STORMSHIELD

Stormshield Endpoint Security

Evolution

Version 2.4.3

CSPN Security Target

Document version:	1.4
Reference:	KILEMA/ST
Date:	02/10/2023

Contents

List of figures

List of tables

Terminology and abbreviations

ANSSI	*Agence Nationale de la Sécurité des Systèmes d'information* (National Cybersecurity Agency of France)
SES	Stormshield Endpoint Security
Security policy	Parameters of security functions
TOE	Target of Evaluation

REFERENCE DOCUMENTS

[CSPN]	FIRST LEVEL SECURITY CERTIFICATION FOR INFORMATION TECHNOLOGY PRODUCTS Version 2.1 of 01/13/2020
[Administration Guide]	Stormshield Evolution 2.4.3 Administration Guide
[SelfProtection]	Detailed Architecture of « Self-Protection » functions Version 1.0 – 13/09/2022

1. PRODUCT IDENTIFICATION

Vendor	Stormshield
Vendor website	www.stormshield.com
Brand name of the product	Stormshield Endpoint Security Evolution
Version evaluated	2.4.3
Product category	Intrusion Detection

2. PRODUCT DESCRIPTION

2.1 Overview of Stormshield Endpoint Security

The Stormshield Endpoint Security Evolution (SES Evolution) software suite is a Windows-based workstation and server security solution - it allows organizations to centrally protect their entire pools of servers, microcomputers and laptop computers from known and unknown attacks, data theft or loss, intrusions or unauthorized operations.

This modular suite combines the following security modules:

- **Host-IPS (Intrusion prevention)**. SES blocks attacks by detecting the execution of intrusion techniques such as (but not limited to) buffer overflow, keylogging attempts or the corruption of in-memory processes.
- **Application control**. SES allows whitelisting of authorized applications and blacklisting of risky applications.
- **External device control.** SES allows monitoring of removable data media such as USB devices, external hard drives, network cards, CD/DVD burners and serial ports.
- **Network access control.** SES implements an application firewall that allows monitoring applications access to the network.
- **Wireless network security.** SES is able to monitor the use of WiFi and Bluetooth connections and apply specific policies according to the connection
- **Response capability.** SES enables workstation remediation following a security event.
- **Forensic capability.** SES is able to search for indicators of compromise on workstations.

The security administrator configures the security policy of a protected pool of devices by using a centralized administration system. Changes made to this policy are deployed and applied dynamically and automatically on all workstations. This agent communicates with the centralized administration system in a secured manner.

This target of the evaluation is the software agent deployed on the workstation.

2.2 Using the product

2.2.1 Operating infrastructure

The figure below illustrates the interactions between the components and the traffic involved in Stormshield Endpoint Security Evolution:

