

CyberSecurity

AIRBUS



SOC 4.0 Managed Security Services





Securing Critical Business

SUMMARY



Introduction

- Why a SOC service is needed
- Challenges in OT security monitoring and operations

SOC 4.0 Managed Service

- SOC 4.0 at a glance
- Protective Monitoring
- Additional Services
- Cyber on Demand Services

SOC 4.0 Features

- Security Information and Event Management (SIEM)
- Monitoring and Data Onboarding
- Use Cases Developments
- Asset Inventory and Network Mapping
- Vulnerability Management
- Malware Detection
- Anomaly Detection
- Incident Response
- Cyber Threat Intelligence
- Log Management

What can SOC 4.0 monitor

- Purdue Model
- ICS assets types
- Industrial Protocols

Service model description

- SOC 4.0 offering models
- SOC 4.0 operating hours
- SLA

Why Airbus CyberSecurity

- Our SOC experience
- What makes us different
- Contact details

INTRODUCTION



Why a SOC service is needed

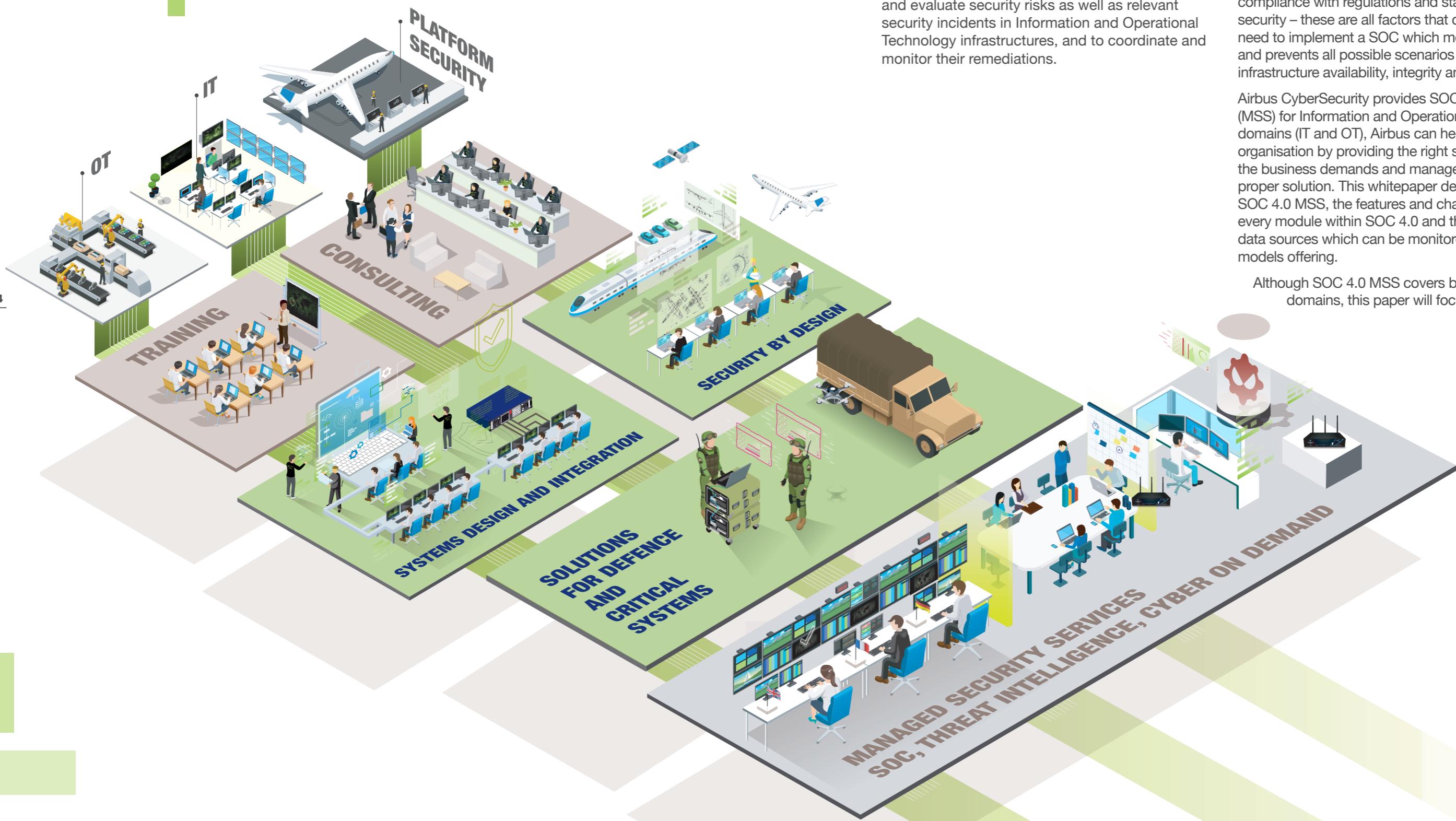
A Security Operation Centre (SOC) is defined as a combination of experts, tools and processes in order to detect, prevent, analyse and evaluate security risks as well as relevant security incidents in Information and Operational Technology infrastructures, and to coordinate and monitor their remediations.

Challenges in OT Security Monitoring and Operations

The increase of cyber-attacks that target Industrial Control Systems (ICS) and Operational Technology (OT), plus the digital transformation, Industry 4.0 and IIoT technologies that establish more connectivity for the ICS are all providing challenges to OT operators. Additionally, the threats from supply chain and information sharing between organisations, compliance with regulations and standards for cyber security – these are all factors that contribute to the need to implement a SOC which monitors, detects, and prevents all possible scenarios affecting the OT infrastructure availability, integrity and confidentiality.

Airbus CyberSecurity provides SOC as a service (MSS) for Information and Operational Technology domains (IT and OT). Airbus can help your organisation by providing the right services to meet the business demands and manage the risks in a proper solution. This whitepaper demonstrates Airbus SOC 4.0 MSS, the features and characteristics for every module within SOC 4.0 and the assets... and data sources which can be monitored and SOC 4.0 models offering.

Although SOC 4.0 MSS covers both IT and OT domains, this paper will focus on the OT side.



SOC 4.0 Managed Security Service Portfolio

SOC 4.0 at a Glance

Airbus SOC 4.0 is a managed security service to monitor Information and Operational Technology (IT & OT) infrastructures, detect and prevent security incidents and cyber-attacks, equipped with systems and tools to enable the required SOC functionalities. The SOC 4.0 MSS portfolio consists of three main categories as illustrated in Figure 1: the core Protective Monitoring service; Advanced Services; and on-demand Consulting services.

