DEFENCE AND SPACE
Cyber Security

# Advanced Threat Monitoring

## Advanced Threat monitoring

**Service description**
APT monitoring is a service providing detection and qualification of malicious activities (including Advanced Persistent Threats – APT) and suspicious behaviors thanks to weak signal analysis, based on our Keelback® Net solution (network sensor and analytic platform) and our extensive security expertise as well as our threat intelligence capability.

**Key customer benefits**
- Flexible solution, adaptable to your existing infrastructure
- Qualified notification by our security analysts
- Clear corrective measures, adapted to your business
- Reactivity thanks to our Keelback Net solution

AIRBUS

# Service description

| | |
|---|---|
| **Detailed description** | • Deployment of a tailor-made and flexible solution compatible with existing security equipment<br>• Capture of traffic flows (FPC) and metadata (DPI) through sensors (Keelback Net)<br>• Analysis of suspicious files<br>• Maintenance and/or improvement of your security status and provision of an amended supervision strategy<br>• Real-time detection of malicious behaviour<br>• Traffic trends analysis (including weak signals) to highlight suspicious behaviour<br>• Qualification and notification of suspicious behaviours and malwares, including their material effect on infrastructure and their operational impact<br>• Recommended actions for containment and remediation. |
| **Opening hours** | Three options available:<br>• 24/365<br>• 7am-9pm, Monday-Sunday<br>• 9am-6pm, Monday-Friday<br><br>During service hours, the team is available by phone or email.<br>A web portal is also available to follow on-going incidents and view summary dashboards. |
| **Service level agreement** | • Time to qualify and notify a critical behaviour: near real time<br>• Time to detect known and emerging threats: quasi instantaneous thanks to threat intelligence capabilities |
| **Operational follow-up** | • Weekly meetings (technical and operational): provides an opportunity for operational teams to work together and discuss on-going activity.<br>• Monthly meeting: service overview (incident review, analysis, trends, recommendations, financial reviews).<br>• Quarterly meeting: strategic review of the last period and opportunity to define the strategy for the coming months (new perimeters, new services). |
| **Deliverables** | • Notification of qualified alerts with associated action plan<br>• Weekly, monthly and quarterly reports |
| **Available offers** | Service quotation on request depending on:<br>• Opening hours,<br>• Bandwith of the monitored network flow. |



**Airbus CyberSecurity**
Metapole 1, boulevard Jean Moulin / CS 40001 / 78996 Elancourt Cedex / France / T: +33 (0) 1 61 38 50 00
Willy-Messerschmitt-Str. 1 / 85521 Ottobrunn / Allemagne / T: +49 (0) 89 607 - 0
Quadrant House / Celtic Springs / Coedkernew / South Wales NP10 8FZ / Royaume-Uni / T: +44 (0) 16 33 71 30 00
Etihad Towers T3 / Corniche Road, 19th floor / P.O.Box: 72186 / Abu Dhabi / Émirates Arabes Unis
**www.cybersecurity-airbusds.com / contact.cybersecurity@airbus.com**