SIEMENS
Ingenuity for life

Cyberintelligent security solutions with Siveillance Suite

From digital buildings to critical infrastructure

siemens.com/security

Executive summary

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 risk.

Our buildings and assets need to be secure for the future. Siveillance Suite, Siemens Building Technologies' extensive portfolio of physical security solutions – from identity and access management to physical incident management and industrial command and control systems – 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.

We're prepared for the fact that it's not **if**, but **when** a cybersecurity incident will happen. Let's take a closer look at how we integrate security into our products, solutions and services.

The Siveillance Suite of products from the Siemens Building Technologies 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.

First things first: What exactly is cybersecurity?

IT security, information security, cybersecurity – there are several terms and definitions in use today regarding security in the digital domain, and it can be quite confusing to know what exactly the terms imply. For the purpose of this document, Siveillance™ Suite from Siemens Building Technologies defines and applies the term "cybersecurity" as follows:

"The protection of company assets against harm caused by digital attacks against the availability, confidentiality, integrity, authenticity, and reliability of information in cyberspace. Cyberspace is the complex system of interactions among people, software, and services by technical means connected to the Internet."

Holistic cybersecurity for Siveillance Suite

The building technologies industry and its customers face a variety of challenges: The physical threats are more obvious, whether it's intrusions into buildings or sites, or incidents occurring on the perimeter, that jeopardize people and assets. But 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. As a leader in the field, we understand these threats, especially the space between physical and cybersecurity challenges and the interactions among technology, people, processes, and communication. We've therefore prepared our portfolio for a fast, complex, and ever-changing threat landscape.

To stay ahead of the curve, we also contribute and adhere to leading international standards, which are essentially codified best practice. For example, as a company we're committed to following international security standards ISA/IEC 62443 and ISO/IEC 27001, as well as the EU General Data Protection Regulation, as cybersecurity guidelines.

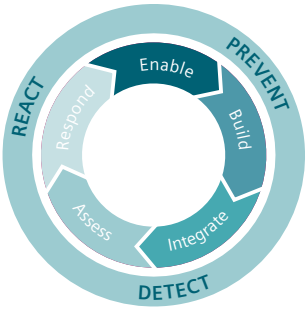
People
Communication
Process
Technology

The Secure by Design approach: From concept to deployment and beyond

Secure by Design is our pledge to address comprehensive security in our product development process by integrating cradle-to-grave activities. Built on the main pillars of prevention, detection, and reaction, this ensures that we continuously develop our products, solutions, and services.

When it comes to physical security, Siveillance Suite is in the best possible position to protect our customers' real estate; and we also understand the need to secure our physical security offerings from emerging challenges in the era of digitalization.

Siveillance Suite stands for security, and it offers a completely flexible and interoperable portfolio for all environments – from assets that require small systems to large, critical infrastructure.



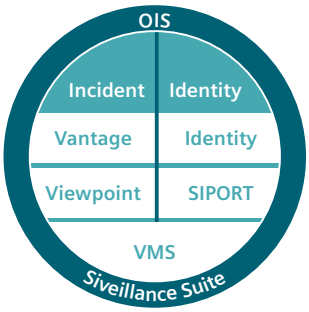
Siveillance Suite – an extensive portfolio for physical security

Incident management:

- **Siveillance Vantage:** Industrial command and control solution
- **Siveillance Viewpoint:** Physical security information management (PSIM)
- **Siveillance VMS:** Video surveillance/video management

Identity management:

- **Siveillance Identity:** Manages and automates physical identities, access privileges and credentials
- **SIPORT:** Access control management
- **Siveillance VMS:** Video surveillance/video management



Siveillance Open Interface Services (OIS) is an interface and integration platform for the integration of subsystems into management stations.

Data protection and the EU General Data Protection Regulation

Siemens understands that data protection is a critical topic for our stakeholders in the digitalization era. We recognize the obligations that apply to any handling of data inside the European Union, and so Siveillance Suite is compliant not only with European regulations, but also with country-specific data protection laws.

On April 27, 2016, the Parliament and Council of the European Union (EU) adopted the EU General Data Protection Regulation (GDPR). The GDPR will be directly applicable to EU Member States as of May 25, 2018, thereby ensuring a harmonized data protection standard across the European Union.