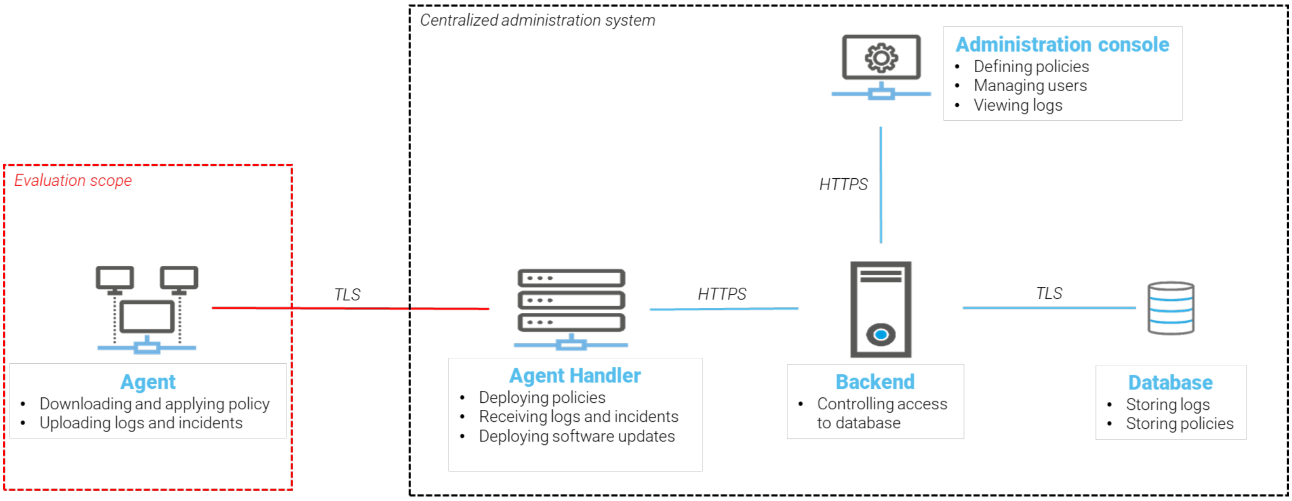
Centralized administration system
Administration console
Defining policies
Managing users
Viewing logs
HTTPS
Evaluation scope
TLS
HTTPS
TLS
Agent
Downloading and applying policy
Uploading logs and incidents
Agent Handler
Deploying policies
Receiving logs and incidents
Deploying software updates
Backend
Controlling access to database
Database
Storing logs
Storing policies

Figure 1: Setup of the product

The **centralized administration system** contains the following components:

- The **administration console** is the administrator configuration interface, it also manages users and reads logs generated by client workstations.
- The security policy is available on the **agent handler** component, from which client workstations can download the policy. The agent handler also deploys software updates and receive logs generated by client workstations.
- Logs and the security policy are stored in a dedicated SQL **database**.
- The **backend** component manages access to the database from the administration console and the agent handler.

On each client workstation, the Stormshield **agent** applies and enforces the security policy, generates logs and reports them to the agent handler.

2.2.2 Deployment

As soon as the centralized administration system is installed and configured, the agent can be deployed on client workstations.

Once SES Agent is installed, and after the client workstation is restarted, it immediately applies the configured security policy. When a security event is detected, an ephemeral Windows notification inform the user about it, an alert is logged in the local log and sent to the SES agent handler.

Stormshield Endpoint Security also builds an update mechanism into its components.

2.3 Scope of evaluation

The evaluation focuses on the agent software component and covers the following functions:

- **Self-protection**: the agent protects itself from attempts by standard users or malicious attackers to disable or uninstall components. In addition, it securely stores its sensitive assets (logs, security policy, secrets)
- **Secure communication**: the agent communicates securely with the agent handler so that the integrity, confidentiality and authenticity of exchanged data (security policy and logs) are guaranteed.

The **innocuousness** of the agent is also under evaluation, i.e., the fact that the presence of the agent does not degrade the level of security of the workstation.

The centralized administration system (Agent handler, database, backend and administration console) is not within the scope of evaluation, neither are the investigation and remediation feature initiated from administration console.

2.4 Evaluation platform

The evaluation platform includes a client workstation and a server. The agent is installed on the client workstation. The server hosts the centralized administration system (agent handler, backend, administration console and the database):

- On the server side, the operating system of the workstation is Windows Server 2019.

- On the client side, the product is evaluated based on the Windows 10 64-bit operating system (the latest version of Windows 10 available at the beginning of the tests).

3. OPERATING ENVIRONMENT

3.1 Typical users

The SES Evolution agent must be installed on the workstation with local administrator rights. After its installation, the agent will be managed remotely through the administration console.

The workstation user does not need to perform any operations on the product, as all settings are configured remotely from the administration console.

