SERVICES PROFILE

# Industrial Control System (ICS) Incident Response and Containment

Virtually all industries today rely on industrial control systems to automate, monitor, and maintain manufacturing processes and run critical operations. This service provides the investigative support and direction your organization needs during a security incident. Roadmaps for remediation are planned and overseen by world-renowned experts to ensure the incident comes to a timely close.

# Industrial Control System Cyber Security is Vital

As industrial operations become more digital, the need to provide safeguards against cyber security threats becomes increasingly critical. While they were once stand-alone systems, industrial control systems are now commonly connected to an organization's IT infrastructure and face the same cyber security threats as corporate networks. It is extremely important to protect these systems from a dynamic threat environment that could cause, to varying degrees, loss of proprietary data, IT assets, and trade secrets, and system downtime that could lead to major risks such as bodily injury, loss of life, production interruption, equipment damage, unnecessary costs, or loss of revenue.

## Value

This service provides:

- Rapid determination of whether a security-related breach has occurred or is actively occurring, allowing your organization to pivot and accelerate response time
- Mitigation of damage to your data and devices with a rapid but controlled response to an active security-related incident
- Minimized ICS production interruption or downtime
- Strategic and tactical recommendations to prevent future attacks
- Adherence to strict chain-of-custody procedures to meet legal and/or compliance requirements

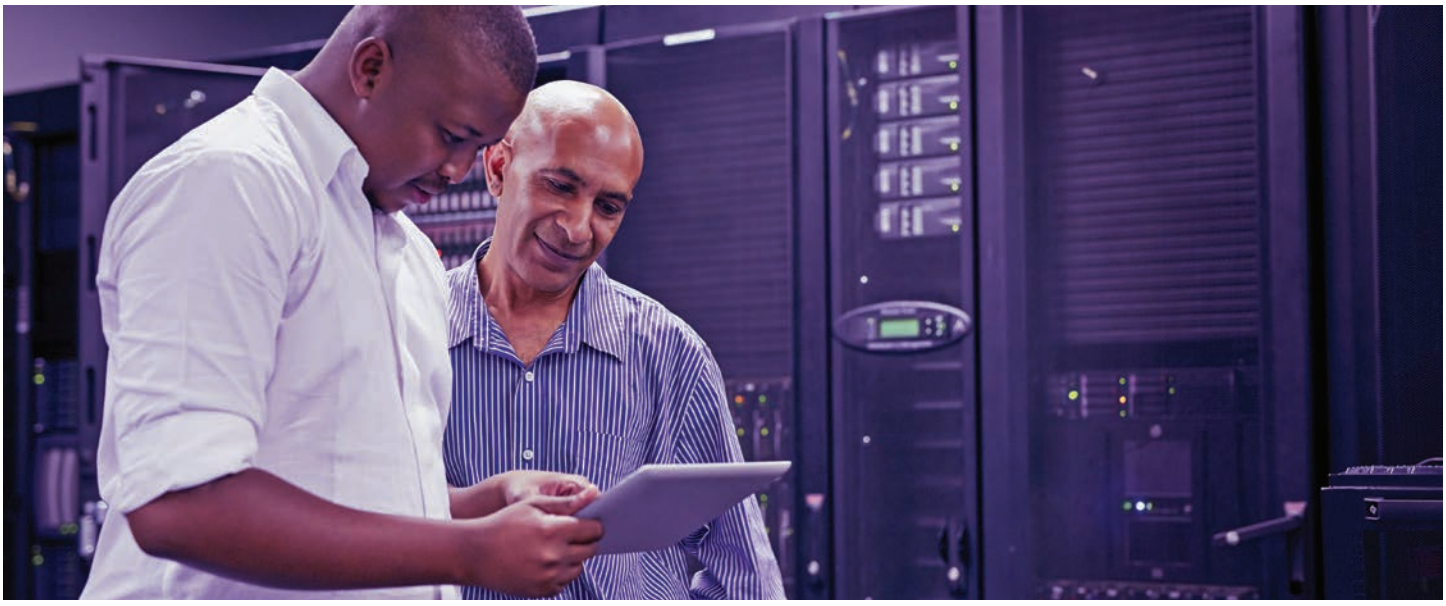
## Deliverables

Incident Response and Containment is delivered in three main phases:

1. Initial Assessment – Scripts are used to gather key data including audits, and investigative planning is performed. Audits are conducted on file and operating systems, and on network logs.
2. Targeted Assessment – Additional scripts are deployed to hosts of interest identified in Phase 1. Analyses are conducted on host memory, host disk, and network logs.
3. Forensic Assessment – A bit-by-bit disk copy and memory dump is completed to preserve data and gather information for further analysis. Forensics are done on host memory, host disk, and the network.

Additional activities may include malware analysis, containment advisement, and remediation advisement.

A report and executive presentation (on request) provide an overview of the attack path and systems impacted, the current risk state of the environment, and strategic and tactical recommendations for remediation.



