

# With Secure Elements EPP + EDR Detailed EDR\_XDR Solutions Overview

2026, 4th edition

Controlled attack simulation with full telemetry analysis  
Environment: Windows 10, Windows 11, Windows Server + Active Directory



Evaluation period: March to June 2026  
Last updated: June 10, 2026

# Table of contents

01	Test summary
02	The importance of telemetry detail in the context of incidents
03	Protection model evolution
04	Scope, objectives and limitations of the 2026 edition
05	Certification model
06	Security feature availability
07	Agent Configuration and Operating Mode
08	Environment configuration
09	Operational Assessment – Phase 1
10	Operational Assessment – Phase 2
11	Responding to scenarios from Phase 2
12	Telemetry, correlation and incident visibility assessment based on Phase 2
13	Test conclusions

# Test Summary

## WithSecure Elements EPP + EDR

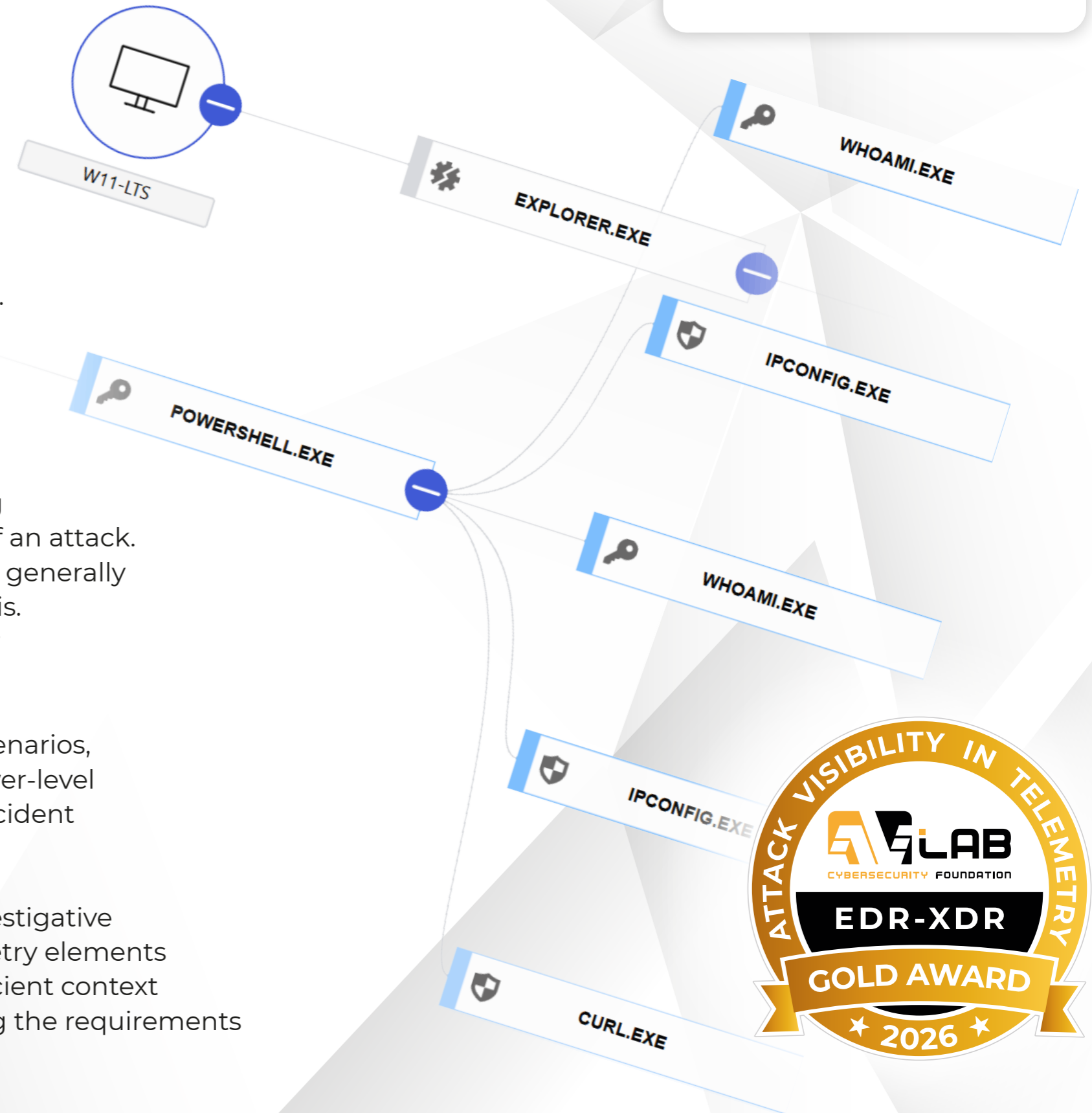
W / I / T / H<sup>®</sup>  
secure

WithSecure provides broad visibility across attack activity, including process execution, lateral movement, reconnaissance, persistence, and exfiltration. Throughout the tested scenarios, the platform consistently exposed process relationships, user context, command-line activity, network communication, and cross-host events, enabling analysts to reconstruct attack chains and investigate incidents efficiently. The solution demonstrated particularly strong visibility into WMI-, SMB-, and PsExec-based activity, including source-to-target host relationships during lateral movement scenarios.