3.2 Operating environment of the product

The evaluated product, the agent software, can be integrated into an environment as shown in the figure below:

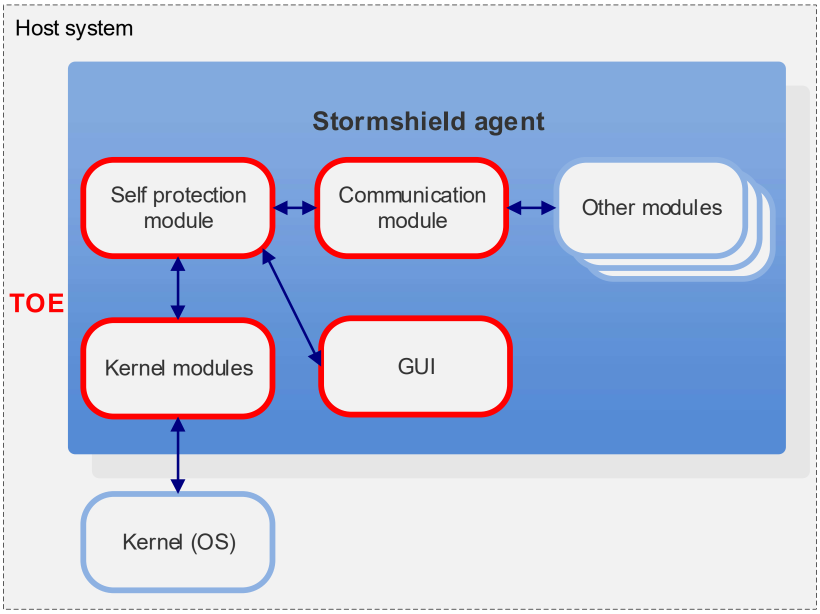

Figure 2: Scope of evaluation

The agent supports these Windows versions:

- Windows 7 and later versions for user workstations;
- Windows Server 2008 R2 and later versions for servers.

3.3 Assumptions about the environment

A.USER_WORKSTATION

The agent is installed on a clean workstation.

Permissions on system resources must remain standard permissions, and access to “Program files” folders and system folders in particular is restricted to administrators only.

The configuration of the workstation does not require any particular hardening; however, it must not weaken the security of the workstation.

User and administrator accounts use a robust authentication method.

A.POLICY

The security policy generated outside the scope of the TOE by the SES console is assumed to be trustworthy.

This policy does not allow the “challenge” feature, which makes it possible to perform administration operations by exchanging temporary passwords with the centralized administration system.

Safe mode must also be disabled for standard users on the workstation on which the agent is installed.

A.NON_ADMIN_USER

Users of the workstation system have no “administrators” rights.

4. SENSITIVE ASSETS

4.1 User assets

The user assets to be protected by the agent are:

- **UA.Logs:** All data collected by the agent (security events, system operating events and monitoring data).

  Protection requirements: confidentiality, integrity, authenticity.

4.2 Sensitive assets in the TOE

The TOE-specific sensitive assets are:

- **TA.Software**: the agent's software including all installed resources required for the product to run.

  Protection requirements: integrity during execution (guaranteed by the ToE), authenticity during installation (guaranteed by the operating system), availability (guaranteed by the ToE).

- **TA.Policy**: the agent's security and configuration policy.

  Protection requirements: confidentiality, integrity, authenticity.

- **TA.Secrets**: the cryptographic keys and secrets that make it possible to guarantee the authenticity and confidentiality of data and exchanges between the agent and agent handler.

  Protection requirements: confidentiality, integrity.

4.3 Summary

Type of asset	Asset	Confidentiality	Integrity	Authenticity	Availability
User	UA.Logs	●	●	●	
TOE	TA.Software		●	●	●
	TA.Policy	●	●	●	
	TA.Secrets	●	●		

Table 1: Summary of sensitive assets

5. THREATS

In the description of threats below, the term “attacker” shall be taken to mean any malicious code or individual who has local or remote access to the workstation and who doesn’t have any privilege.

- **T.Logs**: a local attacker accesses logs or alters them (UA.Logs). They can for example attempt to look up events collected from other users on the host with the purpose of obtaining confidential information. The attacker can attempt to conceal malicious operations by deleting data collected by the agent.

