ABB Ability™ Cyber Security Analytics
Protect control systems against potential security threats

ABB Ability™ Cyber Security Analytics Service, identifies, classifies and helps prioritize opportunities to improve the security of your control system. Data is automatically collected and analyzed to produce actionable information that help mitigate cyber risks for your control systems.

To find security weaknesses within your system's defense, Cyber Security Analytics Service collects system data for comparison against industry best practices and standards. This not only pinpoints areas that require action, but also helps protect your control system by ensuring it has multiple layers of security.
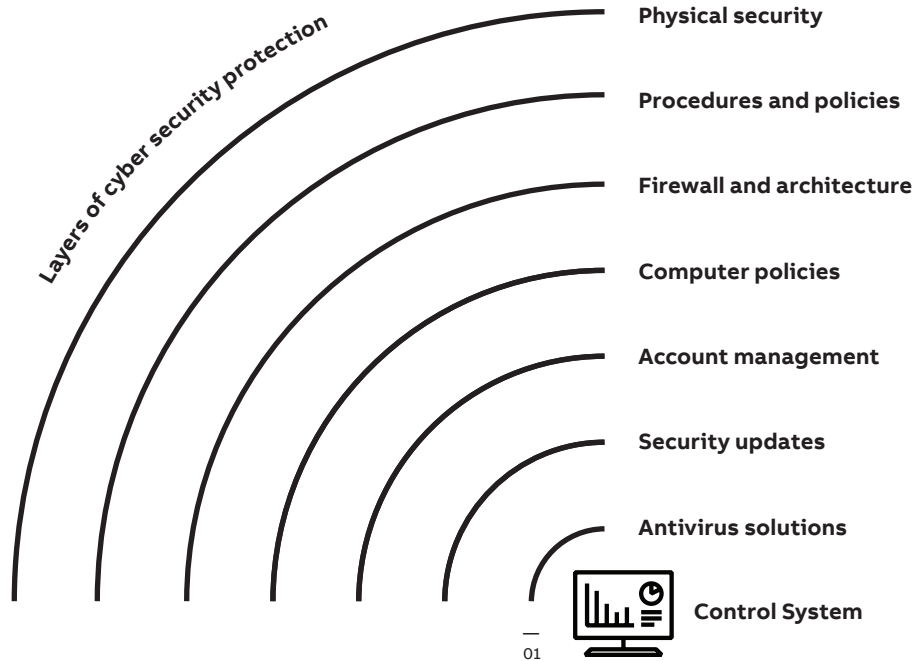
Features:
- Automatic, non-invasive data gathering with ABB's Security Logger
- Proactive analysis of Key Performance Indicators (KPIs) to detect possible security weaknesses
- On-demand analysis before or after maintenance and shutdowns
- On-site or remote access for customer personnel and ABB support
- Twice-a-year performance analysis by ABB experts identifies issues, finds trends and helps maintain elevated security
- Configurable email alerts are supplied when KPIs are outside site-specific thresholds

Benefits:
- Improves system availability through reduced security risk
- Accelerates problem solving by providing visualization and analysis of security policies and computer settings
- Configures security settings to align with site-specific needs or corporate requirements
- Identifies trends to help develop mitigation plans for the most common security weaknesses
- Reduces response time and travel expenses by providing remote access to ABB experts for troubleshooting
- Ensures continuous improvement of your security status and compliance with your settings and procedures

Protect your control system
Scheduled or on-demand monitoring of KPIs

Layers of cyber security protection

- Physical security
- Procedures and policies
- Firewall and architecture
- Computer policies
- Account management
- Security updates
- Antivirus solutions

Control System

—
01

—
01 ABB uses the Defense in Depth strategy to ensure you have multiple layers of protection.

Scheduled monitoring and analysis to quickly identify vulnerabilities
ABB Cyber Security Analytics Service is accessed through a service delivery platform conveniently deployed on any control system at your location. You can view data gathered through a web-based window (channel) that is easily accessible by customer or ABB personnel. With ABB Cyber Security Analytics Service, you get the advantage of scheduled or on-demand security monitoring and data analysis to greatly reduce the time and effort needed to uncover weaknesses within your security procedures, system policies and computer settings. Data is classified based on KPIs to provide a list of problematic items that are then prioritized based on severity, criticality and/or financial impact. Monthly profile updates are provided to ensure security data are assessed against the latest security settings. This analysis leads to informed, responsive decision making by your team, who can regularly and more easily ensure there are multiple layers of protection in place (Figure 1).