The platform combines behavioral detections, event correlation, MITRE ATT&CK mapping, and incident investigation capabilities, allowing analysts to understand both individual events and the broader context of an attack. Network telemetry, process trees, and graphical event relationships were generally available and contributed to effective threat hunting and incident analysis. Cross-host correlation was also observed, providing visibility into attacker movement between systems.

Some limitations were identified in telemetry consistency. In selected scenarios, command-line visibility was incomplete or unavailable, and access to lower-level telemetry was occasionally reduced. These limitations did not prevent incident investigation but could affect the depth of analysis in specific cases.

Overall, the solution provides a high level of visibility, correlation, and investigative capability across a wide range of attack techniques. While certain telemetry elements are not consistently available in every scenario, WithSecure delivers sufficient context for incident response, threat hunting, and attack reconstruction, meeting the requirements of Level 2 – Advanced Visibility & Correlation.



**FULL**

The function works in its full scope without significant limitations.

**PARTIAL**

The function works, but with noticeable limitations.

**LIMITED**

The function is present but provides minimal visibility or analytical value.

**NONE**

The function is unavailable or no relevant visibility was observed.

**Attack Description**

Simulation of data retrieval via DNS TXT, reconstruction of the payload in %TEMP%, execution via LOLBin, and exfiltration.

**PARTIAL**

Copying the payload between PCs before execution, then running the RAT as an EXE and quietly capturing keystrokes.

**FULL**

User downloads ISO, mounts it, and executes EXE, triggering payload and C2 communication (HTTP/mTLS).

**FULL**

Payload is delivered via WebDAV and executed by the user, establishing C2. The compromise is then extended to another endpoint through SMB file transfer and remote execution via WMI.

**FULL**

The attacker copies the payload to a remote host via SMB and executes it using PsExec as a SYSTEM service, thereby achieving remote code execution.

**FULL**

Using a local LLM model to dynamically select subsequent steps. After verifying SMB connectivity to the target host, remote code is executed via WMI, which creates, compiles, and runs the payload on the victim's system, generating multi-stage process telemetry.

**FULL**

The attack uses an external AI model as a decision-making layer to control actions on the host. The script collects system information, saves it to a file, compresses it, and sends it externally via HTTP, while the AI issues subsequent decisions based on the system's state.

**FULL**

Clicking a phishing link launches mshta, which downloads and executes PowerShell. The script collects system data, establishes persistence via a Scheduled Task, runs rundll32 to hide its activity, and then exfiltrates data over HTTPS (curl). The entire chain uses LOLBIN.

**FULL**

## The importance of telemetry detail in the context of incidents

Modern attacks, including long-term activities carried out by advanced threat groups (APTs), are rarely limited to a single incident. They often begin with a seemingly harmless phishing message, which is actually only the first stage of an extensive chain of activities involving maintaining access, escalating privileges, so-called lateral movement, and data exfiltration [1].

In such scenarios, it is not only the detection of a single alert that is crucial, but also the ability to record and correlate all relevant technical artifacts. Recording even partial information about potential incidents allows for the reconstruction of events that took place in the analyzed environment. EDR-XDR solutions that monitor systems and applications, thanks to data correlation and automation mechanisms, support security teams in identifying the relationships between the stages of an attack.

Based on the collected telemetry, it is possible to determine what actions the attacker took, in what order, using what processes, applications, and user accounts. In the case of attacks spread over time, it is particularly important to maintain a consistent chronology of events and visibility of changes in user context and permissions. This information can be presented in the form of a logical or graphical reconstruction of the incident (e.g., as a process tree or a map of connections between hosts), which will certainly facilitate understanding of the full course of the operation.

Another important element of a mature EDR-XDR platform is the ability to perform advanced queries, allowing analysts to manually search raw telemetry, build their own queries, and verify investigative hypotheses. In the case of multi-stage campaigns, a ready-made alert often does not reflect the full extent of the compromise. Only in-depth analysis allows for the identification of additional traces of the breach, connections between systems, and the attacker's actual goal.

The broader the range of monitored events and the greater the depth of telemetry, the greater the organization's ability to understand the attacker's intentions and techniques, and consequently to mitigate the impact of the incident and adapt security policies to real threats.



[1] See an example of an APT attack on our editorial office in 2026:

<https://avlab.pl/przypadek-falshywego-phishingu-to-element-dlugofalowego-ataku-grupy-storm-1679/>



## Protection model evolution

Product categories such as EPP, EDR, XDR, and SIEM are increasingly overlapping in terms of functionality. In practice, the differences between them no longer stem from commercial nomenclature, but from the scope of telemetry collected, the method of correlating it, the level of automation, and the ability to reconstruct multi-stage attack chains.

Many modern solutions referred to as EDR have expanded their capabilities to include integration with SaaS services, identity systems, and selected network sources, bringing them closer functionally to the XDR class. At the same time, some products positioned as XDR still rely primarily on endpoint telemetry, offering limited cross-domain correlation. This means that the product name does not always reflect its actual level of operational maturity.

The table below is for organizational and illustrative purposes only. It presents the typical characteristics of each class of solutions, assuming that specific implementations may go beyond this framework or combine elements of several categories.

### EPP

Focuses primarily on prevention. Signature and reputation-based blocking with limited telemetry storage and minimal investigative context.

