expel®

Service guide

Version 1.7

www.expel.io

Contents

Overview

Welcome

Thank you for choosing Expel!

Our goal is to measurably improve your security posture over time and to provide answers, not just alerts. We want to make sure your security program is successful and you and your team look like superheroes.

After reading this guide, you should have a clear understanding of how to start using the service to quickly respond to threats and implement changes that will quantifiably reduce risk. If you walk away from this guide with more questions than answers, or just want to chat about what you've read, please don't hesitate to contact us:

E-Mail: soc@expel.io

Phone: 1-844-397-5762

We're a service, not a product, and a service is defined by people and relationships. That's why it's so important to us that we're constantly communicating to make sure we're always aligned with your goals and workflow.

Why we're here

We don't think value is measured by the volume of alerts. Threat detection is important, but it's ultimately a means to answer the following questions:

- What do I need to care about and why?
- How can I be confident nothing is falling through the cracks?
- What tactical response actions do I need to do to right now to get the bad guys out?
- Based on what's impacting me, what strategic resilience actions can I take that will have the largest impact on preventing the bad guys from getting in again?

What to expect

Here are some things you can expect from us:

1. **Transparency** — We're sick of the black-box approach too many security vendors take. Hiding the recipe to the secret sauce doesn't help you (or us). It just chips away at trust and confidence. We've designed the service around transparency, and we hope it shows all the way from our platform to the conversations we have.

2. **Answers** — We're here to help you get better. To do that, we're focused on providing you with answers and actions along with measurements that allow you to quantify your improvement and hold us accountable. After all, we're in this together.

3. **Ease of use** — What good is a service if it doesn't make your life easier? We've spent a lot of time designing an onboarding process that's a cake-walk and an intuitive portal that we call the Expel Workbench™. We pair that with a model that allows you to do as little (or as much) as you want. We'll do the rest. We know it's not perfect, it'll never be. That's why we're also committed to getting your feedback and continually improving the system.

4. **Extension of your team** — We're serious about behaving like members of your own internal security team. We're here to fight in the trenches with you.

Using the service

TL;DR *— Just tell me what I need to do... there's too much text in this doc.*

Perform **Investigative Actions** assigned to you. These tasks provide additional data our analysts can't access (but need) to validate alerts.

Respond to **Incidents** by following the detailed Remediation Actions.

Implement **Resilience Actions** to prevent threats from occurring again and enable our teams to respond to threats more effectively.

Getting set up

We know setting up a new technology can be a pain, which is why we've made significant investments in making our onboarding process as quick and easy as possible.

Here's what we need you to do so we can get started:

1. **Install the Expel Assembler** — You'll need to install a virtual appliance called the Expel Assembler. It collects, normalizes, and sends security alerts to us. This is the only piece of technology you need to deploy in your environment.
2. **Provide Console Access** — Expel needs console access to your supported security technologies so we can have a similar view of your environment as your team. This view allows us to accurately investigate potential security concerns impacting your organization.
3. **Hook up the APIs** — The last step required for onboarding is to make sure the Assembler can pull alerts from your vendor technologies. To do this, you'll need to create an API key on your supported technology and enter it in the Expel Workbench. That's it!

   Want some help with this step? No problem! Your engagement manager can do this step for you, assuming we have the right access to the technology. Just let us know.

You can access the **Getting Started with Expel** guide that includes everything you'll need to install the Expel Assembler on the Customers page of our website at https://www.expel.io/for-customers/.

Remember, you're not alone! Your engagement manager, and the rest of the Expel team is here to help. Please reach out if you hit any roadblocks or want to chat about the process.

Once the Expel Assembler is up and running, we'll confirm that everything looks good or reach out to troubleshoot any problems that may arise.

The Expel Workbench

The Expel Workbench is a shared platform that both our teams use together. It's designed to allow you to see everything we see, including alerts we're triaging and investigative actions our analysts are performing. The service was built this way not only to promote transparency, but also to allow you to decide how much (or how little) you'd like to participate in the analysis work.

Want us to do pretty much everything and just tell you what you need to care about? You got it! The Situation Report page will be your go-to. On the other hand, maybe you want to ride shotgun with our analysts and see everything they're doing? Perhaps you even want to participate in the investigative actions here and there? Hey, why not? Knock yourselves out! Dive into Alerts and Activity tabs.

Below, you'll find more info on the different parts of the Expel Workbench. This information will help guide you and your team no matter how you want to use the service.

