EXECUTIVE SUMMARY

Siveillance Suite: Designing a cyber-intelligent security solution

We now live and operate in the era of digitalization, which means increasing interconnectedness and the ensuing requirements for convenience and efficiency. But this also means facing and mitigating the challenges that come with digitalization, namely increasing cyber risks.

Our buildings and assets need to be secure for the future. Siveillance Suite, Siemens Smart Infrastructures' extensive portfolio of physical security solutions helps you protect your valuable assets. Siveillance Suite "thinks security" by following a comprehensive approach to offering you peace of mind: a careful balance of cyber, physical, and organizational security measures for protection from the threats we face today.

Cyber challenges can be multifaceted and can range from insider threat, ransomware attacks, opportunist threat, and hacktivism to terrorist related cyber threat, all of which affect people, technology, and business continuity.

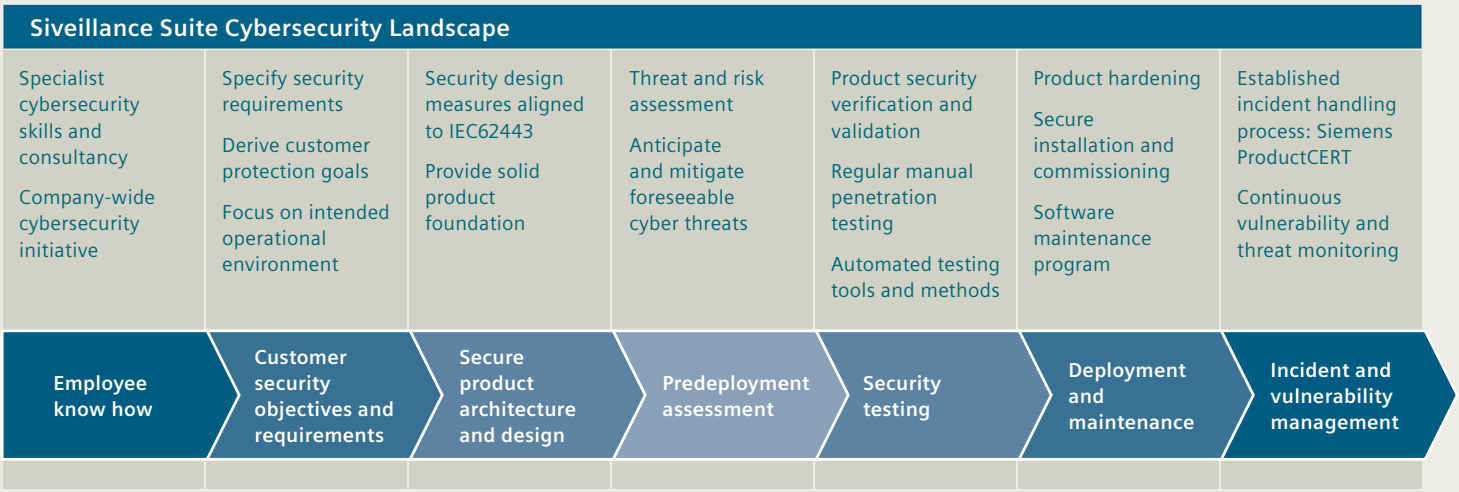
The Siveillance Suite of products from the Siemens Smart Infrastructure Division seeks to address these challenges by allowing you to retain your building security integrity in a holistic manner. In this day and age, securing digital buildings and critical infrastructure means addressing both cyber and physical security concerns, which automatically includes the people and processes behind them.

When it comes to aligning security with business need and the inevitable move toward convenience, we put a premium on cybersecurity from the outset.

A cyber-intelligent portfolio

Siemens Siveillance Suite is an extensive portfolio of physical security solutions that carefully balances cyber, physical, and organizational security. Solutions include:

- *Siveillance Control Pro:* Industrial command and control solution
- *Siveillance Control:* Physical security incident management
- *Siveillance Video:* Video surveillance/video management
- *Siveillance Video Cloud:* Cloud-based video surveillance
- *Siveillance Identity:* Manages and automates physical identities, access privileges and credentials
- *SiPass Integrated:* Access control management



Secure by Design

The Siveillance Suite is developed using our Secure by Design approach. It is our pledge to address comprehensive security in our product development process by integrating cradle-to-grave activities. For cybersecurity, this means following the "cybersecurity landscape", a pathway that engrains cybersecurity at the earliest stages of development through deployment and at every level of our organization.

The Siveillance Suite cybersecurity landscape (above) is organized into seven phases:

- **Employee know how:** Siveillance Suite has access to a global workforce with an abundance of skills, from secure coding specialists and penetration testers to other niche cybersecurity consultants. They are supported by a company-wide cybersecurity initiative for identifying best practices, technical standards, processes, and policies.
- **Customer security objectives and requirements:** Stakeholder and security requirements are identified and analyzed, and the intended operational environment is fully understood and incorporated before specifying security requirements. Regulatory, legal, business, and technological factors are also taken into account throughout the process.
- **Secure product architecture and design:** Secure architecture specifies and assures compliance with a wide range of security measures, requirements, and implementation guidelines. Product design focuses on standardized and secure implementation of software components – checking to make sure that features and functions are secure at the default level.
- **Pre-deployment assessment:** Security threat and risk assessments are performed by experts to anticipate foreseeable threats in the intended operational environment, including client infrastructure and integration of third-party components.
- **Security testing:** Product security testing is conducted regularly, either via manual penetration tests or in conjunction with automated machine security testing. The results are recorded and used as a basis for identifying corrective actions. They are then analyzed and appropriate actions are taken.
- **Deployment and maintenance:** This stage ensures secure implementation and deployment of the Siveillance Suite. We publish cybersecurity hardening guidelines for all Siveillance Suite products and make sure that they are maintained throughout the product lifecycle. A cybersecurity checklist is also completed at deployment.
- **Incident vulnerability management:** Siveillance Suite is subject to our incident and vulnerability handling process in the event that any vulnerability or threat is detected. Both vulnerabilities and incidents are handled by the Siemens ProductCERT team, which operates globally around the clock.

We're committed to providing you with a high degree of cybersecurity in order to provide you with adequate protection from increasing cyber risk in our digitalized world.

Further Reading

Learn more about the Siveillance Suite of security solutions and Siemens approach to cybersecurity at:

usa.siemens.com/security
usa.siemens.com/cybersecurity
usa.siemens.com/cybersecuritywhitepaper

Siemens Industry, Inc.
Smart Infrastructure
1000 Deerfield Parkway
Buffalo Grove, IL 60089-4513
Tel. 847-215-1000

Part # 153-SBT-1307