The Siemens Building Technologies Division data protection department has developed a program that takes both internal and customer factors into account.
We're implementing this program through our data protection officers from the regional companies located in the European Union.

The protection of data in cross-border transactions and transmissions is included in the programs and is of high importance to Siemens.

Privacy by Design

Privacy by Design is a general requirement for the development of data processing operations.

We consider data protection when planning and developing all Siveillance Suite products. For example, tests must be passed so that data protection comes into play at the very beginning of the product planning cycle.

Data protection is also included in our technical and organizational measures, and is implemented in Siveillance Suite by way of certain functions, such as:

- Access control to personal data in the products
- Compulsory use of passwords
- Encryption (of data at rest and data in transit), where appropriate
- Automatic log-out functions
- Two-factor authentication, if necessary

For example, Siveillance Vantage also ensures that personal data like usernames, passwords, and subsystem addressable locations are stored in hashed, nonidentifiable fields to prevent unauthorized access.

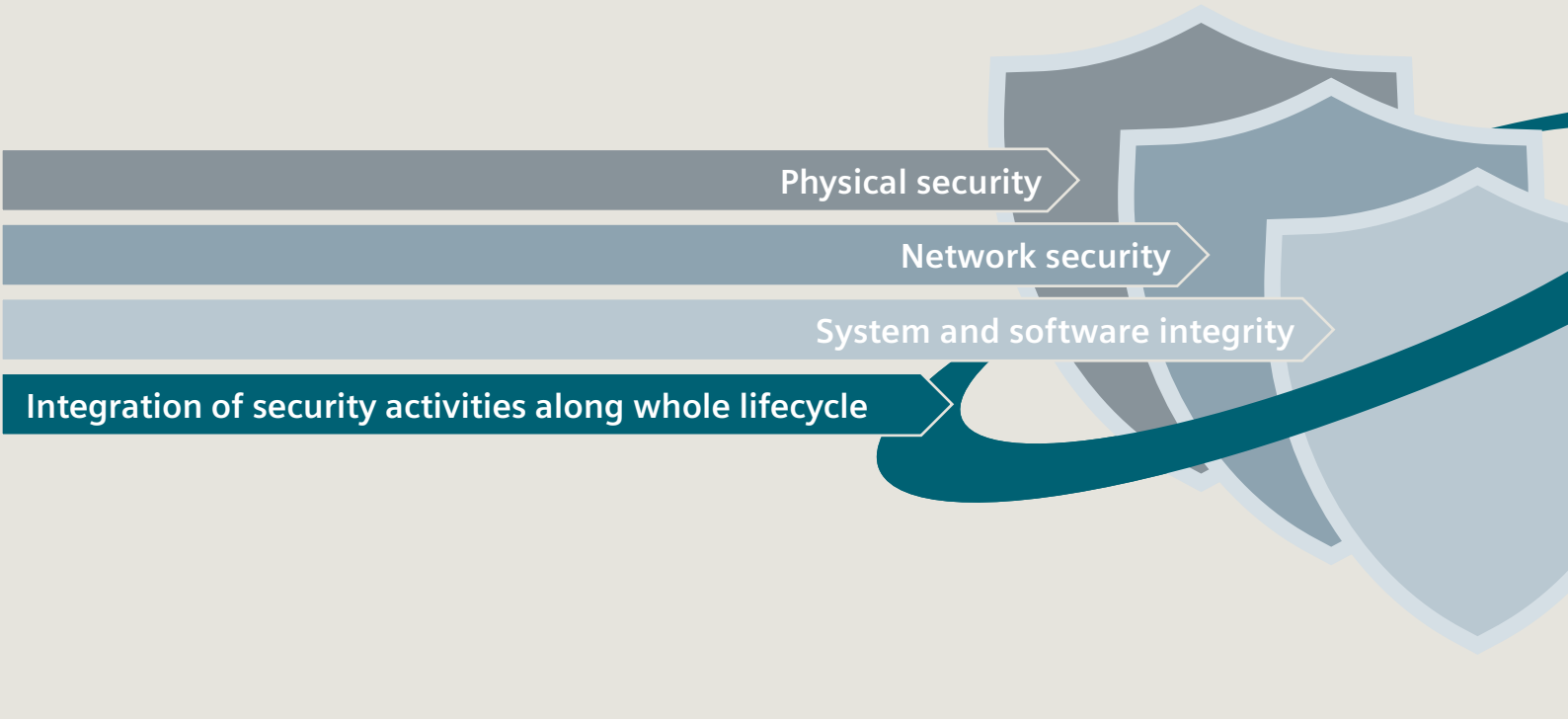
As our customer, you're offered a variety of options for customizing the product (for example, functions and settings) depending on your requirements and sensitivity/criticality of the personal data being processed.
You are free to use any or all of the product's technical and organizational features, and to decide whether and how to store personal data. This decision remains your responsibility in your role as data controller.