# Partners – AVEVA and BlackBerry Cylance

AVEVA creates industrial software that inspires people to shape the future. Our comprehensive software portfolio makes manufacturing more productive, and assets and operations safer and more effective and sustainable. From water and energy to food and infrastructure, our solutions drive meaningful results and turn opportunities into business value.

For our ICS cyber security projects, we work in partnership with BlackBerry Cylance to enable heightened levels of security for customers leveraging our software across their industrial and infrastructure operations. This partnership means that for each project, you get the knowledge and experience of AVEVA pertaining to your AVEVA software and unique operations, as well as the ICS cyber security expertise of BlackBerry Cylance. This collaborative approach is an important differentiator and ensures you get highly relevant and targeted information about your ICS environment and how to efficiently and effectively secure it.

POWERED BY BlackBerry | CYLANCE

## About BlackBerry Cylance

- Global experts work synergistically across practice areas to deliver consistent, fast, and effective services.
- ICS experts that have a wide range of expertise covering both IT and OT capabilities, allowing them to balance the concerns of both sides and ensure that they are aligned, integrated, and consistent.
- Incorporates artificial intelligence into tools and processes to more efficiently and effectively secure the environment to prevent attacks from happening.
- Utilizes multiple techniques to collect information, assess data, provide a risk profile, recommend actions, and highlight notable strengths for an organisation.
- Techniques are designed to not impact operations in any way.

# The AVEVA Customer FIRST Program – Accelerating Your Success!

Customer FIRST is AVEVA's comprehensive, fee-based software maintenance and technical support program that helps you achieve maximum benefit from your investment in AVEVA software. It includes access to our award-winning technical support and services team to quickly resolve issues, software version upgrades and updates, and valuable services and software utilities.

In addition to the base program, we also offer a range of optional success accelerators designed to help you throughout the lifecycle stages of your application.

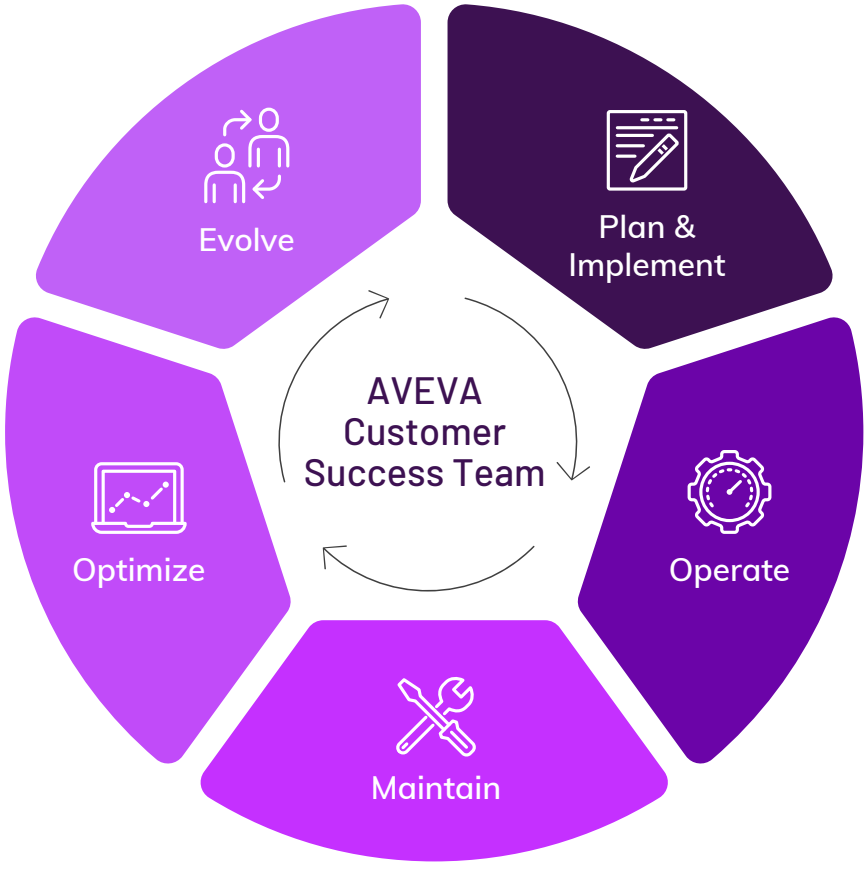
**Plan & Implement** – Engineer best practices and application architecture and improve time to value

**Operate** – Effectively run your software with expert training and drive increased engagement and adoption

**Maintain** – Efficiently maintain your software, including updates, patches, and license management

**Optimize** –Improve software performance and reliability and drive changes to address new market requirements

**Evolve** – Drive innovation through the deployment of major version upgrades, adopt new technology, and future-proof your application




To learn more, please contact your AVEVA representative or visit us online at aveva.com