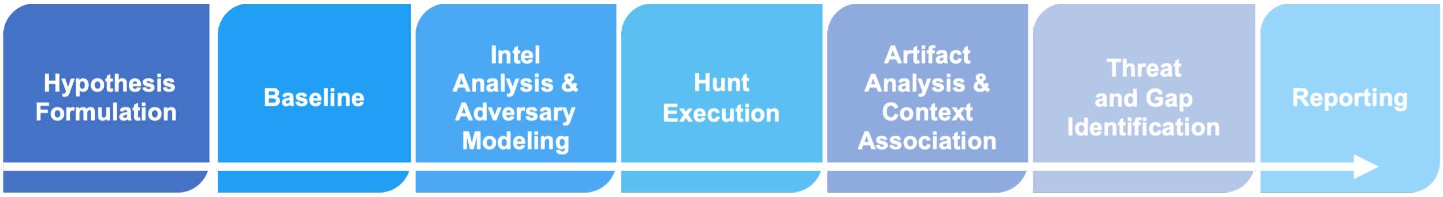
Forescout Frontline Service Description

Forescout Frontline is a team of cybersecurity analysts with a proven history of defensive cyber operations that provides **threat hunting and risk identification services** as well as **incident response services** for both customers and non-customers. During the 1 – 3 day engagement, your Frontline team will follow the methodologies described here.

Threat Hunting Methodology

There are many threat hunting methodologies out there, but the objective is always the same: understand what is happening across your digital terrain, identify undesirable behavior and prioritize risk response.

A typical Forescout Frontline threat hunting process looks like this:



Hypothesis Formulation

Baseline

Intel Analysis & Adversary Modeling

Hunt Execution

Artifact Analysis & Context Association

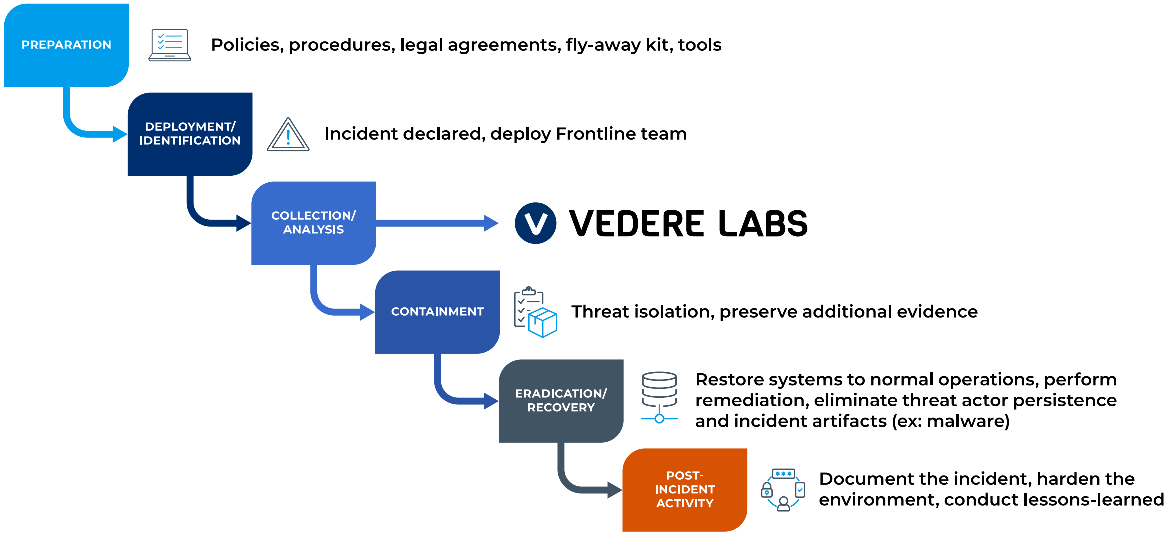
Threat and Gap Identification

Reporting

- **Hypothesis formulation** – The Frontline team will work with you to create an actionable and testable hypothesis, so operators and analysts have a starting point for further investigation.
- **Baseline** – A network baseline serves as a reference point or historical metric to compare with performance throughout the engagement. To allow for easier detection of anomalies and faster response, operators and analysts must understand the environment they are in and what is considered normal, and to have a reference to a “known good state.”
- **Intel analysis and adversary modeling** – Proper intel allows for targeted hunting and faster response and mitigation. During intel analysis, data and information on a potential threat actor are collected from various sources to predict behaviors and any possible threats they may pose. Adversary modeling is the technique of identifying threat actors.
- **Hunt execution** – Using eyeInspect and other Forescout tools, the team discovers artifacts and investigates anomalous and malicious behavior based on intel analysis, deviations from the baseline or in support of the formulated hypothesis.
- **Artifact analysis and context association** – Artifact analysis may include malware sandboxing, reverse engineering, log analysis and string extraction. Context association involves identifying the overall attack chain of a threat actor, which helps to expose gaps within the hunt or investigation.
- **Threat identification and gap hunting** – The Frontline team will draw conclusions based on evidence supporting the original hypotheses. If that hypothesis cannot be proven, we will hunt for gaps (Are we missing a piece of the story? Was the intel provided accurate and actionable?) and restart the threat hunting process in pursuit of a new hypothesis.
- **Reporting** – You will receive a report outlining findings and threats. Typically, mitigation planning begins here as system owners and key stakeholders become involved.

frontline@forescout.com

Incident Response Methodology


PREPARATION
Policies, procedures, legal agreements, fly-away kit, tools
DEPLOYMENT/ IDENTIFICATION
Incident declared, deploy Frontline team
COLLECTION/ ANALYSIS
VEDERE LABS
CONTAINMENT
Threat isolation, preserve additional evidence
ERADICATION/ RECOVERY
Restore systems to normal operations, perform remediation, eliminate threat actor persistence and incident artifacts (ex: malware)
POST-INCIDENT ACTIVITY
Document the incident, harden the environment, conduct lessons-learned

Forescout Frontline's incident response service follows a standard six-step process. Here is an overview of the major actions performed during response and analysis:

- **Preparation** – The Frontline team prepares for incidents before they occur. This phase aims to establish a formal approach to responding to incidents, document policies and procedures, produce legal agreements and confirm the operational status of fly-away kits and required tools.
- **Deployment and identification** – The Frontline team is prepared to rapidly deploy worldwide, when and where needed.
- **Collection analysis** – Frontline members will collect and preserve pertinent data for evidence, analysis and investigation to expedite remediation, recovery and release of information to the public, where appropriate. We will also provide mitigation steps that you can implement to protect yourself.

Vedere Labs performs technical analysis on evidence provided by the Frontline team. Deliverables include threat briefings, indicators of compromise (IOCs), common vulnerabilities and exposures (CVEs), affected software and mitigation recommendations.

- **Containment** – The Frontline team will work closely with you to make an informed decision, choose an appropriate containment strategy and assist in performing the actions needed to prevent further damage to a network or other systems.
- **Eradication and recovery** – We will ensure that threat actor persistence and incident artifacts are eliminated, and appropriate remediation techniques are completed so you can resume normal operations.
- **Post-incident activity** – All incidents are thoroughly documented by our team to facilitate learning, provide incident closure and help to improve existing procedures and capabilities.

At the end of the engagement, you'll have the right information to create an actionable plan for efficiently and effectively addressing each area of risk covered in the report.

Interested? Contact Forescout Frontline

Achieve a baseline of your organization-wide threat landscape across all networks and device types. Email frontline@forescout.com to book your complimentary Threat Hunting and Risk Identification Service*

* This risk identification service is not intended to find and report on an exhaustive list of all possible threats, vulnerabilities or risk mitigation suggestions, and the information provided in the report is "as-is" without warranty of any kind, whether expressed, implied, statutory or otherwise.

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com