More accurate troubleshooting with configurable KPIs
ABB Cyber Security Analytics Service analyzes the following KPIs to accelerate problem solving:
- **Procedures and protocols:** Availability of, and agreement to, written instruction and policies.
- **Security policies:** Compliance with policies implemented on the system, enforced from a central server or implemented on an individual computer.
- **Computer settings:** Assurance that the appropriate settings and applications reside on each computer in the system.

View, analyze and receive alerts on security status
Cyber Security Analytics Service components
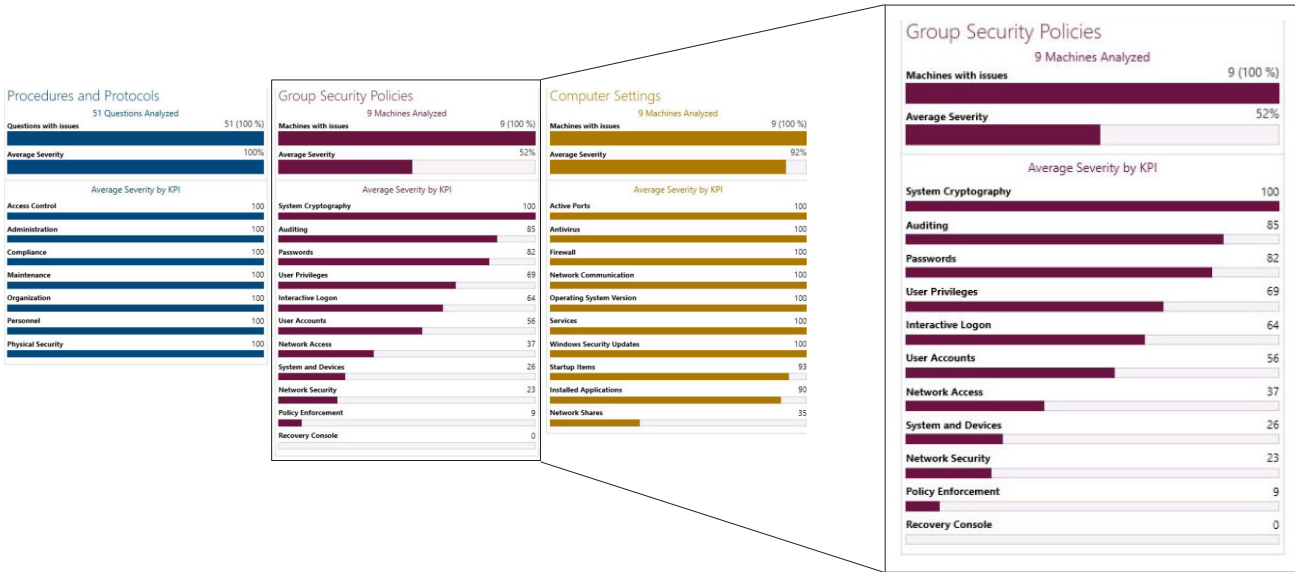
—
02 Through the Cyber Security Analytics Service, you can access three different views for each of your KPIs. The above example shows the KPI analysis view for security policies. The display only shows the KPIs that are outside their threshold and prioritizes them—the bigger the bar line, the greater the need to address the KPI.

—
03 Included in your service agreement are periodic performance reports, which point to actions that will help prevent potential problems.

Simplified view of data and analysis
Access to and visualization of KPI data is provided through an interface that is easy to use and provides three separate views of the data (Figure 2):
- **Raw data** allows you and ABB service experts to view data associated with specific computers and control system settings.
- **KPI analysis** presents a summary of KPIs, ranked by severity, that shows out-of-whack system settings and missing security protection on specific computers.
- **KPI monitoring** empowers you to specify your own set of rules for KPIs and displays each occurrence that falls outside a threshold.