### XDR

Enables cross-domain correlation based on endpoint telemetry. Aggregates and correlates signals from endpoints, identity providers, SaaS platforms, email, and network sources. Focuses on reconstructing attack chains across multiple systems.

### EDR

Endpoint-focused detection and investigation. Provides detailed telemetry (process trees, command lines, artifacts), retrospective analysis, and host-level response actions. Correlation is primarily limited to data generated by endpoints.

### SIEM

Log aggregation and correlation engine based on rules or behaviors. Data normalization, long-term storage, compliance-related use cases, and configurable detection logic. Detection quality depends largely on log quality, integration level, and rule maturity.



The models are simplified and do not fully reflect market dynamics. The historical evolution from EPP through EDR to XDR shows a shift in emphasis from signature-based prevention to deep telemetry, event correlation, and incident reconstruction. Of course, the protection of workstations and servers remains the unchanging core, but it is the range of data sources, the quality of correlation, and the possibility of multi-system analysis that today determine the real effectiveness of IT environment protection.

## Scope, objectives and limitations of the 2026 edition

The purpose of the test is to evaluate the actual capabilities of EDR-XDR solutions in detecting, recording, and correlating multi-stage attacks under controlled laboratory conditions.

The analysis is not limited to the generation of alerts. The depth of telemetry, the quality of event correlation, the ability to reconstruct the attack chain, and the operational usefulness of data from the perspective of a SOC analyst are also evaluated.

### Methodological assumptions

The test is carried out in a structured environment simulating a realistic attack scenario covering the stages from Initial Access to Exfiltration and Impact, in accordance with selected MITRE ATT&CK techniques.

Each stage is performed in a controlled and repeatable manner, with accurate time recording and predefined expected technical artifacts.

In the first phase, the test can be performed in “report-only” mode to assess visibility and correlation without interrupting the scenario. In subsequent stages, the effectiveness of response and automatic prevention mechanisms can be analyzed.

## What exactly are we evaluating?

The test answers the following questions:

01

Does the solution generate a clear alert for the techniques used?

?

02

Does it provide complete and detailed event telemetry?

?

03

Does it enable correlation of events within a host and between systems?

?

04

Does it allow reconstruction of the attack chain in the logical context of the incident?

?

05

Is the data provided operationally useful from the SOC team's perspective?

?

## Test limitations

The test is conducted in a controlled environment and does not reflect the full complexity of production environments involving hundreds or thousands of endpoints, non-standard configurations, integrations with external systems, and actual load.

The attack scenarios, while realistic, are selected examples and do not cover all possible threat variants.

The results should be interpreted as an assessment of the technical capabilities of the solution under precisely defined test conditions. The test ensures repeatability and comparability of results but does not constitute a complete simulation of a large-scale production environment.



### **The 2026 edition introduces a clear distinction between:**

- ✓ technology detection alone,
- ✓ full telemetry visibility,
- ✓ event correlation,
- ✓ attack chain reconstruction.

In the previous edition, these elements were evaluated together. The updated methodology separates detection effectiveness from the quality of the analytical context and the operational capabilities of the tested solution.

### **The comparison criteria have also been standardized, including:**

- ✓ telemetry completeness,
- ✓ local and inter-host correlation,
- ✓ incident presentation consistency in the console,
- ✓ coverage of tested techniques.

The purpose of the changes is to increase the transparency of the methodology and reduce discretionary elements in the final assessment.

## Certification model



### Level 1 – Core Telemetry Visibility

**CERTIFIED 2026**

Awarded to solutions that provide full technical visibility of events within tested scenarios, including:

- 1 Generation of unambiguous security alerts,
- 2 Access to full telemetry (command-line, process relationships, file and registry changes, user context),
- 3 Consistent and accurate event chronology,
- 4 Automatic correlation of events within a single host.

Level 1 confirms that the solution provides sufficient technical visibility of security events at the host level, including clear alerts, key execution artifacts and contextual information required to analyze an incident within a single system.

### Level 2 – Full Attack Chain Correlation

**GOLD AWARD 2026**

Level 2 is awarded to solutions that, in addition to meeting all Level 1 requirements, demonstrate the capability to automatically correlate events across multiple hosts and reconstruct a multi-stage attack chain within a single logical incident.








Solutions that do not provide basic attack visibility in the tested scenarios do not receive certification.

Certification is a summary of a technical assessment based on a defined methodology and uniform comparative criteria. The level awarded confirms that specific requirements for visibility, telemetry, and event correlation have been met.







## Security features availability

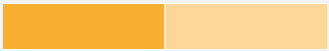
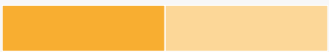
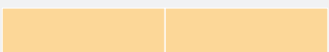
### 1. Detection & Telemetry depth

Basic attack visibility	<b>FULL</b> 
Full attack telemetry	<b>FULL</b> 
Process tree visibility	<b>FULL</b> 
Command-line visibility	<b>FULL</b> 
Network - file - registry telemetry	<b>FULL</b> 
MITRE technique mapping	<b>PARTIAL</b> 
Offline detection capability	<b>FULL</b> 



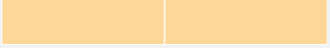

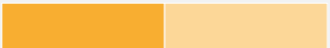

### 2. Event Correlation & Attack Context

Single-host correlation	<b>FULL</b> 
Cross-host correlation	<b>FULL</b> 
Full attack-chain reconstruction	<b>FULL</b> 
Graphical attack visualization	<b>FULL</b> 