As another example, SIPORT allows you to decide whether, where, how, and for what period of time personal data are stored, and to either grant or reject access.

Data processing on behalf of the controller

The responsibility for data protection is and remains with our customer, who then decides which personal data are collected and stored where, how and for how long.

In the context of our maintenance services, Siemens may access personal data. In this event, we act as a data processor and adhere to your instructions, in particular to our contractual agreements.



Cybersecurity initiative governs processes, guidance and best practice for Siveillance Suite

In order to ensure the best possible defense against cyber challenges across all Siveillance Suite products, we rely on our cybersecurity initiative to ensure that our expertise is always available to you. This company-wide initiative is essentially a risk management program that actively drives our holistic security methodology for all Siemens products, solutions, and services, by identifying best practice and deriving company-wide technical standards, processes, and policies.

When it comes to cybersecurity, the initiative's primary goals are the early identification and proactive prevention of security issues and efficient incident management.

Siemens' Building Technologies Division not only continuously invests in technology development for digital protection and product security, it also trains employees to raise and maintain their cybersecurity expertise and awareness.

How Siveillance Suite meets cyber challenges

Siveillance Suite actively drives security measures for deployment in customer environments by following best practice technical standards, processes, and policies. It's at the cutting edge of methods for mastering the challenges companies face today.

Cybersecurity is a critical factor for your business success; it targets the confidentiality, integrity, availability, and protection of data, products, solutions, and services. Siveillance Suite sees cybersecurity as an enabler for the digital transformation and also as a strong factor in business competitiveness. With these goals in mind, the company has deployed dedicated teams, policies, and processes to protect its portfolio.

Implementing comprehensive security in Siveillance Suite

When we develop our security solutions, we follow a holistic approach to offer you a balance of cyber, physical, and organizational security measures for protection against current and future threats. Siveillance Suite is continually improved while we follow our Secure by Design approach: a pledge to include comprehensive security in our development process by integrating cradle-to-grave activities that will ensure continuous enhancements to our products during their lifecycle.

Patches, updates, and upgrades are released as a part of our software maintenance program. This means that we'll provide complete and highly competitive software maintenance to our end customers to increase satisfaction by keeping their solution safe from the latest known threats. It includes technical hotline support run by product experts and, where a valid subscription to the program exists, entitles the customer to free software upgrades.

All Siveillance Suite products follow the "cybersecurity landscape."

