Elevate to WithSecure™

Service Description -
WithSecure™ Elevate

February
2023

Contents

1 Overview

This document describes the services that are provided when you use ‘Elevate to WithSecure™’ to escalate a potential cyber security incident to WithSecure™ for further analysis.

In short, ‘Elevate to WithSecure™’ is an on-demand service that focuses on analyzing technical evidence related to ‘Broad Context Detections’, which is later referred to as ‘Detections’, provided by WithSecure™ Elements EDR.

1.1 Elevate to WithSecure™

Detecting and responding appropriately to the techniques, tools, and processes used by more sophisticated threat actors often requires advanced threat analysis and guidance provided by a specialized cyber security expert.

For these advanced requirements, customers using WithSecure™ Elements EDR can take advantage of the built-in ‘Elevate to WithSecure™’ service.

‘Elevate to WithSecure™’ offers professional, on-demand incident analysis for ‘Broad Context Detections’, referred to generally as ‘Detections’, provided by WithSecure™ Elements EDR. Based on this analysis, a specialized cyber security expert will provide expert advice and further response guidance based on the techniques, tooling, and processes used by the threat actor.

If your company’s risk profile indicates a high likelihood of a serious cyber security incident, we recommend that you complement the ‘Elevate to WithSecure™’ service with our ‘Incident Response’ and ‘Incident Readiness’ services. These services are briefly described at the end of this document and must be acquired separately.

1.2 Elevation Process

When the person managing Elements EDR triggers an escalation of a detection to WithSecure™ by using the ‘Elevate to WithSecure™’ functionality, the Elevate process begins with a ‘Threat Validation’ phase, during which the nature of the detection is validated. Most cases will be resolved during this phase.

If the detection is validated as serious or a genuine attack in this phase, the person managing the Elements EDR can request moving the detection to an optional ‘Threat Investigation’ phase. During this phase, the detection is thoroughly investigated, and concrete suggestions are provided on how to respond to it.

If the ‘Threat Investigation’ phase determines that a 'Major Incident Threshold’ is met, the specialized cyber security expert from WithSecure™ will advise an official escalation to a separate, full-blown ‘Incident Response’ process to further investigate and contain the attack and to minimize the damage done by the threat actor.

1.2.1 Threat Validation

In the ***'Threat Validation'*** phase, WithSecure™ analysts determine the nature of the detection, categorizing it to the four general categories described below, and clarifying to the person managing the 'WithSecure™ Elements EDR' the reason for the categorization.

For proper validation and categorization, a dialogue between a WithSecure™ analyst and the person managing the 'WithSecure™ Elements EDR' is required, which will take place via the Elements Security Center from which the elevation was initially triggered.

Open dialogue and background information help WithSecure™ analysts provide quicker validation results. For example: describing the reason for the Elevation, what piece of information is problematic, and anything specific that the expert needs to validate.

Based on the technical investigation and the dialogue with the escalator, the detection is categorized into one of the following categories:

1. a genuine threat,
2. suspicious activity that should be acted upon,
3. suspicious activity that can be accepted as a risky behavior in the target environment, or
4. a false positive

If the detection is confirmed as a genuine threat, a WithSecure™ analyst will explain the findings and provide guidance on how to react, along with a breakdown of the investigation to this point.

If the detection looks suspicious, the WithSecure™ analyst may recommend additional checks and verifications to understand the background of the detection. Based on these recommendations, the next steps can either be managed independently, or an optional 'Threat Investigation' request can be submitted.

A False Positive is a detection that is purely technically false in nature due to some unforeseen impact of tweaking or updating detection rules, which would flag a benign standard activity as malicious.

A Detection that arises from suspicious activity conducted by a legitimate internal user of the customer is not considered a False Positive. Detecting, alerting, and investigating suspicious activity, whether done by external or internal actors, whether it is legitimate or malicious activity, warrants investigation and validation - the very purpose of the service.

1.2.2 Threat Investigation

If the validation was not enough, or the detection is considered a genuine threat, the customer can request an optional ***‘Threat Investigation’*** phase.

In this stage, The WithSecure™ analysts will conduct further and deeper analysis of the detection. The focus is on analyzing:

1. anomalies, spikes, dips and patterns found in the telemetry of assets and their network connections,
2. data provided by the detection itself, such as abnormal activity of standard programs, running unexpected scripts, and unexpected running of system tools from standard processes,
3. and finally, cross-referencing the telemetry and detection data against the threat intelligence we are seeing globally in our detections and incident response operations

Once the WithSecure™ analyst has determined what type of threat or breach they are dealing with, they will explain the findings to the escalator, along with a breakdown of the investigation to this point.

Additionally, in case of a genuine, ongoing attack, the analyst will suggest steps to stop the breach from doing further damage to the target environment. The primary focus is on short-term containment measures that prevent the current threat from spreading, such as isolating the affected systems or by taking infected devices offline.

This will close the ***‘Threat Investigation’*** phase, providing the results of the deeper investigation and concrete response actions to mitigate the threat.

If the severity of the Elevate case reaches the ***‘Major Incident Threshold’***, or the escalator unable remediate the incident independently, WithSecure™ analysts will recommend escalation to a separate, full-blown ‘Incident Response’ process to further contain and remediate threats in the target environment.