### 3. Threat Intelligence & Enrichment

Suspicious object intelligence (IP, URL, SHA)	<b>PARTIAL</b> 
External enrichment (reputation feeds, threat intelligence, VirusTotal-like services)	<b>PARTIAL</b> 
Approximate file reputation scoring	<b>NONE</b> 

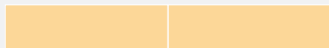

#### 4. Incident Response Capabilities

Workstation isolation	<b>FULL</b> 
File & process containment (quarantine, kill, blocking, isolation)	<b>FULL</b> 
Sandbox or deep file analysis (manual or automated detonation; local or cloud)	<b>NONE</b> 
Proposed remediation guidance	<b>FULL</b> 
Data recovery capability (rollback or backup)	<b>PARTIAL</b> 
Automation or SOAR (native or external)	<b>FULL</b> 





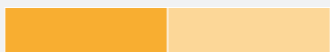
#### 5. Investigation & Hunting

Advanced query capability	<b>FULL</b> 
Raw telemetry access	<b>FULL</b> 
Timeline analysis	<b>FULL</b> 


#### 6. Security Posture & Exposure Visibility

Graphical security posture visualization (vulnerabilities, weak passwords, misconfiguration)	<b>NONE</b> 
Agent configuration validation	<b>FULL</b> 

## 7. Platform & Administrative Controls

Updates management	<b>FULL</b> 
Granular administrative access control	<b>FULL</b> 
Admin console protection (MFA, SSO, audit log)	<b>FULL</b> 
API availability	<b>FULL</b> 
Multi-tenant console for MSSP (multi-company management)	<b>PARTIAL</b> 

## 8. AI-Assisted Operations

AI assistance in console (alert summarization, query generation, recommendations etc.)	<b>FULL</b> 
-------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------

## Agent Configuration and Operating Mode

The test covered EDR-XDR solution operating in a Windows environment, in accordance with a predefined attack scenario and a uniform assessment methodology.

Most of the tested EDR-XDR platforms include an integrated antivirus module. This module remained active so that the environment configuration would reflect a real production deployment that an administrator might use in an organization.

**In the first phase of testing, the solutions could be run in report-only mode, without automatic blocking and remediation. This was done to:**

- ✓ enable full execution of the attack scenario,
- ✓ assess telemetry visibility,
- ✓ analyze the quality of correlation and incident reconstruction,
- ✓ avoid interrupting the attack chain at an early stage.

The configuration of agent policies was based on default settings, with a possible extension of the scope of telemetry collected. For solutions requiring manual policy configuration, settings were used to maximize event visibility and technical artifact logging, while maintaining compliance with the manufacturer's official documentation.

The aim of the study was not to test non-standard experimental configurations, but to evaluate the real capabilities of the platform in a production scenario.

## Environment configuration

The tests were conducted in a controlled virtual environment, including a separate attack infrastructure and victim systems with EDR-XDR agents installed.

### The environment included:

**01**

a separate server simulating the attack infrastructure (Command-and-Control)

**02**

virtual machines running Windows 10 and Windows 11 with the tested agents installed

**03**

optionally, a domain controller (Active Directory) to simulate lateral movement and identity abuse scenarios

The victim systems had a standard operating system configuration with up-to-date security patches and full network access in accordance with the test scenario.

The attack scenarios were carried out using controlled simulation techniques that mirrored selected MITRE ATT&CK techniques. Depending on the test phase, adversary emulation tools and native system mechanisms were used to replicate the attacker's behavior as realistically as possible.

The test did not include social engineering elements (e.g., a real phishing campaign) because the goal was to technically replicate behavior at the host and infrastructure level, not to test user susceptibility to manipulation.

The attacks were carried out in a controlled and repeatable manner, without conducting full campaigns from start to finish. Each stage was performed according to a predefined scenario and documented in terms of expected technical artifacts.



**Attacker Infrastructure**  
(Isolated Zone)



**C2 Server - Kali Linux**  
(Command & Control)



**Attack Tools & Frameworks**

- Atomic Red Team
- Custom Scripts
- Other Simulations



**Payload Delivery**  
(HTTP, SMB, RDP, etc.)



**Internal Network**  
(Lab Environment)



**Active Directory**



**DC - Windows Server**  
EDR/XDR Agent



**Host A - Windows 10**  
EDR/XDR Agent



**Host B - Windows 11**  
EDR/XDR Agent



**Internet Acces**  
(Allowed)

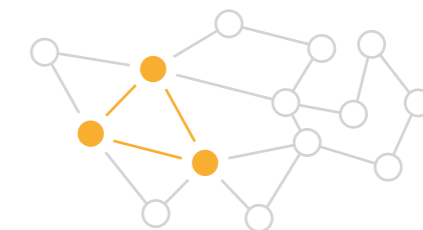


**EDR/XDR Console & Evaluation**



**Central Console**  
(Alerting, Investigation, Hunting)

**MITRE ATTACK Mapping**



**Attack Chain Reconstruction**

**Attack Stages**

Initial Access

Executions

Presistance

Defense Evasion

Credential Access

Lateral Movement

Exfiltration

## Operational Assessment – Phase 1

Settings applied: Telemetry Only (Detect Mode)

Attack Scenario – Adversary Emulation (MITRE ATT&CK via Caldera Framework)

### FULL



The function works in its full scope without significant limitations.

