like CEH, CISSP, CISA etc. They monitor and manage your IDS and IPS 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 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

- Minimize risk of business impacting security breaches
- Increase coverage levels through 24x7x365 management and monitoring by experienced security engineers
- Take advantage of ArcSight SIEM tool's event correlation capabilities, thereby identifying genuine security threats and reducing false positives
- Reduce security administration overheads and use expensive internal staff for other core business functions
- Obtain early warning security intelligence from the Secure Service Portal, to proactively protect business operations from unnecessary down-time and loss of data
- Can meet all compliance requirements including log storage

## 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.