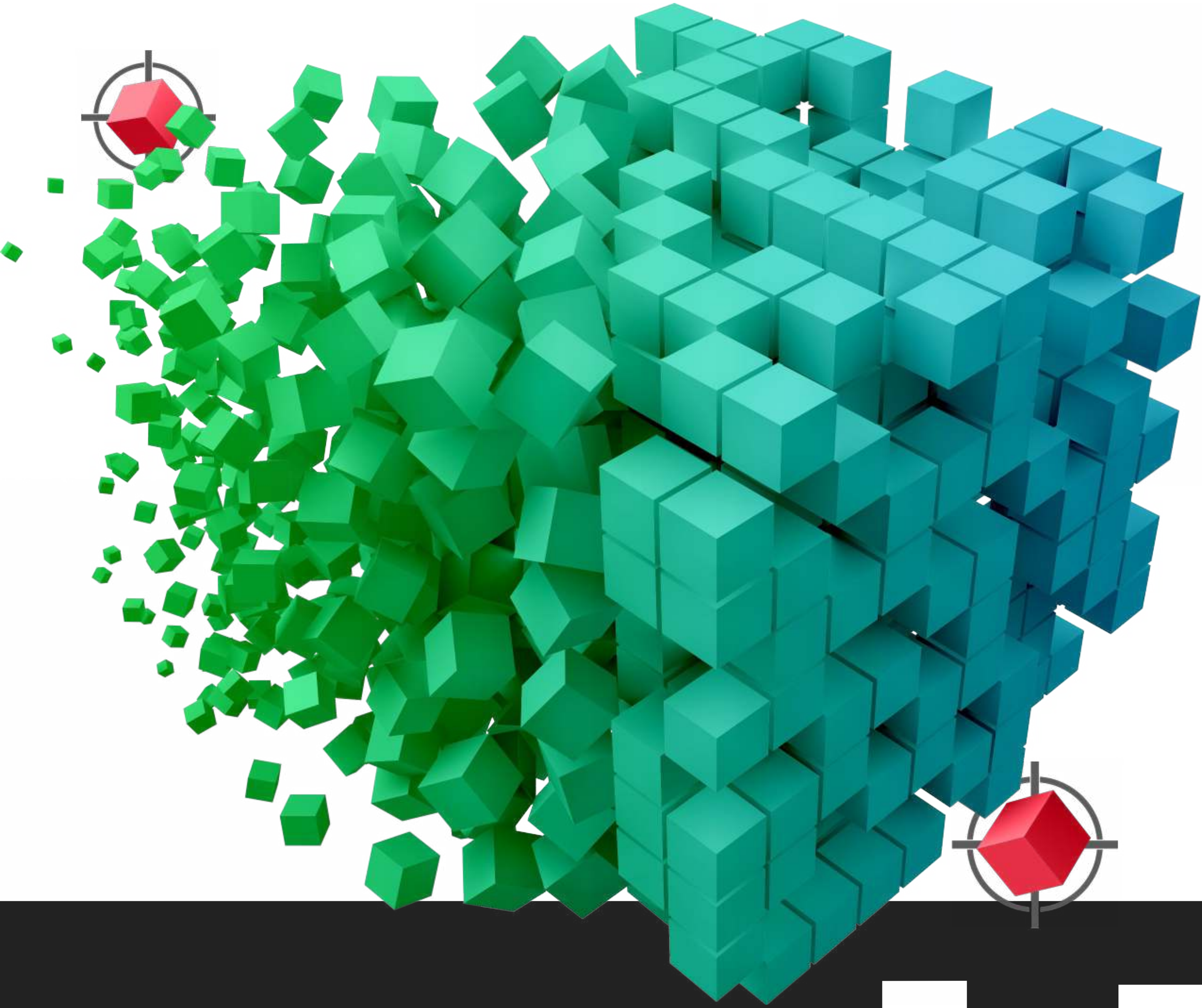
INSIGHTCYBER™

InsightCyber.com



A 26-point implementation model for the InsightCyber service

The InsightCyber Blueprint for Success

The InsightCyber security service is a groundbreaking AI-powered solution to help organizations protect Operational Technology (OT) environments, corporate networks, and OT assets (including IoT and IIoT devices) against a wide range of cyber threats. The service delivers a range of benefits including visibility into assets, monitoring and detection of anomalies, playbooks for response and remediation, and compliance and risk reporting.

This document provides a blueprint for the implementation of the InsightCyber service to achieve optimal ROI. The blueprint spans a set of five levels of maturity:

Maturity Level 1:

Basic

- Disjointed identification of asset and networks
- No monitoring of asset and networks
- Risk levels not identified
- Reactive / ad-hoc incident response
- Unpredictable service performance

Maturity Level 2:

Controlled

- Limited identification of assets and networks
- Minimal documentation of assets
- Reactive posture with some planning in place
- Limited level of risk identification but no monitoring
- Limited identification of service performance

Maturity Level 3:

Standardized

- Assets and networks identified and documented
- Basic monitoring of assets and networks for risk
- Stable and architected OT environment
- Foundation for OT cyber incident response
- Cyber and operational management in place

Maturity Level 4:

Optimized

- Advanced behavioral asset and network inventory management
- Advanced asset and network monitoring with risk rating, metrics, and KPI Reporting
- Operational and cyber incident response measures well aligned

Maturity Level 5:

Innovative

- Fully integrated OT Security Intelligence Center functionality
- Fully aligned operational and cyber incident response with breach detection
- Business objectives, stakeholders, and OT operations fully aligned
- OT risk management process in place

Phase 1

Discovery

Phase 2

Identification and Protection

Phase 3

Advanced Monitoring

Phase 4

Incident and Breach Response

THE 26-POINT MODEL

Working through a service provider or directly with InsightCyber, customers can choose the level of maturity that best suits their needs. In all cases, the implementation process begins with an initial phase of discovery, which reflects InsightCyber's core tenet that "you cannot protect what you cannot see." From there, customers can go much deeper—ultimately through five total phases, which together comprise 26 points of action.