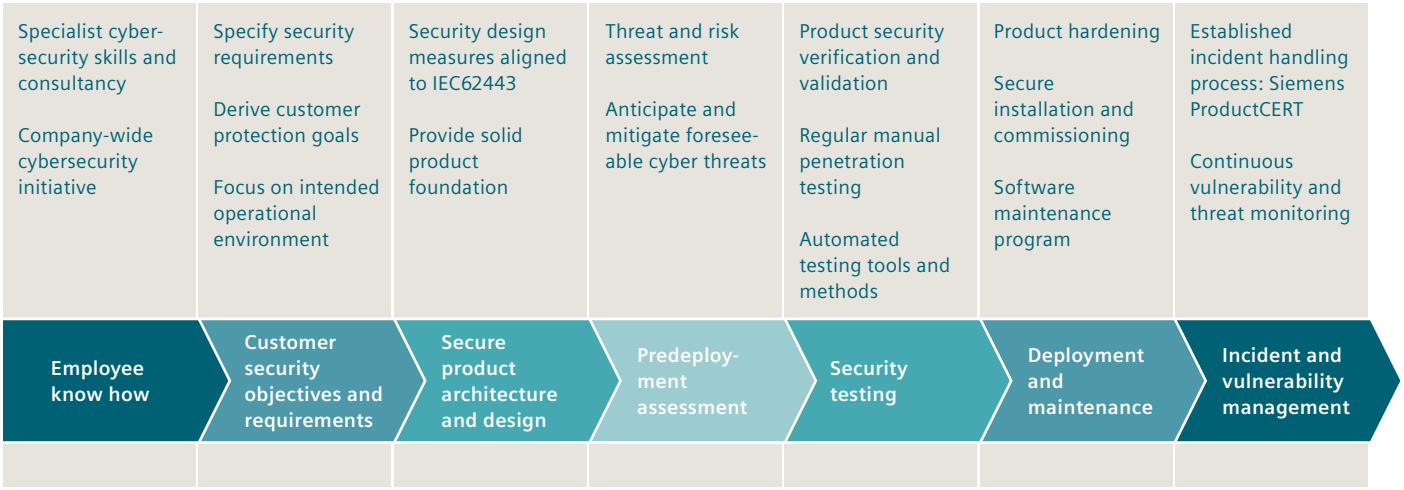
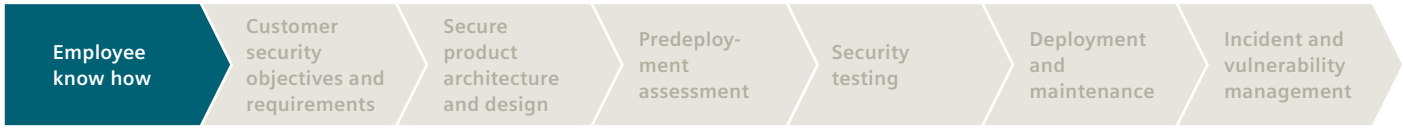


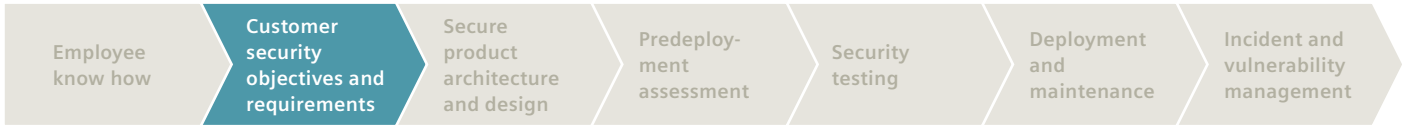
Figure 1 – Siveillance Suite cybersecurity landscape

Siveillance Suite cybersecurity landscape activities



Siemens takes its responsibility to provide cybersecurity training and awareness to its employees and to grant access to the right skill sets across the company very seriously. 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. This enhances the portfolio because it means that as technology, the market, customer needs and cyber challenges evolve, Siveillance Suite will be well equipped to face the challenges that emerge, whatever the location.

Figure 2 – Siemens Building Technologies cybersecurity network



As part of our holistic approach to security and to ensure you as the customer are at the forefront of our security view, our initial focus is on the intended operational environment for deployment of a product or solution. As a result, various stakeholder and security requirements need to be identified and analyzed, and the intended operational environment itself must be understood fully and incorporated before specifying security requirements. The resulting requirements specification serves as input for the 'Security Product Architecture and Design' phase as a basis for the design of security measures. The development of security requirements is combined with regular engineering activities, for instance, the identification of potentially conflicting requirements.

We specify and decide on security features of each intended operational environment at the beginning of a project, by using a reference scenario, for example. Any divergence from that scenario is checked for its impact on the security landscape. The cybersecurity level of the deployment also depends on the features of each type of operational environment. For example, either a "basic" or "advanced" installation of a solution may be recommended to maintain security integrity, depending on its critical cybersecurity requirements. Regulatory, legal, business and technological factors are also taken into account throughout the process.

Our goal is to continuously and methodically respond to stakeholder security demands: from analyzing the various product and solution stakeholders, defining stakeholder needs and security requirements, prioritizing them, and then assigning the results to the product or solution release plan.

