Intrusion Monitoring

Detect, alert and get recommendations in the event of intrusion

Short description:
Network security service: detection and prevention of network intrusion and/or endpoint intrusion.

Key benefits:
Supervise, analyse, remediate and protect your network's infrastructure and endpoint against intrusion or cyber attacks.

Service family:
- Advanced Security Monitoring

AIRBUS

Service description

Detailed description	• Supervision service adapted to your current or targeted security level in order to maintain and/or improve it. • Detection in real time of behaviour covered by the supervision. • Notification and communication of suspicious behaviour and potential impact on infrastructure and business operations. • Recommendations and action plans. • Maintenance and expansion of knowledge database, including 'reflex sheets' to facilitate qualification of incidents and to provide remediation plans. • Capture of suspicious flows (networks, memory and storage) to improve numerical analysis and investigation. A service desk is also included as standard.
Opening hours	Three options available: • 24/365 • 7am-9pm, Monday-Sunday • 9am-6pm, Monday-Friday During service hours, the team is reachable by telephone or email. A web portal is also available to follow on-going incidents and consult dashboards.
Service level agreement	• Availability of service. • Efficiency of service. • Service attributes.
Operational follow-up	• Weekly meeting (technical and operational): allows both operational teams to work together and exchange information related to on-going activity. • Monthly meeting: service overview (incident review, analysis, tendencies, recommendations, financial review). • Quarterly meeting: review last period's strategy and define strategy for the next 6-month period (new perimeters, new services).
Deliverables	• Notification of security incidents or suspicious behaviour with accompanying action plan. • Monthly report detailing the level of service provided and achievement of key performance indicators. • Quarterly reports on security dashboards. • On-demand reports or analyses (additional charge applies). A secure and dedicated web portal is available to access documents.
Available offers	Service quotations on request, depending on: • Opening hours. • Volume and types of equipment. • Scope of detection (network and hosts).

Airbus CyberSecurity
Metapole 1, boulevard Jean Moulin / CS 40001 / 78996 Elancourt Cedex / France
Willy-Messerschmitt-Str. 1 / 82024 Taufkirchen / Germany
Quadrant House / Celtic Springs / Coedkernew / South Wales NP10 8FZ / United Kingdom
Etihad Towers T3 / Corniche Road, 19th floor / P.O.Box: 72186 / Abu Dhabi / United Arab Emirates
www.airbus-cyber-security.com / contact.cybersecurity@airbus.com