The incident response process is not covered by the Elevate to WithSecure™ service and must be acquired separately. See Section 5, Complementary Services, for further information and the conditions for reaching the ‘Major Incident Threshold’.

2 Service availability

To make use of the service, the following prerequisites must be met:

- Valid WithSecure™ Elements EDR subscription
- Deployed WithSecure™ Elements Agent(s)
- Valid Elevate to WithSecure™ add-on subscription
- Access to WithSecure™ Elements Management Console

2.1 Service Hours

WithSecure™ Elevate service is available 24/7/365. Our target time for starting the threat validation phase is within 2 hours of when the Elevate request was made. Once the validation is complete, you will see the results immediately in your WithSecure™ Elements Security Center.

2.2 Service Language

Elevate to WithSecure™ is available in English only.

3 Data collection & retention

To elevate detections, a WithSecure™ Elements EDR Agent must be installed on at least one device. These agents are installed on devices designated by the customer on their network to detect and preserve evidence about security anomalies. The agent sends data to WithSecure™ for analysis.

The WithSecure™ Elements EDR Agent collects event-based data of the following types from the device on which it is installed. This data is referred to later as 'Event Data':

- technical user identifiers
- domain names and network connections
- metadata of process creation, behavior, and access to various systems and subsystems

Additionally, the agent collects information on applications installed on the devices where the sensor is installed, as well as system/network information and other metrics.

The collected data is stored in identifiable form for as long as it remains useful for processing, up to the duration of the customer's engagement with WithSecure™ Elements EDR. As of the time of writing, data is stored for one (1) year on a rolling basis during the customer engagement, and is deleted within two (2) months after the termination of engagement. Manually collected data is stored for three (3) months on a rolling basis.

For full details, refer to WithSecure™ EDR Privacy Policy Document in www.withsecure.com

Learn more

4 Licensing

WithSecure™ Elevate is licensed through two types of 'Tokens': one for 'Threat Validations' and one for 'Threat Investigations'.

These tokens are offered in pre-packaged combinations that vary in size, for example 2/1. In this example, the license would contain 2 Validation Tokens for 1 Investigation Token.

The tokens have varying validity periods that match the WithSecure™ Elements EDR subscription validity period (12, 24 or 36 months). Unused tokens will expire after the validity period is over.

If the detection under scrutiny is more than 7 days old, an Investigation Token is used for Elevation. Otherwise, the elevated detection is first validated using a Validation Token.

For more information about the WithSecure™ Elevate licensing, or the separately available Incident Response and Incident Readiness services, contact your local WithSecure™ representative.

5 Complementary services

If your company's risk profile indicates a high likelihood of a serious cyber security incident, we recommend that you complement the 'Elevate to WithSecure™' service with our 'Incident Response' and 'Incident Readiness' services. These services are briefly described below and must be acquired separately.

5.1 Incident Response

If the severity of the Elevate case hits the 'Major Incident Threshold', WithSecure™ analysts will recommend escalation to a separate, full-blown 'Incident Response' process to contain and remediate threats in the target environment. The Incident Response process is not covered by the Elevate to WithSecure™ service.

The 'Major Incident Threshold' is considered reached when one of the following conditions is met:

- Elevate to WithSecure™ spent exceed 2 hours without expected resolution within the next hour.
- More than five devices have been infected in the target environment
- A business-critical asset has been compromised.
- A compromised device has been identified that does not have Elements EDR coverage.

Incident Response services are provided by the WithSecure™ Global Incident Response team, who operate 24/7 and specialize in major cyber crises, having dealt with live incidents for some of the world's largest organizations (including constituents of the Dow Jones, NASDAQ, and FTSE 100, and government agencies and departments).

Incident Response services follow their own service descriptions and must be procured separately. In some instances, due to the classification of the impacted data, government vetting may also be required, as well as continued reporting to the regulators or customers.

WithSecure™ recommends that clients obtain a WithSecure™ Incident Response Retainer, as this ensures SLAs, commercial coverage for immediate response, and reduced incident response day rates. In scenarios where the customer does not have a retainer, WithSecure™ offers organizations the ability to engage in incident response as a walk-in customer. Walk-in customers experience higher fees than retainer clients and will be serviced per availability, whereas retainer clients have guaranteed support within 72 hours.

5.2 Incident Readiness

Organizations with a strong readiness baseline can minimize the use of reactive incident response, streamline incident response costs, quantify spend, and improve cross-departmental collaboration.

Our readiness activities are used to establish your baseline response capability, including when it is relevant to Elevate detections, before building on this foundation by improving the quality and performance of playbooks, practicing the response to a live incident through simulation exercises, and training security teams to configure tooling correctly.

Incident Readiness Services enable clients to:

- Master first responder skills and understand key risk and incident scenarios.
- Uplift their incident response and business continuity management systems by creation plans, processes, and playbooks.
- Design major incident and crisis management organization and process design.
- Exercise communication and coordination during incident response, major incident, crisis management and disaster recovery response practices.
- Continuously improve by embedding a preparedness culture in their organization.

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.