This stage is implemented in order to ensure a solid product foundation. Secure architecture is an embedded discipline that specifies and assures compliance with a wide range of security measures, requirements, and implementation guidelines. For example, the Siemens Building Technologies Division product development process for Siveillance Suite follows a mandatory cybersecurity policy aligned with IEC 62443.

This policy provides measures for secure development of each product in accordance with the appropriate security level required for your intended operational environment.

Secure coding focuses on standardized and secure implementation of software components fundamental to our products, solutions, and services, while secure configuration looks at the hardware components – checking to make sure that features and functions are secure at the default level.

Security threat and risk assessments are performed by experts to anticipate foreseeable threats in a product or solution's intended operational environment. This assessment starts early on in the process to identify and mitigate risks appropriately, and it's repeated as required.

Any identified threats or risks need to be treated adequately, with mitigations that are developed and implemented in the development or engineering project. This process also takes into account your existing infrastructure as well as the integration of third-party components.

Product security testing is conducted regularly, either via manual penetration tests or in conjunction with automated machine security testing. Its purpose is to ensure that the selected product, solution, or service meets your specified security requirements, to demonstrate that the product component, solution, or service fulfills your security expectations, and to make sure that it's securely configured when in its intended operational environment. This is achieved by trying to break the system in order to secure it.

The results of the security tests are recorded and used as a basis for identifying corrective actions. They are then analyzed and appropriate actions are taken: for example, a reevaluation is performed and/or mitigation plans defined.

Employee know how | Customer security objectives and requirements | Secure product architecture and design | Predeploy-ment assessment | Security testing | **Deployment and maintenance** | Incident and vulnerability management

This stage ensures secure implementation and deployment of Siveillance Suite. We publish cybersecurity hardening guidelines for all Siveillance Suite products and make sure that they are maintained throughout the product lifecycle. Our engineers follow these guidelines rigorously at the point of deployment. The secure (base) system configuration and hardening defines how a system needs to be configured for a secure operation in the intended operating environment. Configuration options include determining which applications to install, activating or deactivating application settings, and setting up user and system accounts and access rights.

A cybersecurity checklist is also completed at deployment that includes performing operational measures like:

- Port whitelisting
- Using appropriate antivirus software
- Network protection (including network segregation, firewall, demilitarized zone)
- Performing system updates/patches
- Correct user administration
- File system protection
- Physical protection of interfaces
- Log file monitoring
- Deactivation of extraneous services

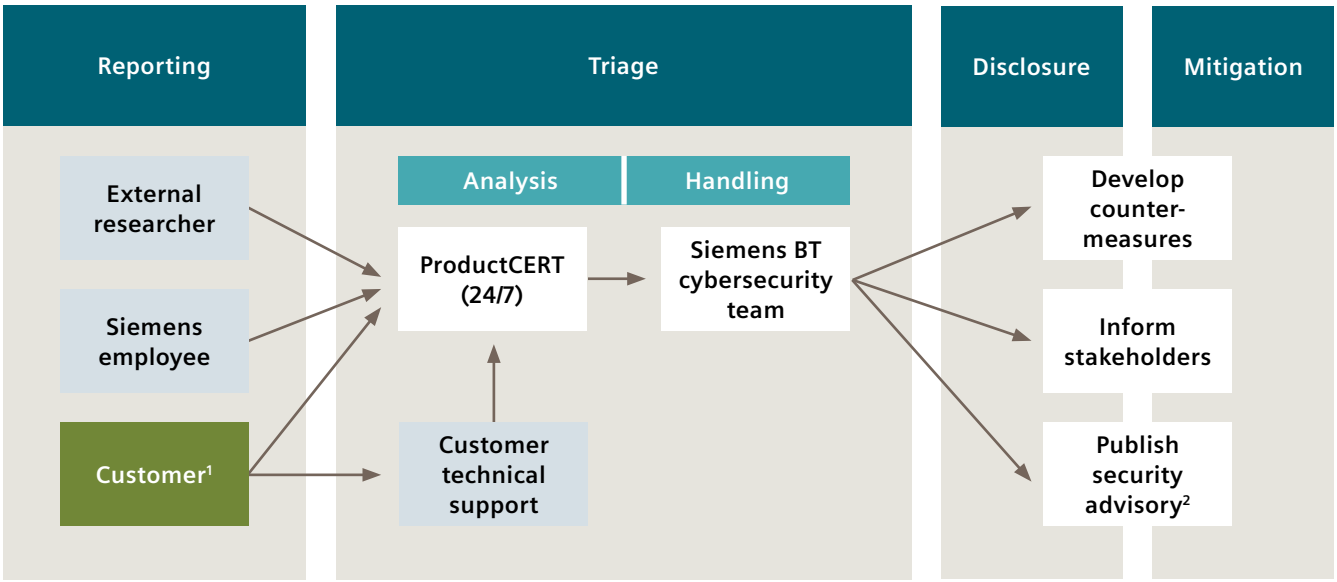
Employee know how | Customer security objectives and requirements | Secure product architecture and design | Predeploy-ment assessment | Security testing | Deployment and maintenance | **Incident and vulnerability management**