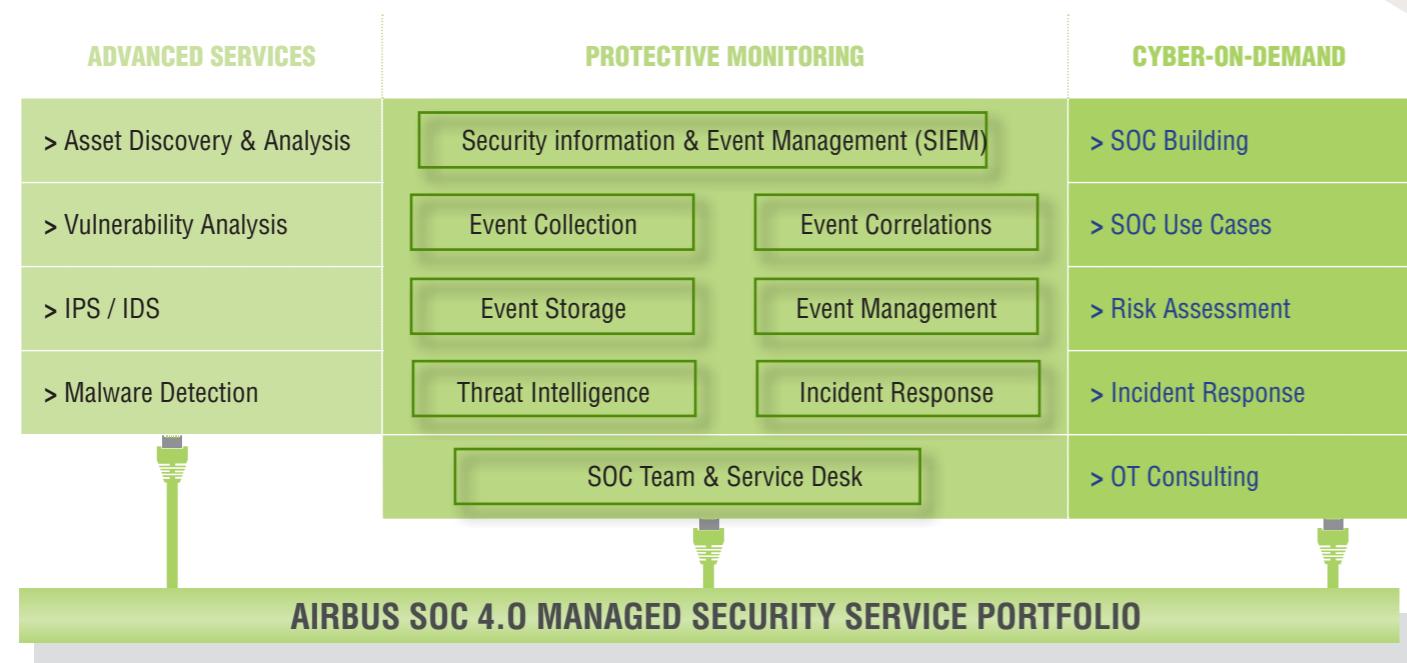
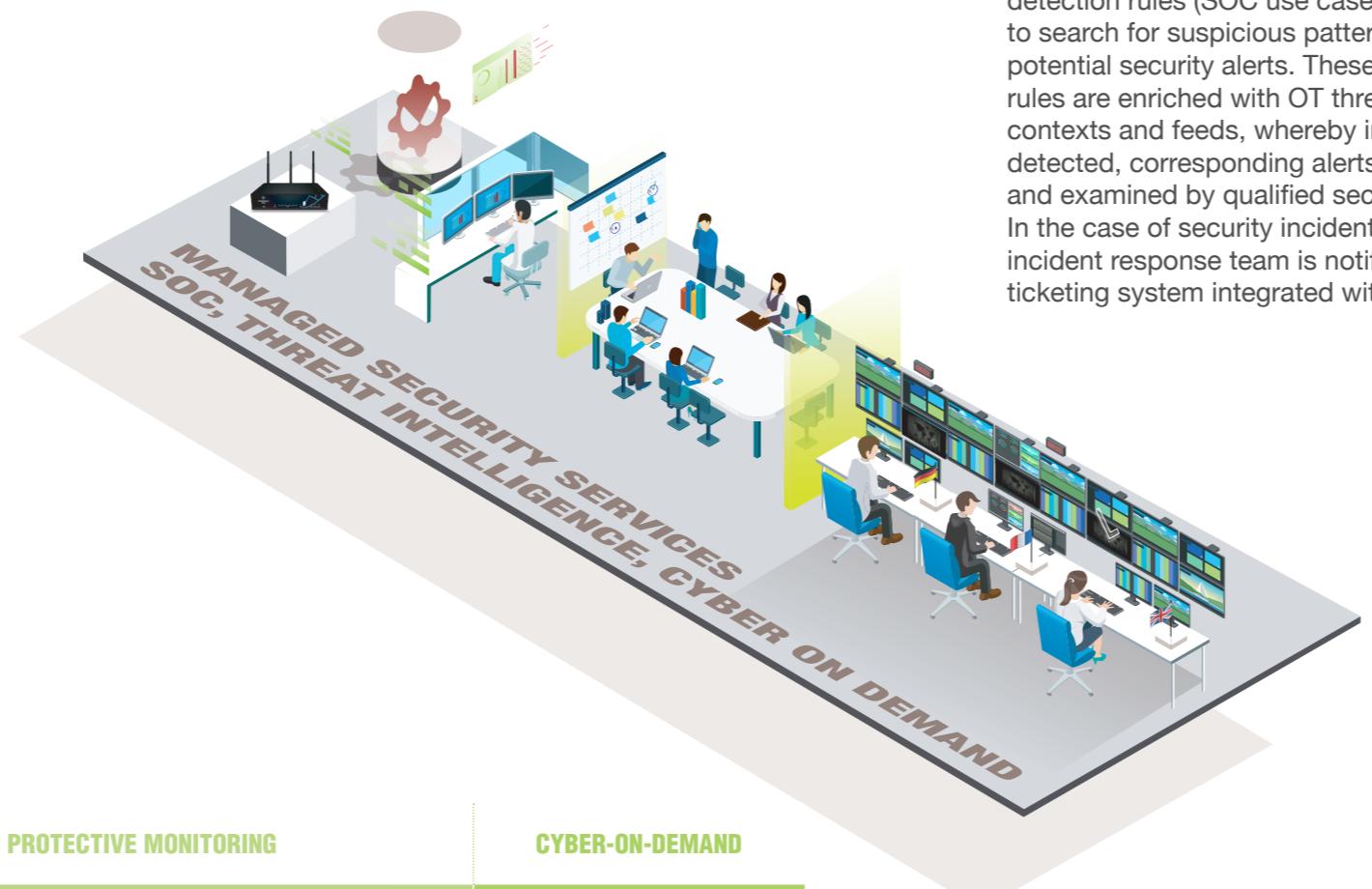


Figure 1: Airbus SOC 4.0 Managed Security Service Portfolio

Protective Monitoring

Protective Monitoring is the core service of Airbus SOC 4.0 for OT security monitoring. Within this service, security logs and operational data from OT assets such as PLC, RTUs, SCADA, Engineering station, Historians, etc. are captured, collected, forwarded, stored, and processed in very high numbers (up to 1500 events per second). The events are then correlated using specific and customised detection rules (SOC use cases) which are used to search for suspicious patterns and indicate potential security alerts. These detection rules are enriched with OT threat intelligence contexts and feeds, whereby irregularities are detected, corresponding alerts are generated and examined by qualified security analysts. In the case of security incident discovery, the incident response team is notified using the ticketing system integrated within SOC 4.0.