The *Situation Report* page

The Situation Report is your landing page. The goal of this page is to give you an overview of what's happening in your environment and what you need to do about it (if anything). Here are some specific items you'll find on this page and what they mean for you:

1. **Investigations** — Investigations occur when an analyst needs to analyze additional data to assess a potential threat. A lead investigator is assigned to each Investigation. This is the analyst who is ultimately responsible for coordinating the investigation and determining if the activity they're investigating represents an actionable security concern and therefore an incident.
2. **Investigative Actions** — Each investigation contains individual investigative actions assigned by the lead investigator. These investigative actions could be assigned to an Expel analyst or a member of your own internal team. Some of these tasks are automated, like when you see "Job Running," but others require manual action from your team or ours.
3. **Incidents** — These represent actionable security concerns in your environment that our analysts have identified. Incidents require you and your team to respond. But don't worry, each incident includes detailed information on how to address the threat. Incidents come in two severities:
    a. **Incident** — An incident represents an actionable security concern within your environment. This type of activity is typically associated with non-targeted commodity malware.

b. **Critical Incident** — Critical incidents represent an actionable security concern that Expel believes has or will result in significant impact to your organization. Critical incidents can be either targeted or non-targeted in nature, but all targeted activity will result in a Critical incident.

Targeted incidents typically represent attacks that include spear-phishing, customizable and difficult to detect malware and interactive "hands-on-keyboard" attacker activity. Non-targeted incidents are opportunistic attacks which are not specific to your organization. Commodity malware activity is most commonly associated with these types of attacks. Non-targeted incidents are typically not critical, but can be depending on the potential impact to your organization.

4. **Remediation Actions** — Once we identify a security incident, the remediation work can begin. Remediation actions are tasks assigned to your team to resolve specific incidents. These tasks provide your team with clear, detailed instructions on how to quickly respond to an active threat.

5. **Resilience** — The Resilience tab includes proactive recommendations to protect your organization based on both threats Expel detects within your environment as well as your overall security posture and settings. Unlike remediation actions, which are tactical actions to resolve an incident, resilience recommendations are strategic actions or policies you can implement to prevent threats from occurring in the future (Disrupt Attackers), or enable both of our teams to respond to active threats more effectively (Enable Defenders).

The *Alerts* page

The Alerts page contains all the security alerts for your organization that currently require analysis, are actively being analyzed, or have already been analyzed. Depending on what's discovered, each alert, or group of alerts, could result in an incident that requires your attention.

If you rely on Expel to analyze all alerts within your environment, then you don't have to do anything on the Alerts page. In fact, you can ignore Alerts entirely, unless you're just curious about what our analysts are up to at any given moment. If, on the other hand, you want members of your team to participate in analysis, we can coordinate these efforts between your team and ours using the alert management workflow in the Expel Workbench.

The *Activity* page

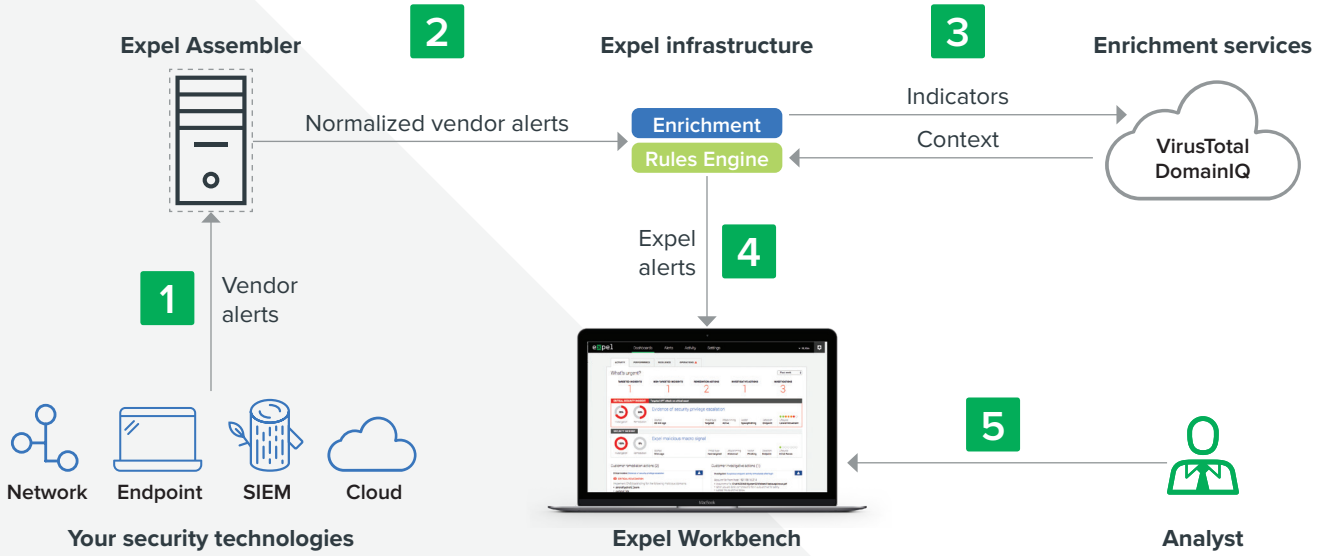
The Activity page contains more detailed information about security incidents, actions and investigations that require attention, are currently being worked on, or have already been resolved. You can think of the Situation Report page as a snapshot of what's currently happening in your environment and the Activity page as an in-depth and historical review.