Regarding emergency management, Siveillance Suite, like all of our products and solutions, is subject to an incident and vulnerability handling process in the event that any vulnerability or threat is detected.

Incident handling process: We have a support mechanism for customer-reported vulnerabilities or other detected issues. Both vulnerabilities and incidents are submitted to our technical support team and handled by the Siemens ProductCERT team, which operates globally around the clock.

Vulnerability management: This is our process for fine-tuning our security. Continuous threat monitoring allows us to detect and fix potential vulnerabilities in our products and solutions, reducing your exposure to risk. Siveillance Suite has all of its software components registered, and so will be notified if and when security vulnerabilities are found.

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.



[1] The customer can use either route to report a vulnerability or potential incident
[2] https://www.siemens.com/cert/en/cert-security-advisories.htm

Figure 3 – Siveillance Suite incident handling process

Siveillance Suite portfolio in detail

Siveillance Suite incident management

Siveillance Vantage

The command and control solution from Siemens, Siveillance Vantage, is specifically designed to support security management at critical infrastructure sites, industrial complexes, campus-type environments, or multi-site applications. It offers precisely the kind of on-time support needed to react effectively to security and safety incidents at any time.

Cybersecurity measures in Siveillance Vantage

Both Siveillance Vantage and Viewpoint product development processes integrate the following Security by Design elements:

- **Certificate-based data exchange**
  Certificates are an important way to define a trusted source of communication. They establish that a server, for example, is not an imposter but rather is already known and can be trusted. Siveillance Suite seamlessly integrates certificates in our customers' IT infrastructure.
- **LDAP-based authentication**
  LDAP stands for lightweight directory access protocol, a defined protocol for authentication and authorization. The most common use of LDAP is Microsoft's Active Directory, which applications (including our products) can use to log in using their Windows accounts as opposed to application-specific logins.
- **Secure encrypted communication (HTTPS, SSH)**
  Encrypted communication is important for our customers in order to prevent man-in-the-middle attacks and ascertain that sensitive security data cannot be intercepted or changed in transit. HTTPS is one of these communication protocols, and it is the de facto standard for secure web communication. SSH is a secure shell communication protocol that is the default for terminal access to Linux servers.

Siveillance Viewpoint

Our innovative and powerful physical security information management (PSIM) solution Siveillance Viewpoint supports mid- to large-sized industrial customers in managing risks while reducing operational costs.

It is a single platform that integrates all subsystems using open integration methods and provides our customers with a comprehensive security view of their physical business landscape.

Cybersecurity measures in Siveillance Viewpoint

Both Siveillance Vantage and Viewpoint product development processes integrate the following Security by Design elements:

- **Certificate-based data exchange**
  Certificates are an important way to define a trusted source of communication. They establish that a server, for example, is not an imposter but rather is already known and can be trusted. Siveillance Suite seamlessly integrates certificates in our customers' IT infrastructure.
- **LDAP-based authentication**
  LDAP stands for lightweight directory access protocol, a defined protocol for authentication and authorization. The most common use of LDAP is Microsoft's Active Directory, which applications (including our products) can use to log in using their Windows accounts as opposed to application-specific logins.
- **Secure encrypted communication (HTTPS, SSH)**
  Encrypted communication is important for our customers in order to prevent man-in-the-middle attacks and ascertain that sensitive security data cannot be intercepted or changed in transit. HTTPS is one of these communication protocols, and it is the de facto standard for secure web communication. SSH is a secure shell communication protocol that is the default for terminal access to Linux servers.