### PARTIAL






The function works, but with noticeable limitations.



### LIMITED



The function is present but provides minimal visibility or analytical value.

Initial Access	T1566.001	Download Macro-Enabled Phishing Attachment	<b>FULL</b> 	Single host	<ul style="list-style-type: none"> <li>✓ Full telemetry visibility</li> <li>✓ Including parent-child relationships</li> <li>✓ Full command-line</li> <li>✓ Graphical visualization</li> <li>✓ Process correlation</li> <li>✓ Attack chain reconstruction possible</li> </ul>
Execution	T1106	Execute process via Win32 API (Process.Start)	<b>FULL</b> 	Single host	<ul style="list-style-type: none"> <li>✓ Full telemetry visibility</li> <li>✓ Including parent-child relationships</li> <li>✓ Full command-line</li> <li>✓ Graphical visualization</li> <li>✓ Process correlation</li> <li>✓ Attack chain reconstruction possible</li> </ul>

<p><b>Persistence</b></p>	<p>T1566.001</p>	<p>Creating persistent access by Scheduled Task after reboot</p>	<p><b>FULL</b></p> 	<p>Single host</p>	<ul style="list-style-type: none"> <li>✓ Full telemetry visibility</li> <li>✓ Including parent-child relationships</li> <li>✓ Full command-line</li> <li>✓ Graphical visualization</li> <li>✓ Process correlation</li> <li>✓ Attack chain reconstruction possible</li> </ul>
<p><b>Defense Evasion</b></p>	<p>T1036.004</p>	<p>Masquerading via scheduled task name (win32times)</p>	<p><b>FULL</b></p> 	<p>Single host</p>	<ul style="list-style-type: none"> <li>✓ Full telemetry visibility</li> <li>✓ Including parent-child relationships</li> <li>✓ Full command-line</li> <li>✓ Graphical visualization</li> <li>✓ Process correlation</li> <li>✓ Attack chain reconstruction possible</li> </ul>
<p><b>Credential Access</b></p>	<p>T1555.004</p>	<p>Enumerate stored credentials (Windows Credential Manager)</p>	<p><b>FULL</b></p> 	<p>Single host</p>	<ul style="list-style-type: none"> <li>✓ Full telemetry visibility</li> <li>✓ Including parent-child relationships</li> <li>✓ Full command-line</li> <li>✓ Graphical visualization</li> <li>✓ Process correlation</li> <li>✓ Attack chain reconstruction possible</li> </ul>

<p><b>Lateral Movement</b></p>	<p>T1021.002</p>	<p>SMB mount, file transfer, and remote execution via PowerShell</p>	<p><b>PARTIAL</b></p> 	<p>Full cross-host</p>	<ul style="list-style-type: none"> <li>✓ Full telemetry visibility</li> <li>✓ Including parent-child relationships</li> <li>✓ Full cross-host correlation recognized</li> <li>✓ Full command-line</li> <li>✓ Graphical visualization</li> <li>✓ Process correlation</li> <li>✓ Attack chain reconstruction possible</li> </ul>
<p><b>Exfiltration</b></p>	<p>T1048.002</p>	<p>Upload file via HTTPS using curl to external service (file.io)</p>	<p><b>FULL</b></p> 	<p>Single host</p>	<ul style="list-style-type: none"> <li>✓ Full telemetry visibility</li> <li>✓ Including parent-child relationships</li> <li>✓ Full command-line</li> <li>✓ Graphical visualization</li> <li>✓ Process correlation</li> <li>✓ Attack chain reconstruction possible</li> <li>✓ Exfiltration &amp; C2 activity visible</li> </ul>

## Operational Assessment – Phase 2

Settings applied: Default

### Methodological assumptions

The results of each attack scenario are interpreted from two operational perspectives: the attacker and the Security Operation Center. This approach helps to determine not only whether the attack was technically successful, but also how clearly it was visible and understandable from the defender's point of view.



### Attacker's perspective

From the attacker's point of view, the key issue is whether the individual techniques were executed according to the planned scenario and whether the chain of attacks could be carried out in whole or in part.

- 1 Was the payload successfully executed?
- 2 Was communication or control of the host established (if applicable)?
- 3 Was it possible to maintain or extend access (e.g., lateral movement or exfiltration)?
- 4 At what stage was the attack chain interrupted if it was stopped by defensive mechanisms?

This perspective helps determine whether the solution actively disrupts the attack or merely logs the activity.



### SOC-Defender

From a security team perspective, the key factors are the quality and completeness of the information presented in the security console and whether the incident can be quickly understood and investigated. From this perspective, we assess:

- 1 Was a clear security alert generated?
- 2 Is there sufficient telemetry data available to analyze the event?
- 3 Were related events automatically correlated?
- 4 Can the attack chain be reconstructed in the context of a single incident?
- 5 Does the analysis require manual correlation of events?

The tables below summarize the operational results of each attack scenario using simplified visual indicators for both perspectives.

## Responding to scenarios from Phase 2

### Custom Attacks Scenarios

**FULL**


The function works in its full scope without significant limitations.