Advanced Services for SOC 4.0

Additional and advanced capabilities can be added on top of the core service to empower SOC operations in order to meet customers' specific demands. SOC 4.0 is a modular service that provides flexibility to accommodate any future expansions.

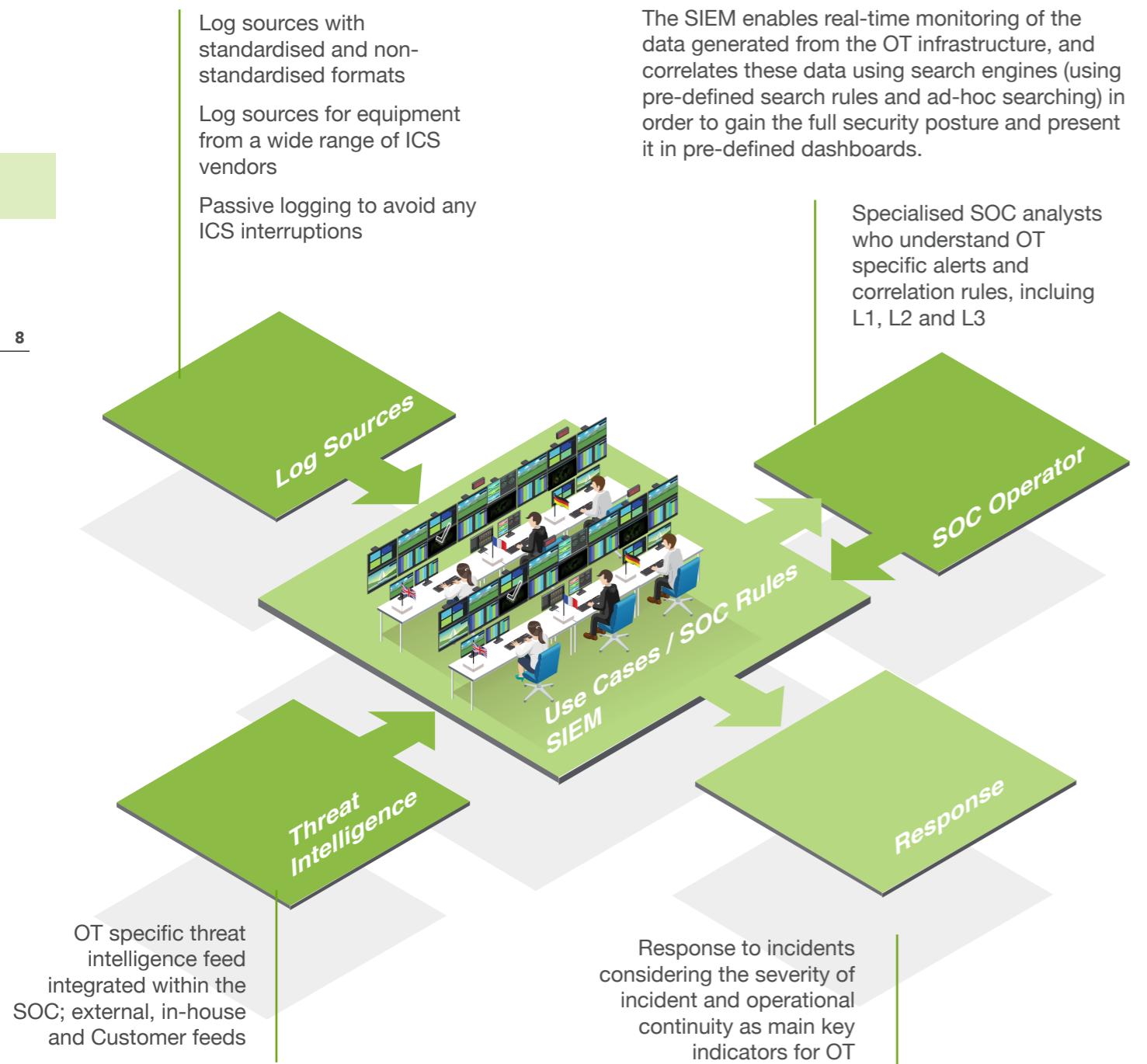
- Asset Discovery and Analysis add-on service provides an automatic discovery for the OT assets and identifying new assets added or existing assets disconnected from the network, it also provides the system configurations for assets such as PLC firmware version, OS version, etc.
- Vulnerability Analysis is a service for managing all vulnerabilities (tracking and scoring vulnerabilities) associated with the discovered assets and provide reports and recommendations for remediations.
- Intrusion Prevention and Detection Systems (IPS/IDS) is the advanced service that gives the possibility to detect all anomalies, malicious activities, human errors, and outsider cyber-attacks.
- Malware Detection provides end-point protection from malware and Zero-day threats, and host-based intrusion prevention against new vulnerabilities.

Cyber-on-Demand

These are consultancy services that help customers to define and build security managed services and to provide support during SOC operations.

- SOC Building service is a consulting service to help customers to setup a SOC programme, define requirements and SOC scope such as operation hours, SOC tools, etc. then develop structure and determine the delivery method for the SOC (either in-house or outsourced). This can also be applied to the enablement of an OT service on an existing IT SOC.
- SOC Use Cases consultancy service is to identify all possible and applicable use cases based on OT infrastructure risks and operational requirements.
- Risk Assessment service to assess OT threats and vulnerabilities, identify and score all risks, and then develop remediations roadmap.
- Incident Response service support customers in the case of emergency response, preservation of evidence, triage and investigation assistance.
- Other OT Consulting services such as threat intelligence, Active Directory audit, awareness sessions and demonstrations, and other kinds of reports related to OT security.

SOC 4.0 Features



Security information and event management (SIEM)

The SIEM is the foundation of SOC 4.0 as it acts as the main data platform, as illustrated in **Figure 2**. It collects all data and security logs from multiple data sources to gain wide visibility and provide a comprehensive insight about the OT security posture and enable fast detection and response to all cyber-attacks. The SIEM automates and orchestrates all security tools such as asset discovery and vulnerability scanning tools within SOC 4.0.

The SIEM enables real-time monitoring of the data generated from the OT infrastructure, and correlates these data using search engines (using pre-defined search rules and ad-hoc searching) in order to gain the full security posture and present it in pre-defined dashboards.

Specialised SOC analysts who understand OT specific alerts and correlation rules, including L1, L2 and L3

Data Onboarding

The objective of data collection and onboarding is to make sure that the right information flows to the right places at the right time. This is crucial to the success of SOC 4.0 as it enables the detection of threats and provides the situational awareness for SOC analysts to react to and investigate incidents with minimal delay.

Data onboarding for the OT infrastructure is considered to be a challenging task, not only because it requires considerable time, cost, effort and knowledge, but also since it requires the collection of the data and security logs passively and without interruption to the operations of the plant or the factory. Airbus understands these challenges and provides practical solutions based on OT infrastructure, ICS system architecture and existing technologies (security solutions) in use. Different solutions can be used to satisfy and achieve this mission such as OT sensor solutions, remote management tools, syslog machine collector, Log receivers, and many others.