Siveillance Suite portfolio in detail

Siveillance Suite identity management

Siveillance Identity

Siveillance Identity Self-Service Portal is an intuitive web-based portal that offers in-house access request management across multiple sites. Designed to streamline and simplify access request management processes, the portal's automated approval workflows can be easily configured, enforced and audited and allow employees and decision makers alike to handle access privileges more efficiently. Designed with the needs of small to enterprise-scale companies in mind and adhering to company policies and regulations, Siveillance Identity Self-Service Portal is the ideal choice for manufacturing industries, offices, higher education, financial, and insurance companies who are looking for the optimal solution for simplifying their access approval management and boosting operational productivity, transparency, and security.

Cybersecurity measures in Siveillance Identity

To ensure the security integrity of Siveillance Identity, certain recommendations are made, for example:

- Limit network access based on the "least privilege" principle
- Segregate network into zones
- Use secure component communication protocols, for example, LDAP-based for authentication and HTTPS for secure encrypted communication
- Uses secure, verified third-party components

SIPORT

SIPORT is a comprehensive, modular and reliable system for access control and time management. It provides a simple solution that allows authorized people like employees and visitors to move through a building or building complex with ease while keeping unauthorized people out. SIPORT is exceptionally well equipped for globalization due to its scalability and networkability. It is a robust and flexible security solution that can be modified for various market needs, including office complexes, banks, insurance companies, hospitals, refineries, and airports.

Cybersecurity measures in SIPORT

To ensure the security integrity of SIPORT, certain recommendations are made, for example:

- End-to-end encryption from card to card reader to controller to management station, to prevent eavesdropping
- Secure, segmented architecture on client-server side
- Digitally-signed communication between client and server prevents transmission interference
- User authorization permission checks when a client establishes a connection to a server

SIPORT has also been tested and certified in accordance with procedures approved by TÜV IT, an authorized independent certification body, including:

- General organizational test
- Technical test of the application
- Tests of the procurement, development and maintenance of information systems

Siveillance VMS

Siveillance VMS is a powerful IP video management software (VMS) designed for deployment environments ranging from small and simple to large-scale and high-security. Its single management interface enables the efficient administration of the system, including multiple cameras and security devices. There are three versions to fulfill diverse customer needs and technical requirements.

Cybersecurity measures in VMS

To ensure the security integrity of Siveillance VMS, certain recommendations are made, for example:

- Restrict access to servers
- Use network infrastructure that supports physical network or VLAN segmentation
- Segregate camera and server networks
- Place the mobile server in a "demilitarized zone" (DMZ) with one network interface for public access and one for private communication with other servers
- Correct and appropriate use of firewalls
- Control access to servers, clients and applications
- Correctly configure VMS with roles that control access to the system and designate appropriate tasks and responsibilities

Siveillance Open Interface Services (OIS)

OIS is an integration platform for Siveillance Suite that allows integration of Siveillance product and third-party subsystems via a single application programming interface (API).

- Acts as the module for integrating numerous types of subsystems
- Allows preprocessing of information from a subsystem
- Provides a set of standardized interfaces
- Software development kit (SDK) available for additional integrations

In addition, OIS provides a built-in powerful, configurable logic that allows:

- Interoperability between integrated subsystems with no interaction needed from a building management station
- Filtering and forwarding of events to one or multiple management stations
- Preprocessing of messages and alarm acknowledgement handling
- Manual command execution from management stations
- Execution of logic commands based on preprogrammed rules using easy scripting language

OIS comes with an easy-to-use web interface for fast configuration in a familiar and straightforward web environment.

Cybersecurity measures in OIS

Because OIS is an integration technology built into Siveillance Suite products, the cybersecurity measures it employs are considered to be part of those of the products themselves. Consequently, OIS also uses the overarching security activities that are part of the cybersecurity activity landscape.

Siemens Common Remote Service Platform (CRSP)

This is the platform used for delivering secure remote access for Siveillance Suite. Data and information related to building infrastructure are accessible worldwide with a reliable, high-performance, and secure remote access platform. This platform ascertains that the remote services delivered by Siemens meet your stringent cybersecurity requirements.