**PARTIAL**


The function works, but with noticeable limitations.

**LIMITED**





The function is present but provides minimal visibility or analytical value.

**NONE**


The function is unavailable or no relevant visibility was observed.

Attack Description	Used tools	Stages	Attack's MITRE ID	Attacker's Perspective	Security Operation Center Perspective	Assessment
Simulation of data retrieval via DNS TXT, reconstruction of the payload in %TEMP%, execution via LOLBin, and exfiltration.	Custom + PowerShell script	<ol style="list-style-type: none"> <li>Initial Access</li> <li>Execution</li> <li>Defense Evasion</li> <li>Command &amp; Control</li> <li>Exfiltration</li> </ol>	T1059.001 T1071.004 T1105 T1218.009 T1036.005 T1564.001 T1041	Downloading DNS chunks, delivering the payload, execution, and successful HTTP communication (status code 200).	<ul style="list-style-type: none"> <li>✓ Blocking of the attack</li> <li>✓ Security alert generated</li> <li>✗ Command-line telemetry available</li> <li>✓ Attack chain visibility</li> <li>✓ Attack reconstruction possibility</li> <li>✓ Graphical processes correlation</li> </ul>	<b>PARTIAL</b> 
Copying the payload between PCs before execution, then running the RAT as an EXE and quietly capturing keystrokes.	DuplexSpy	<ol style="list-style-type: none"> <li>Initial Access</li> <li>Lateral Movement</li> <li>Execution</li> <li>Persistence</li> <li>Credential Access</li> <li>Collection</li> <li>Command and Control</li> <li>Exfiltration</li> </ol>	T1204.002 T1056.001 T1113 T1071.001 T1041 T1547.001 T1082	Execute the RAT as an EXE to quietly capture keystrokes. There are no exploits, it has a low profile and there is periodic exfiltration to C2.	<ul style="list-style-type: none"> <li>✓ Blocking of the attack</li> <li>✓ Security alert generated</li> <li>✓ Command-line telemetry available</li> <li>✓ Attack chain visibility</li> <li>✓ Attack reconstruction possibility</li> <li>✓ Graphical processes correlation</li> <li>✓ Lateral movement visible</li> </ul>	<b>FULL</b> 

Attack Description	Used tools	Stages	Attack's MITRE ID	Attacker's Perspective	Security Operation Center Perspective	Assessment
User downloads ISO, mounts it, and executes EXE, triggering payload and C2 communication (HTTP/mTLS).	Sliver Server	<ol style="list-style-type: none"> <li>Initial Access</li> <li>Execution</li> <li>Defense Evasion</li> <li>Command and Control</li> <li>Lateral Movement</li> <li>Discovery</li> <li>Collection</li> <li>Exfiltration</li> </ol>	<p>T1566.001</p> <p>T1204.002</p> <p>T1036.005</p> <p>T1071.001</p> <p>T1021.002</p> <p>T1041</p>	The attacker delivers ISO, victim mounts it and runs EXE, establishing payload execution and C2.	<ul style="list-style-type: none"> <li>Blocking of the attack</li> <li>Security alert generated</li> <li>Command-line telemetry available</li> <li>Attack chain visibility</li> <li>Attack reconstruction possibility</li> <li>Graphical processes correlation</li> </ul>	FULL
Payload is delivered via WebDAV and executed by the user, establishing C2. The compromise is then extended to another endpoint through SMB file transfer and remote execution via WMI.	Sliver Server	<ol style="list-style-type: none"> <li>Initial Access</li> <li>Execution</li> <li>Command and Control</li> <li>Lateral Movement</li> <li>Exfiltration</li> </ol>	<p>T1105</p> <p>T1204.002</p> <p>T1071.001</p> <p>T1021.002</p> <p>T1047</p> <p>T1041</p>	The attacker delivers payload via WebDAV, gains C2, then uses SMB and WMI to execute payload on another endpoint.	<ul style="list-style-type: none"> <li>Blocking of the attack</li> <li>Security alert generated</li> <li>Command-line telemetry available</li> <li>Attack chain visibility</li> <li>Attack reconstruction possibility</li> <li>Graphical processes correlation</li> </ul>	FULL
The attacker copies the payload to a remote host via SMB and executes it remotely using WMI (Win32_Process), thereby achieving remote code execution.	Custom + PsExec + Atomic Red Team	<ol style="list-style-type: none"> <li>Lateral Movement</li> <li>Execution</li> </ol>	<p>T1021.002</p> <p>T1047</p> <p>T1570</p>	The attacker uses administrator credentials to access the administrative share, transfers the payload to a remote host, and executes it remotely via WMI (Win32_Process), achieving remote code execution.	<ul style="list-style-type: none"> <li>Blocking of the attack</li> <li>Security alert generated</li> <li>Command-line telemetry available</li> <li>Attack chain visibility</li> <li>Attack reconstruction possibility</li> <li>Graphical processes correlation</li> <li>Cross-host correlation</li> </ul>	FULL