Once security logs and data sets are collected, it will be onboarded to Airbus SOC 4.0 via site-to-site secure VPN that is protected using certificates exchanged in advance. Airbus could also utilise any Identity and Access Management (IDAM)/Privileged Access Management (PAM) solution or multi-factor authentication technologies already in use by the customer.

Log Management

All onboarded data will be logged at Airbus SOC 4.0 - the standard policy will ensure retention of logs in their original format for a pre-determined duration e.g. 12 months. However, these logs can be stored for a period defined by the customer. Analysts and security operations team can access these logs for security investigations and incident response. SOC 4.0 also has redundancy of data storage capability, which provides high data availability, data recovery and automatic failover.



SOC 4.0 Use Cases (UC) Developments

SOC use cases, or the SOC rules development activity, is a critical step in SOC building, because it defines the correlations and detections SOC rules. SOC UC development follows a risk-based approach focused on the OT environment threat landscape, applicable risks to OT assets, attacks scenarios, and the assets or systems to be monitored within the SOC.

Developing and implementing SOC use cases will follow Airbus workflow and framework, which are “Planning, Analysis, Design, Implementation, Testing and Deployment” as illustrated in **Figure 3** below. Once the SOC UC is developed and tested, it will be released as an official UC with version control to the SOC 4.0 UC library: this library can then be utilised with new customers to accelerate their SOC implementation. If an existing UC needs to be modified for specific customer demands, then it should follow a change management process.



Figure 3: Airbus SOC 4.0 Use Cases Development phases



SOC 4.0 Features



Asset Inventory and Management

Automatic asset discovery and analysis is one of the most important tasks for OT security management. Within this service, SOC 4.0 will automatically provide a passive discovery for all networks and identify the connected real time assets, asset configurations and IT/OT communication protocols. A comprehensive report will be generated to demonstrate up-to-date assets and categorise them based on vendors, hierarchy levels (Purdue Model), or utilised protocols.

Airbus SOC 4.0 is a flexible and modular solution, with the capability to roll out a new asset discovery solution on the OT infrastructure when needed, or alternatively to integrate and interface with existing asset discovery solutions used by the customer.

A FLEXIBLE AND MODULAR SOLUTION

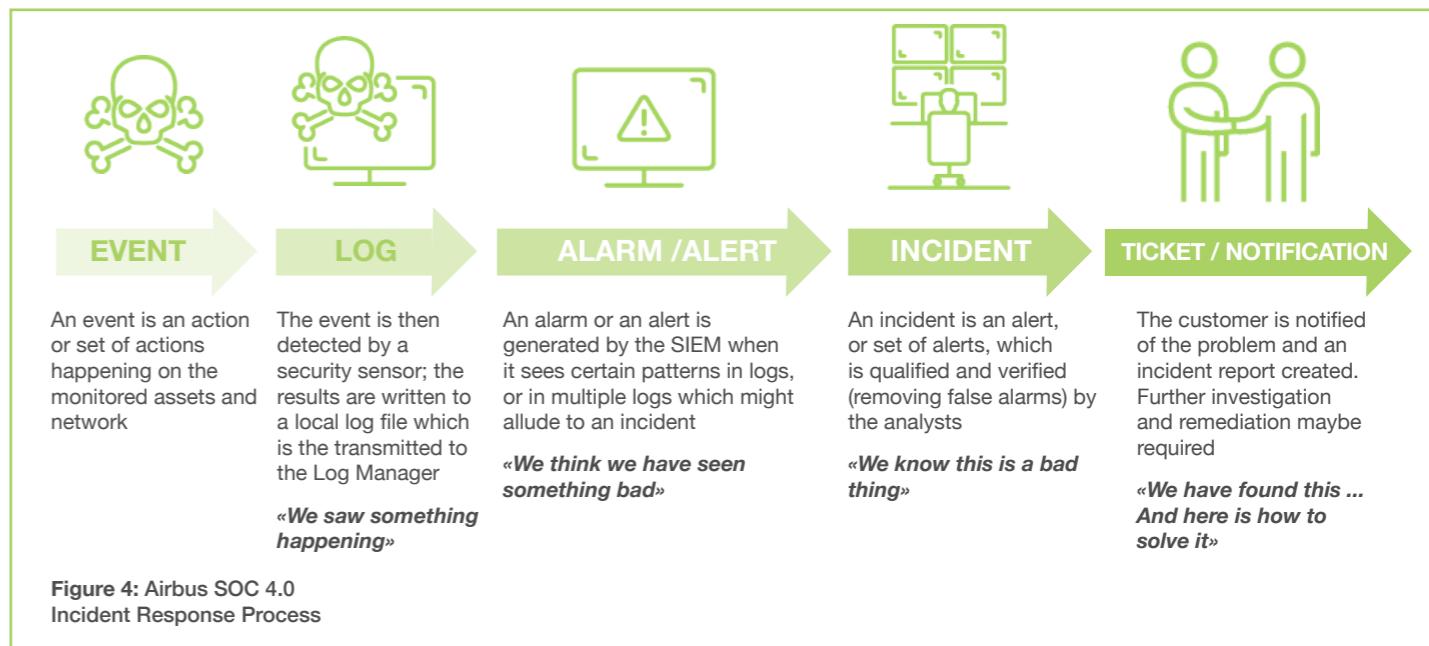
Vulnerability Management and Assessment (VAS)

Another add-on service for SOC 4.0 which empowers Airbus' solution to perform passive vulnerability scanning for the IT/OT infrastructure, and gives the ability to identify vulnerabilities inherited in all systems that can be exploited by adversaries. Our SOC analysts will monitor the outputs from scheduled and on-demand scans in order to identify potential vulnerabilities within the plant or the factory.

Vulnerability management follows a systematic approach starting from discovery, analysis, and prioritisation to remediation. Analysts within SOC 4.0 use network modelling and attack simulations to find exposed vulnerabilities. Scheduled reports will provide a summary of the vulnerability scanning activities and detail whether the vulnerabilities identified pose a specific risk to customer infrastructure. In addition, reports will provide an overview of the recommended remediation actions required to patch and mitigate the identified vulnerability.

Incident Response and Management

SOC 4.0 MSS includes Incident Response and Management within the Protective Monitoring core service. In case of an incident, the security operations team will initiate an incident response based on a systematic workflow. The primary objective of incident management is to notify the customer as quickly as possible about that incident. Airbus incident response process is based on best practices following the SANS Incident Response (IR) methodology as shown in **Figure 4**.



Upon detection, Level 1 SOC analysts will firstly qualify and verify the alert: if the alert is found to be a 'false positive' the analyst will tune the system to ignore it. If not, the alert will be promoted to an incident and a ticket will be created to record the relevant information and the customer incident response team will be notified. The verified new incidents will then be passed to Level 2 SOC analyst to establish the scope of the possible attacks. The analyst is supported by the SOC knowledge base, which collates the latest external threat feeds, along with the supplier and control vendor bespoke cyber intelligence feeds. Depending on the complexity

of the incident it may subsequently be passed to a Level 3 SOC analyst for further investigation to qualify the nature of the threat. Upon completion of analysis by Level 2 or both Level 2 and Level 3 teams, appropriate recommendations will be provided to the customer.