Critical notification when it matters most
To help prioritize issues that require immediate action, site specific rules are applied to targeted KPIs. Any KPI that tracks outside of pre-determined parameters (such as missing MS security updates) triggers an instant alert by email or SMS. This quickly identifies issues that can compromise security so you can address them as soon as they are detected.
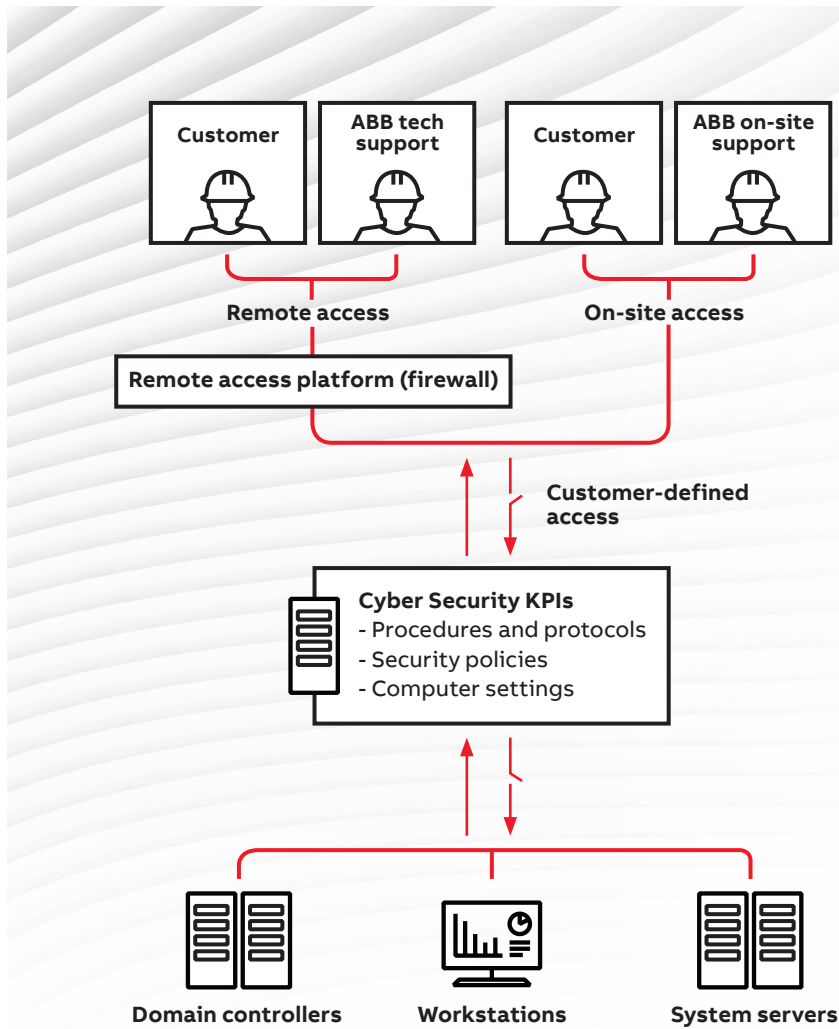
Expert analysis helps predict potential weaknesses
To ensure that your cyber security status is aligned with your security goals, ABB provides periodic performance analyses. ABB experts evaluate the status of your system's security level, determine the statistical accuracy of KPIs and find trends that predict potential vulnerabilities. The resulting performance report (Figure 3) recommends actions to improve procedures and protocols, system policies and computer settings.
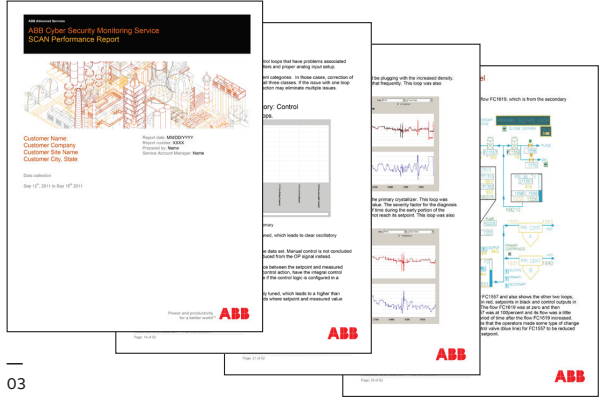
Secure connection for delivery of ABB services
On-site or remote access for customers and ABB experts

—
04 ABB's service delivery platform connects ABB services with your equipment and processes via on-site visits or remote connection. ABB Cyber Security Analytics Service connects to any control system. You control access to the data collected and stored as well as to the control network.

Customer **ABB tech support** **Customer** **ABB on-site support**

Remote access **On-site access**

Remote access platform (firewall)

Customer-defined access

Cyber Security KPIs
- Procedures and protocols
- Security policies
- Computer settings

Domain controllers **Workstations** **System servers**

—
04

—
ABB Ltd.
579 Executive Campus Drive
Westerville, OH 43082
Phone: +1 800 435 7365

3AUA000080942 REV A 06.10.2017 #14995

new.abb.com/process-automation/process-automation-service/advanced-services/abb-ability-cyber-security-services