Currently, CRSP supports connections to SIPORT, Siveillance Viewpoint, and Siveillance OIS, with more connections being developed for Siveillance Identity and Siveillance VMS.

Cybersecurity measures in CRSP

Siemens CRSP is certified by the ISO/IEC 27001:2013 standard; it retains ongoing certification by TÜV Süd in Germany and is listed in the International Register of ISMS Certificates. The central CRSP platform is located within Siemens' own network infrastructure and is protected from unauthorized access from the outside. Within a demilitarized zone (DMZ), a CRSP access server acts like a secure gatekeeper between the Internet and the Siemens network, where your data are stored. It establishes a secured connection between your system and the service engineer's system. A DMZ with proxy server technology is a proven network architecture that ensures that only data that have been previously requested by a Siemens authenticated remote service process are allowed to pass into the Siemens network.

Data management: Siemens classifies customer data as strictly confidential and grants access only on a need-to-know basis. The enforcement of this principle is supported by policy-based access control mechanisms. The measures implemented for data management depend on your individual requirements for data protection, the data type, and the applicable laws.

CRSP applications

The following remote services applications are supported by a CRSP connection:

Remote Operational Assistance
- Check configuration, settings, log books and software versions
- Change configuration and settings
- Execute reports and modules
- Log in and log out

Remote Diagnosis and Repair
- Reboot server and client
- Run diagnosis tools
- Perform data backup and restore

Remote Software Maintenance
- Restore data backup
- Install software updates and upgrades

Remote Commissioning
- Perform remote engineering and project extensions using license change and database extension
- Add and modify configuration and settings

Siveillance Suite and Remote Access Services

In a digitalized world, cyberintelligent security solutions recognize the need for data to remain your company's most valuable commodity. This means that elements like data transfer, storage, efficiency, and optimization will continue to be vitally important for our customers in order to operate a successful business.

Likewise, data, convenience and cybersecurity work together, and Siveillance Suite is prepared for the fact that our customers may require services that support data access, protection of data from cybersecurity threats, and data optimization.

Siemens was one of the first companies worldwide to develop an information security management system (ISMS) for remote services conforming to ISO/IEC 27001 – the norm for systematic cybersecurity management on an organizational level.

Siveillance Suite also offers remote services as part of its solutions to provide its customers with greater convenience in accessing Siveillance Suite products.

We provide an extensive range of services via a secure remote connection. This secure connection gives us access to your systems and allows us to capture and monitor the most important parameters. This enables us to take a proactive approach, minimizing the risk of potential problems so that availability is maintained. The ability to capture data continuously via a secure remote connection paves the way for other services like performance optimization, predictive analysis, and condition forecasting.

Conclusion

As a market leader, Siveillance Suite understands what it takes to meet your cyber and physical security needs today. Our cybersecurity landscape and our combined approach to the security paradigm involving people, process, technology, and communication means that you are provided with today's state-of-the-art solution that is designed to remain at the cutting edge of the building technology industry.

Because we live in the era of digitalization, we're future-oriented – which means that Siveillance Suite is future-proofed in order to arm our customers against both current and potential cyber and physical security challenges. For Siemens, providing a cyberintelligent security solution like Siveillance Suite is a necessary step to minimizing risk while maintaining the integrity of our products and solutions in their intended environment.

Ultimately, whether it's cyber or physical threats, we're committed to safeguarding the only thing that matters to you – security as the foundation of your business.

Contact

For questions about Siveillance Suite, please contact:
siveillance.support.industry@siemens.com

When building technology creates
perfect places – that's Ingenuity for life.

Never too cold. Never too warm.
Always safe. Always secure.

With our knowledge and technology,
our products, our solutions and our
services, we turn places into perfect places.

We create perfect places for their users'
needs – for every stage of life.

#CreatingPerfectPlaces
siemens.com/perfect-places

Published by
Siemens Switzerland Ltd 2017

Building Technologies Division
International Headquarters
Gubelstrasse 22
6301 Zug
Switzerland
Tel +41 41 724 24 24

Article no. BT_0128_EN (Status 08/2017)