Due to the nature of OT systems and the consequences of their disruption on running processes, the resolution for security incidents is usually carried out by the customer's asset owner. However, support can be provided as an additional service to the customer by the Airbus CSIRT team.



SOC 4.0 Characteristics

12

Cyber Threat Intelligence

13

Threat intelligence (TI) is a fundamental component of the Airbus SOC 4.0 MSS and is used daily by the security operations team in conjunction with the other security tools to improve detection and guide investigations. Threat sources include the following:

- External threat sources providers, which deliver Threat Intelligence Contexts and Actions focused on the OT industry or vertical.
- In-house Threat Intelligence generated by Airbus experts from open and closed Threat Intelligence sources.
- Customer-generated sources from the previous event triage results.

Selecting a Threat Intelligence source for OT should have specific selection criteria that meet customer and ICS sector demands. OT Threat Intelligence should have meaningful Contexts and Actions to the specific OT industry or vertical. TI Contexts describe the threat

and demonstrate its impact on the ICS and the affected industry vertical and geographical coverage. OT Threat Intelligence Actions describe the recommended technical and administrative steps that need to be taken to enable hunting and detection for specific threats; i.e. the threats that are presented by the TI feeds.

TI feeds include automatic indicators such as IP addresses, domains, URLs etc., alongside associated context. They also inform SOC analysts of the Tactics, Techniques and Procedures (TTPs) used by adversaries known to target a specific industry or vertical.

Within SOC 4.0, Threat Intelligence is provided in the form of TI contexts and live feeds that are uploaded into the SIEM. Threat Intelligence feeds are used to develop correlation rules, which in turn, feed alerts. SOC 4.0 SIEM has a trace back function, which automatically looks back through historical data for Indicators of Compromise each time a threat source is added. The alerts are reported in standard reports and dashboards.

SOC Team

| Role | Profile | Description |
|------|------------------------------------|--|
| | Service Desk | Call Centre Act as single point of contact for the SLA, responsible for recording security incidents and initiating service and change requests |
| | Level 1 Security Analyst | Real Time Monitoring and Triage specialists Triage and short-turn analysis of real time data feeds and events (such as system logs and alerts) for potential intrusions. All suspected incidents are prioritised and escalated to Level 2 analysts for further study |
| | Level 2 Security Analyst | Analyst Review and analyse potential intrusions and tips forwarded from L1 analysts. It must be completed in a specific time span to support a relevant and effective response. This capability will usually involve analysis leveraging various data artifacts to determine the who, what, when, where, and why of an attack (or intrusion)—its extent, artefacts how to limit damage, and how to recover. Analysts document the details of this analysis with a recommendation for further actions |
| | Level 3 Security Analyst | Incident Responder Prolonged, in-depth analysis of the affected constituents to gather further information about an incident, understand its significance, assess mission impact, and coordinating response actions and incident reporting. Gathering and storing forensic artifacts related to an incident in a manner that supports its use in legal proceedings. Depending on jurisdiction, this may involve handling media while documenting chain of custody, ensuring secure storage, and supporting verifiable bit-by-bit copies of evidence. Interrogation of consistency hosts for vulnerability status, usually focusing on each system's patch level and security compliance, typically through automated, distributed tools. Care and feeding of sensor platforms owned and operated by the SOC: IDS, IPS, SIEM, and so forth. Tuning these systems, minimising false positive, and maintaining up/down health status of sensors and data feeds. |
| | Cyber Threat Analyst | Intel and Trending Collection, consumption, analysis and redistribution of cyber intelligence reports, cyber intrusion reports, and news related to OT security, covering new threats, vulnerabilities, products, and research. Primary authorship of new cyber intelligence reporting, such as threat notices or high-lights, based on primary research performed by the SOC. Extracting data from cyber intel and synthesising it into new signatures, content, and understanding of adversary TTPs, thereby evolving monitoring operations (e.g., new signatures or SIEM content). Holistic estimation of threats posed by various actors against the constituency, its enclaves, or lines of business, within the cyber realm. This will include leveraging existing resources such as cyber intel feeds and trending, along with the OT infrastructure architecture and vulnerability status, often performed in coordination with other cybersecurity stakeholders. |
| | SOC Manager | Operations and Management Supervises the activity of the SOC team, role mapping and resource planning, skills matrix and training planning. Manages the escalation process and reviews incident reports. Ensure compliance to SLA and achieve operational objectives. Coordinating with other stakeholders, ensure SOC performance and communicates the value of security operations to business leaders. |
| | Cyber Security Architect | Cyber Engineering Market research, product evaluation, prototyping, engineering, integration, deployment, and upgrades of SOC equipment, principally based on free or open source software (FOSS) or commercial off-the-shelf (COTS) technologies. Includes budgeting, acquisition, and regular re-capitalisation of SOC systems. Maintain a keen eye on a changing threat environment, bringing new capabilities to bear in a matter of weeks or months, in accordance with the demands of the mission. Testing the security features of point products being acquired by constituency members. Analogous to miniature vulnerability assessments of one or a few hosts, this testing allows in-depth analysis of a product's strengths and weaknesses from a security perspective. This may involve "in-house" testing of products rather than remote assessment of production or pre-production systems. |
| | Cyber on Demand Consultants | Audit and Risk Providing cybersecurity advice to constituents; |
| | OT Security Consultants | Assessments supporting new system design, business continuity, and disaster recovery planning; cybersecurity policy; secure configuration guides; and other efforts. Regular, repeatable repackaging and redistribution of the SOC's knowledge of constituency assets, networks, threats, incidents, and vulnerabilities to constituents. |

What can SOC 4.0 monitor

Depending on the OT/ICS architecture and assets types, different collection methods and techniques can be introduced. Below **Figure 5** shows the reference Purdue Model for ICS infrastructure with different possible data sources for each layer.