Attack Description	Used tools	Stages	Attack's MITRE ID	Attacker's Perspective	Security Operation Center Perspective	Assessment
Using a local LLM model to dynamically select subsequent steps. After verifying SMB connectivity to the target host, remote code is executed via WMI, which creates, compiles, and runs the payload on the victim's system, generating multi-stage process telemetry.	Ollama AI + Custom PowerShell	1. Discovery 2. Execution 3. Lateral movement	T1059.001 T1046 T1021.002 T1047	Collect the host's context and pass it to a local LLM, which selects the most effective lateral movement step. Then use SMB to gain access to the target system and remotely execute code via WMI.	<ul style="list-style-type: none"> <li>✔ Blocking of the attack</li> <li>✔ Security alert generated</li> <li>✔ Command-line telemetry available</li> <li>✔ Attack chain visibility</li> <li>✔ Attack reconstruction possibility</li> <li>✔ Graphical processes correlation</li> <li>✔ Cross-host correlation</li> </ul>	FULL 
The attack uses an external AI model as a decision-making layer to control actions on the host. The script collects system information, saves it to a file, compresses it, and sends it externally via HTTP, while the AI issues subsequent decisions based on the system's state.	OpenAI (API) + PowerShell	1. Reconnaissance 2. Command & Control (AI) 3. Collection 4. Staging 5. Exfiltration	T1082 T1518 T1071.001 T1005 T1560 T1041 T1567	The attacker launches a simple loader that communicates with the AI model and executes its commands. It delegates the analysis of the environment and the selection of actions to LLM, which decides on the next steps based on the data it receives.	<ul style="list-style-type: none"> <li>🔄 Blocking of the attack</li> <li>🔄 Security alert generated</li> <li>✔ Incident generated</li> <li>✔ Command-line telemetry available</li> <li>✔ Attack chain visibility</li> <li>✔ Attack reconstruction possibility</li> <li>✔ Graphical processes correlation</li> </ul>	FULL 
Clicking a phishing link launches mshta, which downloads and executes PowerShell. The script collects system data, establishes persistence via a Scheduled Task, runs rundll32 to hide its activity, and then exfiltrates data over HTTPS (curl). The entire chain uses LOLBIN.	Kali Linux + browser + powershell + schtasks + rundll32 + curl	1. Initial Access 2. Execution (LOLBIN) Execution (PowerShell) 3. Collection 4. Persistence 5. Defense Evasion 6. Execution (LOLBIN) 7. Exfiltration	T1566.002 T1218 T1059.001 T1005 T1053.005 T1036.005 T1218 T1041	I use phishing to launch mshta and bypass standard detection mechanisms. The HTA loads PowerShell in the background, which collects data and maintains access via a Scheduled Task. I use only legitimate system tools (LOLBIN) to minimize detection, and I send the data externally via HTTPS.	<ul style="list-style-type: none"> <li>✔ Blocking of the attack</li> <li>✔ Security alert generated</li> <li>✔ Command-line telemetry available</li> <li>✔ Attack chain visibility (execution stage)</li> <li>✔ Attack reconstruction possibility</li> <li>✔ Graphical processes correlation</li> </ul>	FULL 

## Telemetry, correlation and incident visibility assessment based on Phase 2

The table summarizes the observations derived from all executed attack scenarios in phase 2 and presents the overall assessment of telemetry visibility, event correlation and incident reconstruction capabilities of the evaluated solution.

✓ requirement for obtaining Level 1 or Level 2 Certification

✗ no requirements

### FULL



The function works in its full scope without significant limitations.

### PARTIAL








The function works, but with noticeable limitations.






### LIMITED



The function is present but provides minimal visibility or analytical value.

Attack Description	Required for at least Level 1 Certification	Required for Level 2 Certification	Assessment	Comment
Basic attack visibility	✓	✓	<b>FULL</b> 	Attacks are detected and blocked (AMSI, DeepGuard), and key events are visible in the console.
Full attack telemetry	✗	✗	<b>PARTIAL</b> 	Telemetry is available for many events (processes, command-line, network), but sometimes full RAW data is missing in the event of an early lockup. This is not always sufficient for incident analysis, but it is more a characteristic of WithSecure software than a flaw.
Parent-Child Process Visibility	✓	✓	<b>FULL</b> 	Parent-child relationships are consistently evident in all scenarios allowing for a complete reconstruction of the process tree without any gaps in the chain.

Attack Description	Required for at least Level 1 Certification	Required for Level 2 Certification	Assessment	Comment
Command-line visibility	✓	✓	<b>PARTIAL</b> 	Command-line telemetry is available in most scenarios. However, occasional gaps reduce analytical consistency and may limit full reconstruction of some attack stages.
User context visibility	✓	✓	<b>FULL</b> 	The user context (e.g., LAB\user1, LAB\user2, LAB\Administrator) is consistently displayed in events and allows actions to be attributed to a specific account.
Timestamp integrity	✓	✓	<b>FULL</b> 	Events have consistent and accurate timestamps, enabling them to be sorted and correlated correctly during incident analysis.
Single-host correlation	✓	✓	<b>FULL</b> 	Events within a single host are effectively correlated (process tree, detections, file operations), enabling the analysis of the attack's progression locally.
Cross-host correlation	✗	✓	<b>PARTIAL</b> 	Visible lateral movement, along with identification of the source host and correlation of events across systems, enabling full correlation between hosts.