How the service works

Our service improves your security posture over time. To do this, it's essential we tune the flow of security events from your existing security devices (we call these "vendor alerts"). This tuning process takes place primarily at the beginning of service delivery. It's basically a set of detection rules specific to your organization which are stored in our rules engine.

Once you've completed onboarding, you have no obligations other than responding to notifications our system sends about malicious activity we've identified in your environment or recommendations for strategic resilience improvements. Nevertheless, we thought it would be useful to give you a look under the hood. While we're popping the hood open, this is still a pretty high-level overview, so please don't hesitate to reach out if you have additional questions.

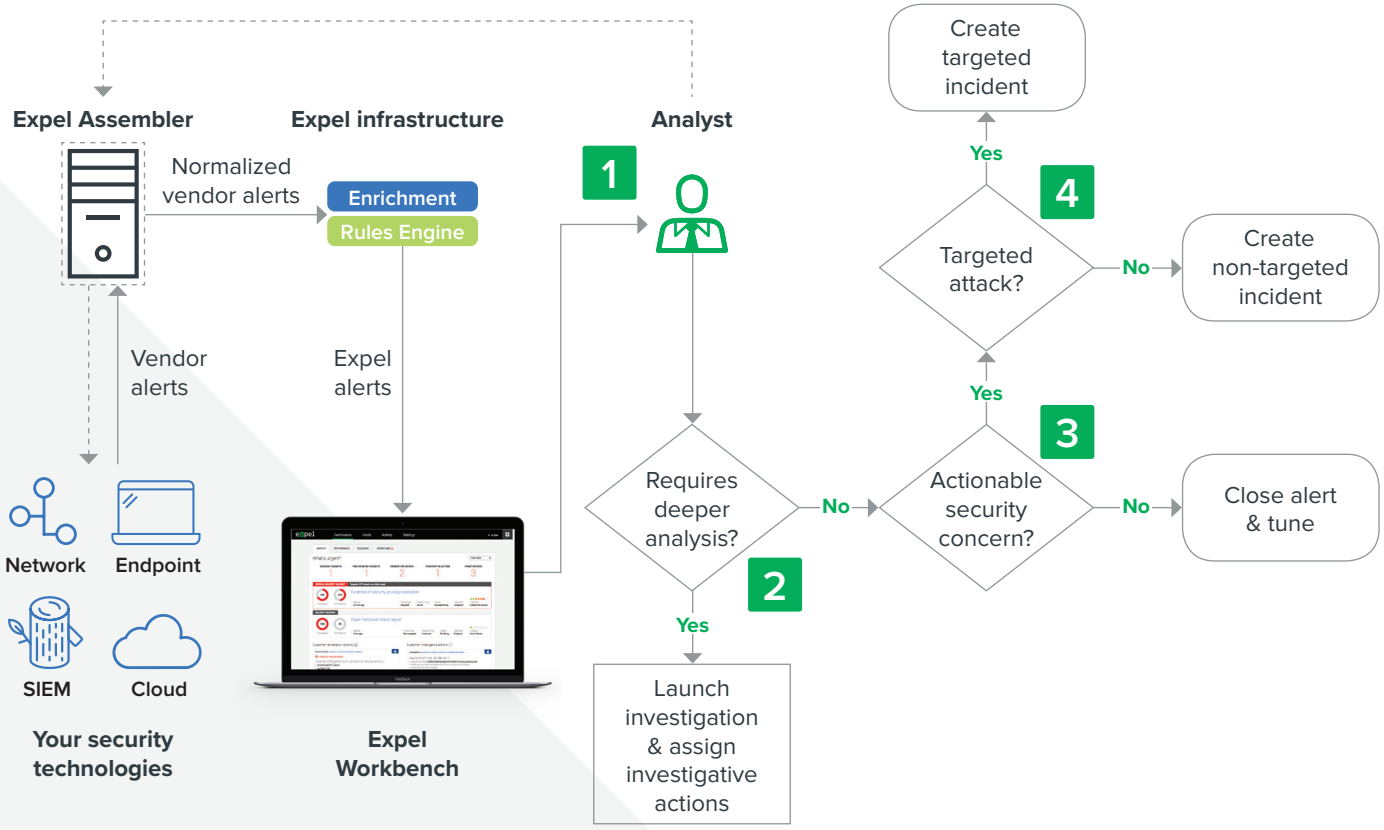
Alert dataflow



1. The Expel Assembler pulls vendor alerts from your monitored security technologies.
2. It then parses, normalizes, and sends your alerts to us via a secure VPN tunnel.
3. We "enrich" these alerts with additional context from third-parties or our own historical data sources. These might include cross referencing traditional IPs, domains, and file hashes.
4. The contextualized alerts are then sent to our rules engine. Here we improve the signal-to-noise ratio by applying analytic and correlation rules to identify potentially malicious activity.
5. If the rules engine identifies potentially malicious activity, it groups and correlates the vendor alerts into a single Expel alert and sends it to the Expel Workbench for human analysis.