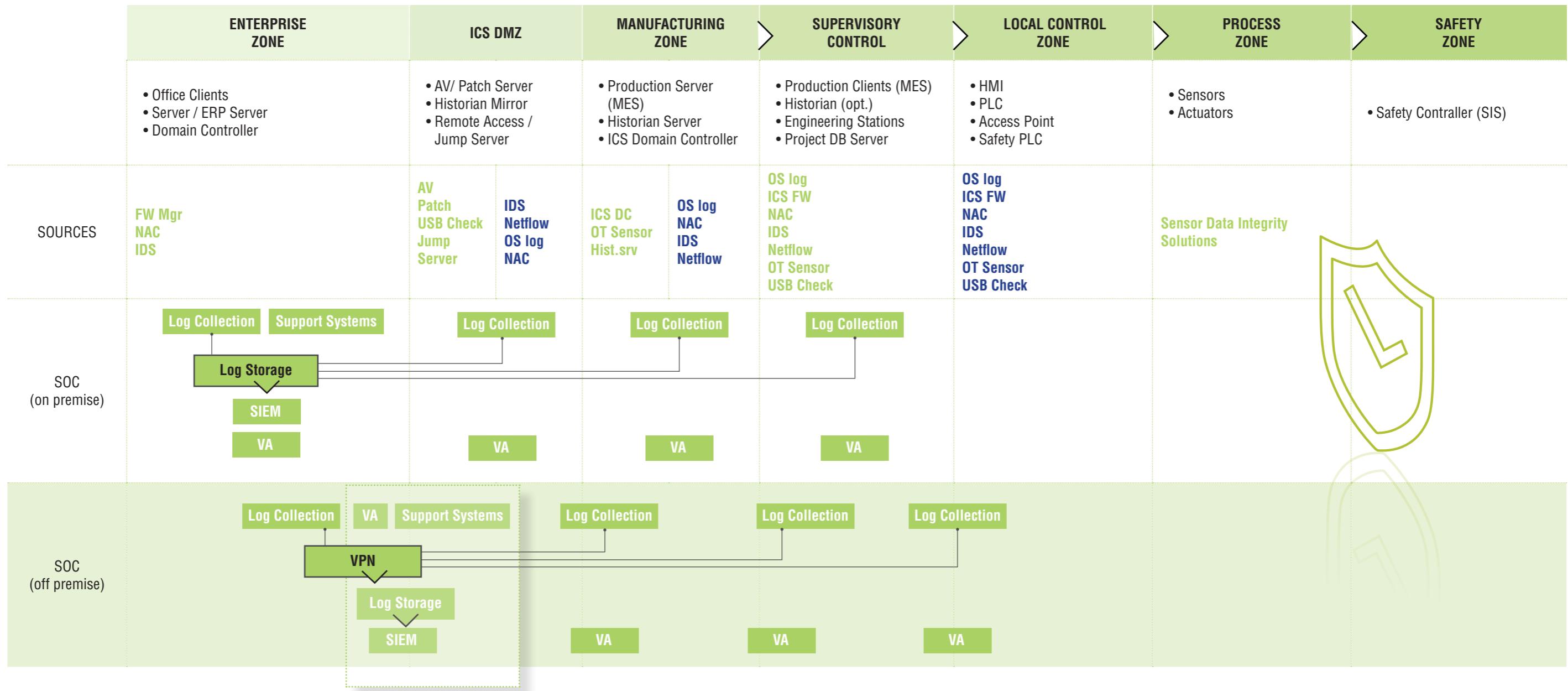


Figure 5: Purdue Model and possible data sources for SOC 4.0 monitoring

Based on the Purdue Model example, the OT infrastructure could have different asset types such as PLC, HMI, Engineering workstation, SCADA servers, Historian, MES and ERP servers, AV/Patch server, Domain Controller, Jump server, OPC server, and other assets. Most of the assets in Level 2 and upwards are PC-based assets, Firewalls, Switches and Routers. The data collection will mainly focus on collecting logs from the operating system's security events, system error logs,

logs from databases such as Active Directory, SQL, AV/WL solution database, etc., syslogs from firewalls and switches, and logs from running Applications such as Network Performance and Management Applications, Remote Access Applications, and others.

On the other hand, assets in Level 1 are mostly consisting of embedded devices such as PLC and HMI. Therefore, the data collection techniques will be based on monitoring

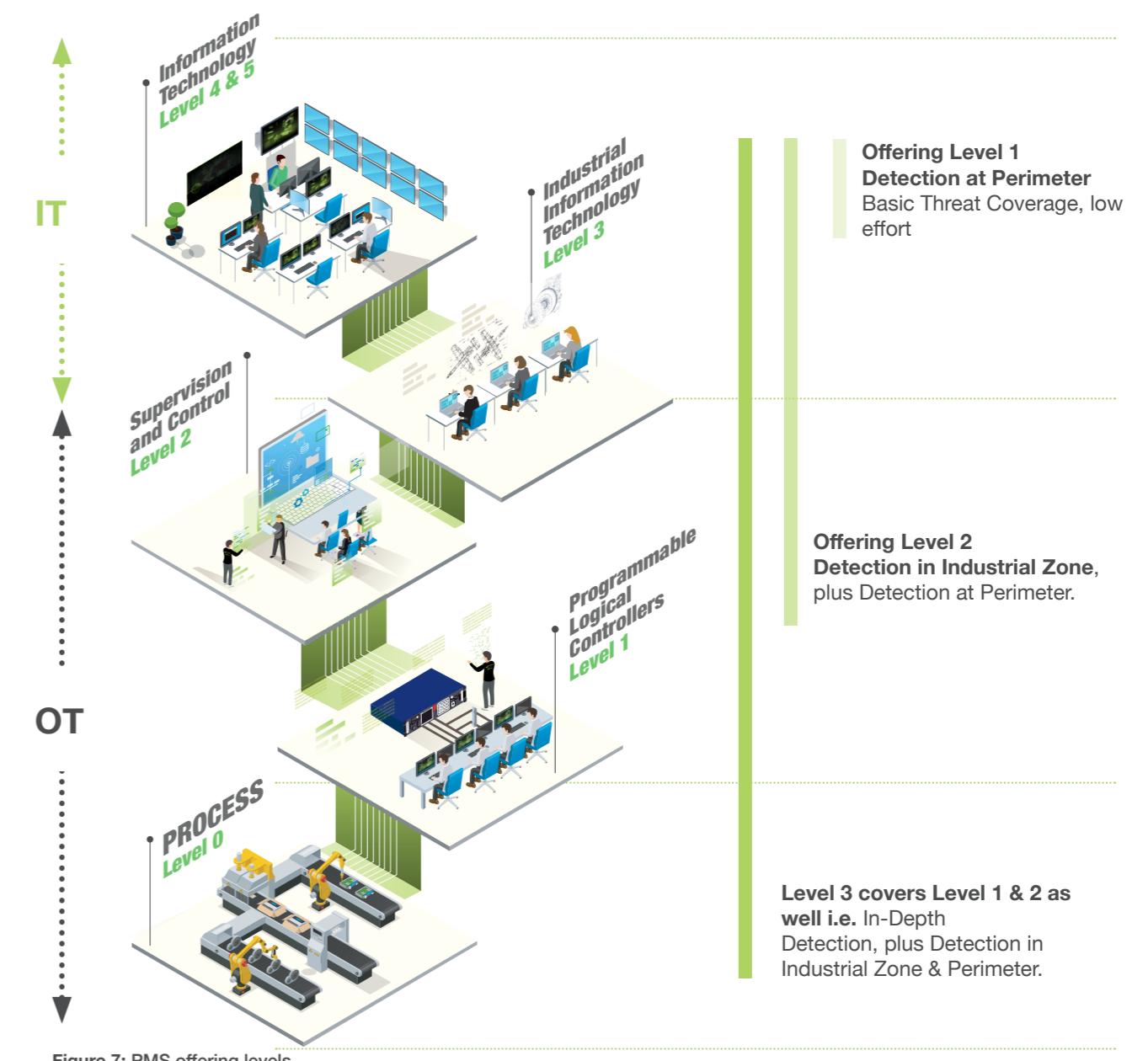
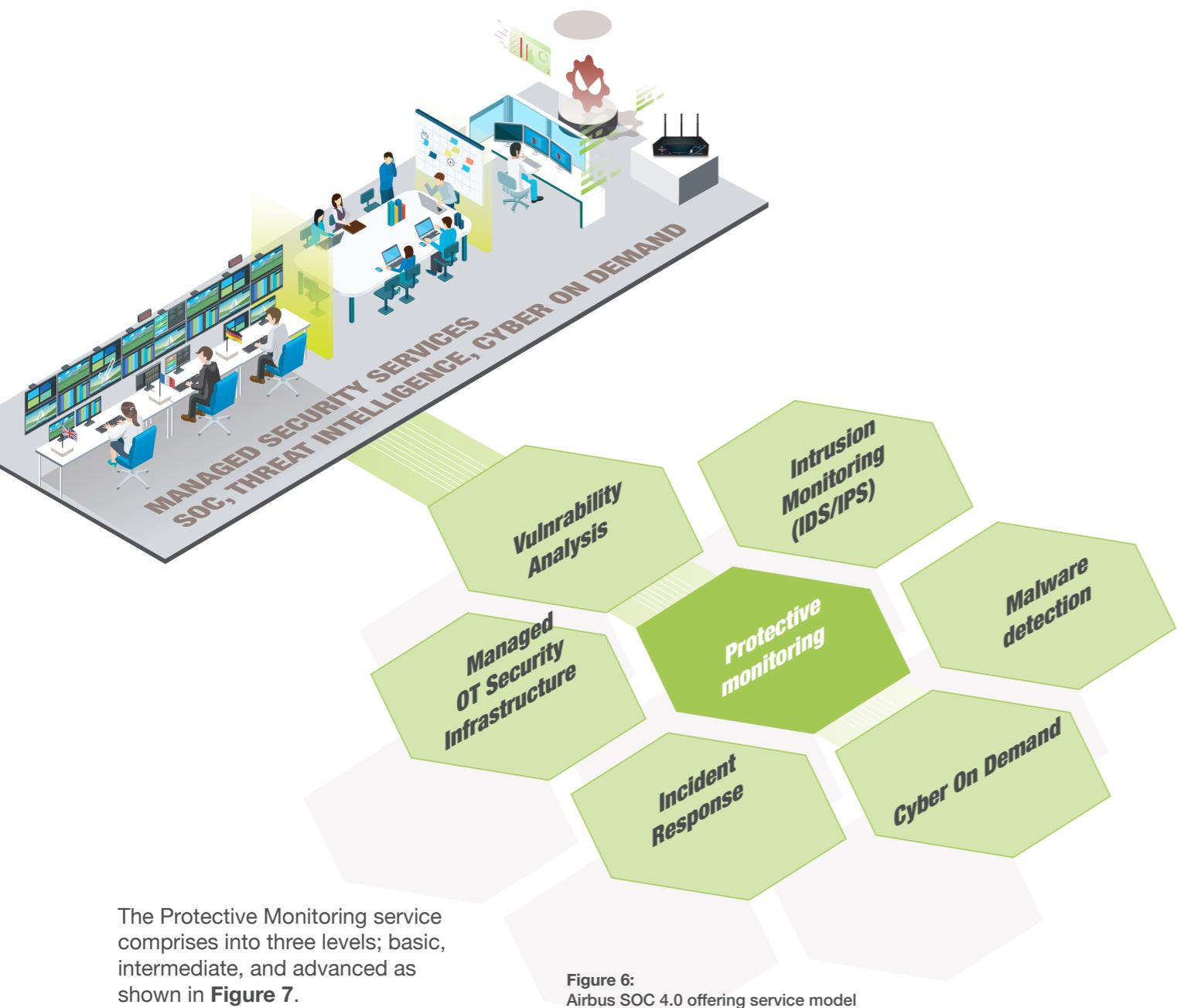
passively the network traffic generated by these devices in order to capture the asset behaviour, monitor some process values, and monitor the read/write commands to PLC, HMI, VFD or other IED. However, Level 1 and 2 assets use industrial protocols, which are different from the traditional IT protocols. Hence, SOC 4.0 has the capability to perform Deep Packet Inspection for these industrial protocols such as DNP3, MODBUS, S7 comm, EtherNet/IP and many others. SOC 4.0 can monitor