Attack Description	Required for at least Level 1 Certification	Required for Level 2 Certification	Assessment	Comment
Network telemetry	✘	✘	<b>FULL</b> 	Visible network telemetry (C2 connections, APIs, webhook.site, SMB/WMI), including IP addresses, ports, and traffic direction, enabling communication analysis.
File & registry telemetry	✘	✘	<b>FULL</b> 	Detailed telemetry of file operations (create, modify, execute, delete) is displayed along with the process context, enabling analysis of the artifacts used in the attack.
Remediation guidance	✘	✘	<b>PARTIAL</b> 	The available response actions (isolate device, scan, collect forensics, enumerate tasks/processes) are operational in nature rather than contextual recommendations for full remediation, which requires further manual analysis.
Graphical attack visualization	✘	✘	<b>FULL</b> 	A graphical representation of the process tree and the relationships between events, enabling a quick understanding of the attack sequence.
Advanced query capability	✘	✘	<b>PARTIAL</b> 	Event filtering and search capabilities are available, but there is no advanced, flexible query language comparable to KQL or SPL, which limits advanced threat hunting and large-scale investigations.

## Test conclusions

WithSecure provided broad visibility across the tested attack scenarios, including fileless execution, lateral movement, AI-assisted activity, remote execution, and data exfiltration. The solution consistently exposed process relationships, command-line activity, user context, network communication, and host-to-host interactions, enabling analysts to follow attack progression and understand the sequence of events.

Particularly strong results were observed in scenarios involving WMI and SMB-based lateral movement, where the platform identified both the originating and target hosts while maintaining visibility into the associated process activity. Event correlation and attack reconstruction were generally straightforward, supported by graphical process relationships and MITRE ATT&CK mappings.

The solution also demonstrated good visibility into reconnaissance, collection, staging, and exfiltration activities. Communication with external services, including AI platforms and data exfiltration endpoints, was visible through network telemetry and associated process context. In several scenarios, the platform generated detections that highlighted suspicious behavioral patterns rather than relying solely on static malware classification.

The primary limitation observed during testing concerned telemetry consistency. While telemetry was generally comprehensive, command-line visibility was not available in every scenario, and access to lower-level forensic details was occasionally reduced when threats were blocked at an early stage. These limitations affected analytical depth rather than overall visibility.

From an operational perspective, WithSecure combines prevention, investigation, and response capabilities within a single workflow. Features such as host isolation, forensic collection, device scanning, and cross-host investigation support incident response activities beyond initial detection.

Overall, the solution delivers strong visibility, effective event correlation, and practical investigative capabilities across a wide range of attack techniques, meeting the requirements of Level 2 – Advanced Visibility & Correlation.

– Detection 2/2: Binary file executed from webdav Info 15.04.2026 06:35:15 U

– Details

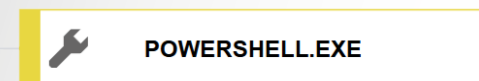
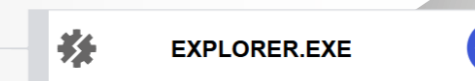
Description	Detected file execution from a WebDav directory and saved temporary with the '%temp%\tfsstore\tfs_dav\{1070ff56-100a-4db5-bf56-6dfcd69702c4}.exe'. The temporary created file under 'tfs_dav' along with the file extension shows what t
MITRE ATT&CK ID	<a href="#">T1218.007</a> <a href="#">T1071.001</a>
Event ID(s)	<a href="#">803b5ff6-3895-11f1-8bb7-0242ac11001f</a>

– Activity context

– File access

**cmd.exe** ⓘ

Username	LAB\td
Command line	cmd.exe /C vaultcmd /listcreds:"Windows Credentials"
Path	%systemroot%\system32
PID	1744
SHA1	<a href="#">e59c13fdd74e1ad950c98f905795ecdefffb8221</a> ⓘ
Execution start	14.04.2026 12:56:40 UTC+00:00
Execution end ⓘ	14.04.2026 12:56:40 UTC+00:00





To learn more about the collaboration, please visit the Attack Visibility in EDR-XDR Telemetry page, where you can also track the results of recent editions.

[CHECK OUR WEBSITE](#)

We also conduct tests of other types:



### Advanced In-The-Wild Malware Test

We evaluate the effectiveness of protection software against threats in the wild, and reveal the true ability of the product to neutralize threats.



### Test of modules to protect online banking

Antivirus solutions are subjected to scenarios of payment details theft, information manipulation by banking Trojans and other malware.



### Cyber Transparency Audit

We verify information from Endpoint Protection software vendors for compliance with specific standards and the idea of transparency.

For more information, please visit our website...



**The AVLab Cybersecurity Foundation** is an independent organization dedicated to protecting privacy and security on the Internet. We are a member of AMTSO (Anti-Malware Testing Standards Organization), which works to improve the transparency, objectivity and quality of testing. Also, we are a member of MVI (Microsoft Virus Initiative) in this matter as well.

We build awareness of users in the field of digital protection. We issue opinions, technical analysis and tests of IT solutions in the field of cybersecurity. Our strongest assets include thorough and detailed reviews, preparation of reports related to privacy and endpoint protection, and in particular, security tests that make us recognizable all over the world as one of the most trusted and popular testing laboratories.

To learn more about other opportunities for cooperation, please refer to our full offer and contact us: [kontakt@avlab.pl](mailto:kontakt@avlab.pl)



[www.avlab.pl](http://www.avlab.pl)