- **T.Software**: a local attacker changes the behavior of the agent (TA.Software) by exploiting a vulnerability of its detection functions (for example, the attacker executes code with the level of privilege of the agent due to a memory management bug in the software) or temper with any of its components.

- **T.Policy**: a local attacker changes the agent's behavior by modifying the policy or configuration provided by the administration console (TA.Policy). It can, for example, attempt to disable some or all of the security rules that the agent applies or modify the contact address of the centralized administration system to reroute communications to a malicious administration manager.

- **T.Secrets**: a local attacker accesses confidential data on the agent or alters data (TA.Secrets). They can for example attempt to steal one of the agent’s private signature keys stored on the host with the purpose of transferring data altered to hide traces of their malicious operations.

- **T.TrafficInterception**: an attacker on the network accesses confidential data between the agent and agent handler (UA.Logs, TA.Policy and TA.Secrets). They can for example capture network traffic between the agent and centralized administration system to read its contents.

- **T.TrafficAlteration**: an attacker on the network alters confidential data between the agent and agent handler (UA.Logs, TA.Policy and TA.Secrets). They can for example attempt to forward configurations or secrets to the agent by spoofing the identity of the agent handler or modify sent logs on the fly.

6. SECURITY FUNCTIONS

This section presents the security functions in Stormshield Endpoint Security Evolution.

TOE self-protection functions

- **F.LogProtection**: protection of local event logs. The agent stores its logs (UA.Logs) in the form of files. These files are protected through the implementation of restrictive ACLs that prevent non-privileged users from obtaining read/write access. The agent reinforces this protection by prohibiting unauthorized access to these logs via a kernel module (only modules inside the ToE have access to such data).

- **F.SoftwareProtection**:. Should an agent be compromised by an attacker via a flaw in its detection functions, the TOE provides defense in depth to ensure that the attacker cannot leverage this vulnerability to further compromise the TOE (TA.Software, TA.Policy, TA.Secrets) nor previously collected data (UA.Logs).

- **F.ConfigurationProtection**: protection of the agent's policy and secrets (TA.Policy, TA.Secrets). Such data is stored in the form of files and registry keys, and is protected through the implementation of restrictive ACLs that prevent non-privileged users from obtaining read/write access.

  The agent complements this protection by locking access to such data through a kernel module. Configuration data is stored in a signed container that is verified every time the agent starts.

Secure communication functions

- **F.ConfigurationDownload**: downloading and verification of the integrity and authenticity of security policies and secrets (TA.Policy, TA.Secrets). The confidentiality and integrity of data that the agent receives from its handler are protected with an encrypted TLS tunnel. The tunnel is always mounted upon the agent's request. The agent checks the agent handler authenticity with a certificate validation mechanism, and then verifies the signature of the received configuration.

- **F.LogLoading**: secure transfer of event logs (UA.Logs) to the centralized administration system. Before any data is sent to the centralized administration system, it is wrapped in signed containers that allow the recipient to verify its authenticity. The confidentiality and integrity of data that the agent sends to its handler are protected with an encrypted TLS tunnel. The tunnel is always mounted upon the agent's request. The agent checks the agent handler authenticity with a certificate validation mechanism

7. FUNCTIONAL COVERAGE

7.1 Threats and sensitive assets

	UA.Logs	TA.Software	TA.Policy	TA.Secrets
T.Logs	●			
T.Software		●		
T.Policy			●	

T.Secrets				●
T.TrafficInterception	●		●	●
T.TrafficModification	●		●	●

Table 2: Threat/Sensitive asset coverage

7.2 Threats and security functions

	F.LogProtection	F.Software Protection	F. Configuration Protection	F.Configuration Download	F.LogLoading
T.Logs	●				●
T.Software		●	●	●	
T.Policy			●		
T.Secret			●		
T.TrafficInterception				●	●
T.TrafficModification				●	●

Table 3: Threat/Security function coverage