different control system vendors such as Siemens, Rockwell, Honeywell, Emerson, ABB, Yokogawa, Schneider Electric, GE, and Mitsubishi, among many others, and perform Machine Learning techniques to baseline the ICS assets and capture the deviations, critical changes or malicious activities.

Service model description

SOC 4.0 offering model

SOC 4.0 is a modular Managed Security Service that fits small, medium and large organisations/OT infrastructures. Figure 6 illustrates the offering model for SOC 4.0 MSS: the Protective Monitoring Service (PMS) is the core service for SOC 4.0, where all other services are options that can be added to complement the PMS. Depending on the scope of the SOC and the requirements, SOC 4.0 offers the flexibility to add these services at any time of the cyber security programme lifecycle.



| | Offering Level 1: Detection at Perimeter | Offering Level 2: Detection in Industrial Zone | Offering Level 3: In-Depth Detection |
|---------------------------------------|---|---|---|
| Benefits | Generic and high-level cybersecurity monitoring of your OT systems | Adapted and granular cybersecurity monitoring of your OT systems | Tailored and very granular cybersecurity monitoring of your OT systems |
| Threat coverage | Basic Common attacks (such as virus infection) should be detected | Intermediate Common and some dedicated attacks (such as DoS) should be detected | Enhanced Common up to complex and targeted attacks (such as APTs) should be detected |
| Deployment effort: Data collection | Perimetric systems (Firewall logs & Antivirus management server logs) | + Supervision systems (Domain Controller, Historians, Engineering workstation, SCADA Servers, Industrial IHM) | + Full command control network flow (OT sensors, workstation seal, specific firewalling & zoning with industrial protocol DPI...) |
| Deployment effort: SOC Use Cases | Standard OT use cases (based on system monitoring: system alarm, SNMP, etc. with little SOC process adaptation) | Specific OT uses cases (based on system monitoring and OT sensors) | Highly tailored OT uses cases (based on system monitoring, OT sensors and operational processes and behaviors) |

Service model description



Service Level Management

The Service Level Management shall manage the Service Level Agreement (SLA) with the customer and ensure that services are designed to meet the agreed Service Level Targets (SLT) and Key Performance Indicators (KPIs).

The Service Level Management function:

- Defines documents, agrees, monitors, measures, reports and reviews the level of service provided to the customer.
- Ensures that the customer has a clear and unambiguous definition and expectation of the level of service to be delivered.
- Identifies those interfaces which constitute links in the service delivery chain.

- Provides and improves the relationship and communication between the supplier Service function and the customer.
- Monitors and improves customer satisfaction through the quality of service delivered.

Service Level Targets measures Airbus performance to deliver SOC 4.0 MSS, they include SOC operating hours and incident notification to customer team. Key Performance Indicators measure SOC 4.0 MSS in terms of availability, efficiency and quality.