Threat detection and investigation methodology

"Human analysis," sounds like a simple step, but this is where the rubber meets the road. Security analysis is part art and part science — and as methodologies mature, we're equipped to codify them in our rules engine and the surrounding automation framework that's baked into the Expel Workbench. This enables our Expel analysts to spend more time on higher-order, more valuable analysis activities.



Here's how our analysts drive detection through investigation:

1. The analyst opens an Expel alert using the Expel Workbench.
2. If we require additional help or data to validate a security concern, we'll launch an investigation and assign individual investigative actions to members of your team or ours. This might include pulling a process listing off a particular host, or running a SIEM query to identify other machines that connected to a suspicious server. Whenever we can, we'll attempt to pull the data ourselves by connecting directly to your security technologies. This connection transits the Assembler via VPN tunnel.
3. If we determine that an Expel alert does not represent an actionable security concern, we'll add details of our analysis, close the alert, and tune the activity so it doesn't occur again (if appropriate).
4. On the other hand, if the Expel alert represents a legitimate threat, we'll create an incident and include details based on our analysis. Likewise, we'll create a targeted incident if we find evidence of a targeted attack.

Threat hunting service

Expel constantly reviews alerts coming from your security technologies, kicks off investigations, and, when we identify an incident, provides you with a holistic story around what happened, how it happened, and recommended next steps. But what about threat activity that your security technologies missed? That's where hunting comes into play.

Hunting is an additional service that goes beyond investigating the alerts received from your security technology. To hunt, Expel analysts pull large sets of data from your environment and apply various hunting methodologies to identify malicious behavior. Our hunting methodologies align with the adversarial techniques described in the MITRE ATT&CK Matrix.

Below is how Expel analysts hunt in your environment:

1. At the start of your service, we work with you to map our library of techniques to your environment.
2. Hunting sessions occur every month. During that time, data is collected by Expel from your network, endpoint and/or SIEM technologies, depending on the technique being applied.
3. An investigation is created with the data set that requires further review from an analyst (this investigation is available to you even before it's completed).
4. The analyst reviews the data and documents their work within the investigation.
5. If malicious activity is identified during review of the data, an incident will immediately be created, and you'll be notified.
6. Once the hunt is complete, Expel analysts use the knowledge they've gained about your environment to tune the technique for next time. If possible, the analyst will also create a new detection in our rules engine to generate an alert immediately next time the activity occurs.

Expel services availability and continuity

Service availability

Expel commits to a 99.95% availability of our portal as stated in our contract.

If changes require a partial or complete service outage, customers will be notified 7 days prior to these scheduled outages. In some instances, we may be required to perform emergency maintenance. In those cases, we'll notify you within one hour prior to performing the maintenance.

Customers can view historic performance, as well as subscribe to receive downtime notifications, by visiting the Expel Status page.

How we calculate Service Availability:

With respect to any calendar month, the difference between total monthly time and unscheduled downtime, divided by the total monthly time. Represented algebraically, service availability for any calendar month is determined as follows:

$$\text{Service availability} = \frac{\text{Total monthly time} - \text{Unscheduled downtime}}{\text{Total monthly time}}$$

Where total monthly time is the amount of time, measured in minutes, in a given month.

For example: If, in the month of October, the service experiences 15 minutes of unscheduled downtime and 45 minutes of scheduled downtime. The Service Availability would be as follows:

$$99.96\% = \frac{((31 \text{ days} * 24 \text{ hours} * 60 \text{ minutes}) - 45 \text{ minutes}) - 18 \text{ minutes}}{(31 \text{ days} * 24 \text{ hours} * 60 \text{ minutes}) - 45 \text{ minutes})}$$

Expel business continuity and disaster recovery

Expel has a documented disaster recovery plan and conducts annual testing exercises to test this plan. During this annual exercise, Expel validates its triggers, verification, incident handling, implementation and failback procedures.

Our security operations center (SOC) has a primary link to our data center location in North America with a

secondary link available if required. Should our SOC experience a failure impacting service delivery we have the ability to failover to remote work. In the event of an extended SOC closure, Expel has the ability to set up operations in another location and resume service delivery.

Feedback

We've said it before, and we'll say it again: we thrive on feedback in all forms. Please don't hesitate to reach out with questions or concerns. We look forward to working with you and constantly improving together.

© Expel, Inc.