Phase 1: Discovery (timeframe: 2-3 weeks)

In the Discovery phase, InsightCyber Collectors perform the capture of raw network and asset data. An essential step in this phase is the validation of assets, a process that distinguishes "confirmed" assets, which are in place as intended, from "unknown/rogue" assets, which are often undetected or misidentified. The steps in this phase are as follows:

1. **Gather initial information about the environment on the following:**

   Sites – Location of each facility in which collectors will be installed

   Zones – Specific areas within the facilities in which assets are located

   Users – Points of contact for the site and possibly specific zones

   Alerting – Process for delivering alerts and notifications to the client

2. **Install InsightCyber Collector(s) and perform burn-in and discovery of network(s) and asset(s)**

3. **Document and classify each specific asset, with the purpose of establishing:**

   Internal name

   Intended purpose

   Associated connectivity

   Location

   Type (e.g., computer system, IoT device, Raspberry Pi, PLC, etc.)

   Point(s) of contact (See item 1)

   Operational risk criticality (related to risk modeling)

4. **Validate and categorize each asset as either confirmed or unknown/rogue**

5. **Create asset groups based on customer-driven criteria, comprising factors including:**

   Site/facility and/or zones

   Functional groups (based on manufacturer, tags, asset types, etc.)

Phase 2: Identification and Protection (timeframe: 1 -2 weeks)

In the Identification and Protection phase, we introduce the configuration steps required to enable monitoring and create metrics and KPIs for reporting. Also, since asset(s) and network(s) have been identified, we can create asset tags combining different asset(s) into groups. The steps in this phase are as follows:

6. **Define complete lists of "confirmed/validated" asset(s) (metric: percentage of confirmed/unconfirmed assets)**
7. **Review network connectivity**

   Identify network segments that communicate externally

   Determine networks that are internal to the organization, connected to supply chains, and connected to external vendors (based on raw data with no custom analysis)

   Determine network segments with higher risk values (based on asset percentage of critical assets per vLAN)
8. **Review and validate network connectivity (internally and externally)**
9. **Cross-reference identified assets against known vulnerabilities and malware to identify attack patterns**
10. **Create reports on:**

    Confirmed assets

    Unknown/rogue assets

    Network connectivity

    Risk Rating report on assets
11. **Create "canned" metrics and KPIs**

Phases 1 and 2 comprise our basic offering, which provide customers a mature process for the inventory, identification, monitoring, and reporting of network(s) and asset(s).

The following two phases enable the deeper benefits of our advanced offerings, which include services from the InsightCyber Intelligence Center.

Phase 3: Advanced Monitoring

In the Advanced Monitoring phase, we introduce InsightCyber Intelligence Center operations, which provide the deeper "Data Sciences" behind our technology. The Intelligence Center delivers measurable business value through intelligent data processing and real-time data analytics, which are designed to dovetail easily with customers' existing internal operations. The steps in this phase are as follows:

12. **Develop custom configuration models for 24/7 monitoring**
13. **Implement new alerting profiles based on asset groups**
14. **Implement new alerting profiles based on networks**
15. **Implement customized reports based on risk rating and criticality along with customized KPIs and metrics**
16. **Create operational profiles for confirmed asset groups**
17. **Create new Incident Response Processes, including playbooks, based on custom alert profiles**
18. **Create alerts for rogue connectivity**
19. **Create alerts for operational anomalies**

Phase 4: Incident and Breach Response

In the Incident and Breach Response phase, the InsightCyber Intelligence Center provides 24/7 monitoring, alerting, and reporting. It also includes Incident and Breach response, which is critical to the protection of operations, revenue, and regulatory compliance. The steps in this phase are as follows:

20. **Generate custom alerts based on risk criticality and regulatory controls**

    Establish criticality of asset(s) based on physical, environmental, and/or revenue impact

    Establish risk rating of asset(s) by creating asset groups

21. **Initiate custom APIs and metrics**
22. **Initiate custom reporting based on regulatory controls**
23. **Initiate custom metrics and APIs based on regulatory controls**
24. **Initiate the Incident Response (with alerts and playbooks) with custom alerts and reporting**
25. **Test the Incident Response process with remediation planning**
26. **Initiate remediation Activity Tracking (ITIL, Ticketing, etc.)**

About InsightCyber

InsightCyber is on a mission to keep the world’s critical infrastructure, supply chains, and manufacturing operations cyber-safe, preventing attacks that can have catastrophic human and economic impact. The company’s AI-powered security service continuously monitors an industrial enterprise’s environment, providing insight and protection against a wide range of cyberthreats. To learn more, please visit https://insightcyber.com.