SOC 4.0 service hours

SOC 4.0 MSS is operating in three different patterns as per below table;

| | Profile | Description | Operating Pattern |
|---|------------------|--|-------------------|
| 1 | Standard | Five days a week Monday to Friday, from 9:00 until 17:00 | 8x5 |
| 2 | Extended | Daily from 09:00 until 17:00 including holidays | 8x7 |
| 3 | Around the clock | Daily with 24 hours service for all 365 days of the year | 24x7 |

Customers will have the ability to amend their Service Hours coverage; for example, if they wish for their Service Hours coverage to move to 12:00 to 16:00; this can be actioned. However, the request will need to be raised to Airbus with a defined lead time.

Why Airbus CyberSecurity



Our SOC experience

Airbus CyberSecurity provides dedicated Cyber Security solutions to protect governments, national agencies, critical infrastructure, manufacturing and commercial organisations around the world from increasingly sophisticated cyber threats through a range of protective and responsive services.

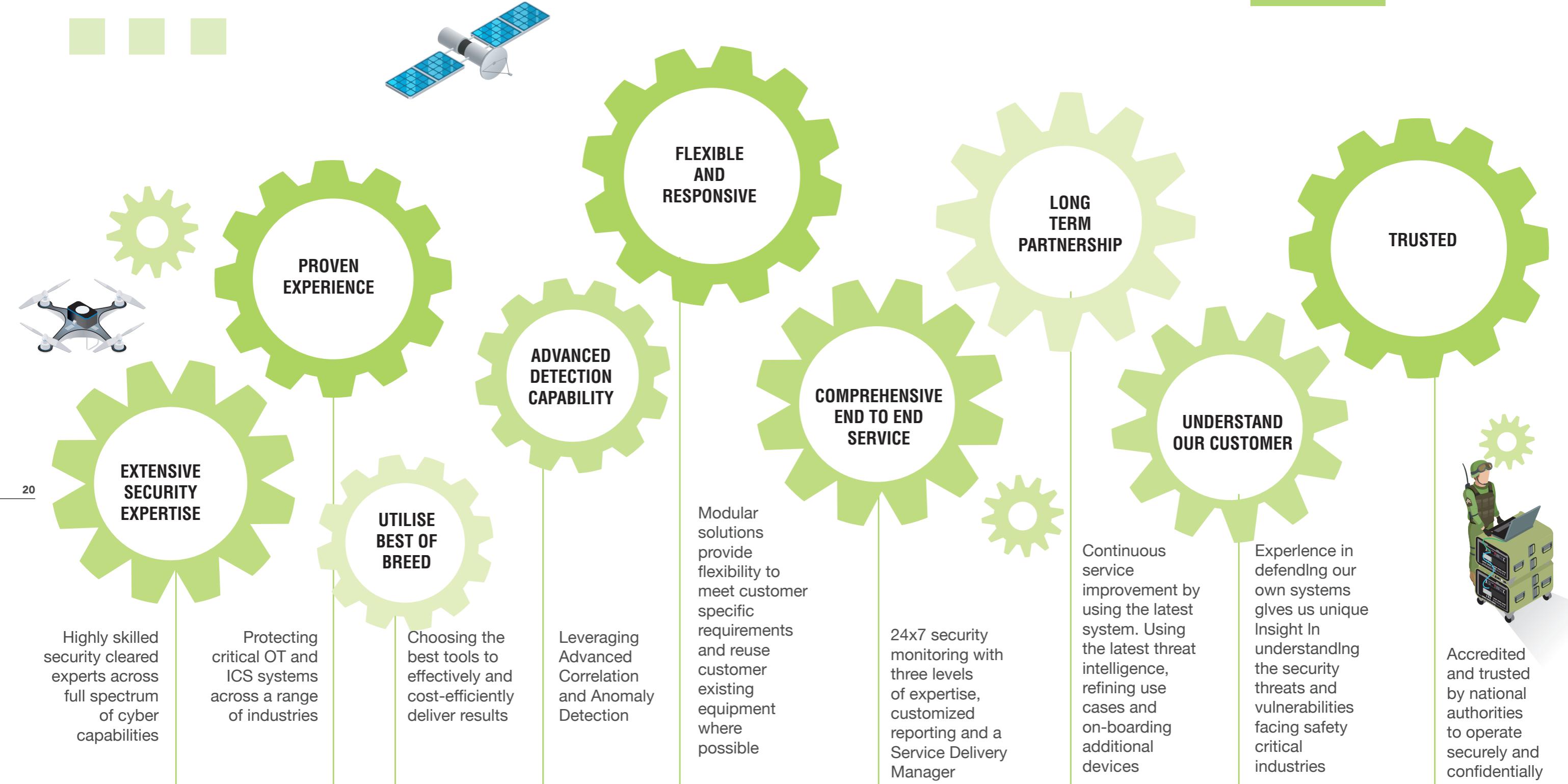
Our Cybersecurity solutions were developed to protect the Airbus business from cyber-attacks. Over a number of years, our methodologies, tools and processes have been continuously refined to protect us against the evolving cyber threat scenario. The same highly experienced individuals and technologies used to defend Airbus systems are made available to our commercial and Government clients, in order to ensure that their systems and networks are as well protected as those of Airbus.

Based on our heritage, within the aviation, maritime, defence and space sectors, Airbus is well equipped to operate in a highly regulated, global and complex business environment. Operating on a 24/7 basis, our Cyber Security solutions can be adapted to the customer's specific requirements. Airbus continues to invest heavily in developing our Cybersecurity solutions to ensure that we provide the best defence possible against current and future cyber threats.

Our ISO/IEC 27001 certified SOC services deliver highly accurate, near real-time detection and alerting against the world's most sophisticated threat actors and provides a global view across the business, all from a single management platform. This, combined with our powerful global Threat Intelligence (TI) and in-house developed malware analysis tools, means we can accurately and quickly identify even the most advanced cyber-attacks.

| Airbus CyberSecurity | | |
|--|---|---|
| Best of breed technologies configured to best meet our customers' specific requirements | Protecting critical IT and ICS systems across a range of industries | Highly skilled security cleared experts across full spectrum of cyber capabilities |
| 24*7 security monitoring with three levels of expertise, customised reporting and a Service Delivery Manager | Bespoke use cases and threat intelligence to detect cyber-attacks at all stages of the cyber kill chain enabling earlier identification and informed mitigation actions | Modular solutions provide flexibility to meet customer specific requirements and reuse customer existing equipment where possible |
| Accredited and trusted by national authorities to operate securely and confidentially | Experience in defending our own systems gives us unique insight in understanding the security threats and vulnerabilities facing safety critical industries | Continual service improvement by tuning system, using the latest threat intelligence, refining use cases and on-boarding additional devices |

What makes us different





Contact us



FOR MORE INFORMATION: Airbus CyberSecurity

FRANCE

Metapole 1, boulevard Jean Moulin /
CS 40001 / 78996 Elancourt Cedex/
France

GERMANY

Willy-Messerschmitt-Str. 1 /
82024 Taufkirchen / Germany

UNITED KINGDOM

Quadrant House / Celtic Springs
/ Coedkernew / South Wales
NP10 8FZ / United Kingdom

UNITED ARAB EMIRATES

Etihad Towers T3 / Corniche Road,
19th floor / P.O.Box: 72186 /
Abu Dhabi /
United Arab Emirates

contact.cybersecurity@airbus.com
www.airbus-cyber-security.com