IntelFinder and ThreatConnect

Threat Intelligence Playbook

IntelFinder

+

ThreatConnect™

Overview

IntelFinder is a fully automated and scalable service for customer-specific and actionable threat intelligence. The unique automated design enables IntelFinder to provide a comprehensive all-inclusive intelligence service at a fraction of the cost compared to existing services on the market. IntelFinder performs on-going monitoring to identify a wide variety of potential threats that exist outside of its users' perimeters, providing detailed and easy-to-understand alerts on identified threats.

With IntelFinder, ThreatConnect Platform users can receive IntelFinder intelligence reports within the platform, enabling them to easily consume intelligence that is not normally available on Threat Intelligence Platforms.
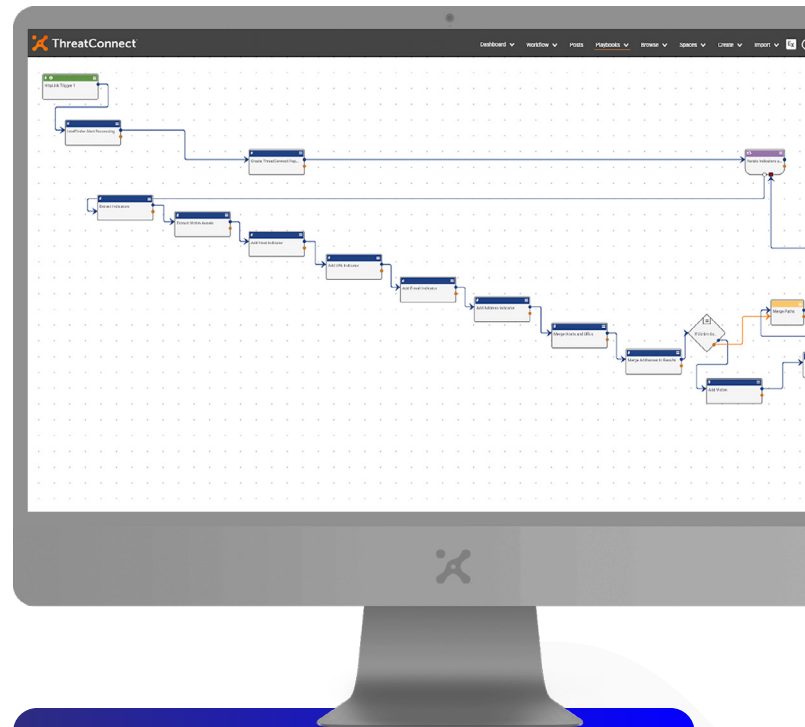
❗ The Challenge

Organizations face a wide variety of external threats, from malicious attacks to non-malicious insider threats. While visibility to events taking place outside of an organization's perimeter can provide valuable intelligence, existing solutions on the market are designed mainly for large enterprise users, making them inaccessible to many. A high price point and a design with large security teams in mind result in a costly and complex integration for teams that wish to gain such visibility.

✓ The Solution

IntelFinder Alerts for ThreatConnect enables security teams to expand their intelligence collection to include many types of threats, all within the ThreatConnect Platform. Users can receive reports on a variety of external threats, such as similar domain registration, leaked employee credentials, exposed internal subdomains, leaked source code, leaked internal documents, and more.

Key Features

- **A Holistic Approach to Threat Intelligence** – IntelFinder's monitoring does not focus on a specific type of threat but provides a wide coverage of different types, including malicious and non–malicious ones.

- **Detailed Intelligence Reports** – IntelFinder reports are available within the ThreatConnect Platform including detailed descriptions of the findings, providing clarity and context.
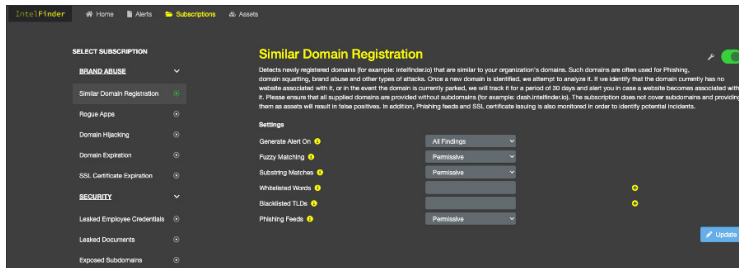
- **Mitigation Recommendations** – Every report is provided with specific mitigation recommendations, enabling organizations to easily act on discovered threats.

- **Indicators Extraction** – Indicators and victim assets are automatically extracted, enabling ThreatConnect Platform to quickly perform further analysis.

- **Easy Setup and Maintenance** – The IntelFinder dashboard enables easy setup and maintenance of the monitoring activities, designed with users with any security background in mind.

- **Low Barrier of Entry** – IntelFinder is provided at a fraction of the cost compared to existing comparable threat intelligence services.

The IntelFinder and ThreatConnect Advantage

IntelFinder provides visibility into a variety of threats that are not normally available on Threat Intelligence Platforms. Together with ThreatConnect, users can receive reports on such external threats within the platform and triage this information.

IntelFinder Alerts leverages ThreatConnect Playbooks for processing, allowing users to customize the behavior for the alerts received. A default Playbook template is provided as a basis for getting started. Users can customize this template to perform actions such as sending notifications via Slack, automatically deploying indicators to a blocking solution, or enriching and pivoting on information learned about indicators. ThreatConnect Playbooks allows maximum flexibility in handling these alerts.

About IntelFinder

IntelFinder is the world's first fully automated and scalable SaaS–based solution for customer–specific and actionable threat intelligence. IntelFinder's goal is to make threat intelligence accessible and relevant to all organizations. To that end, it provides a full, comprehensive, all–inclusive threat intelligence solution for as low as $250 a month per brand. Founded by a "Legends of Fraud" award–winning industry veteran and elite military intelligence experts, IntelFinder brings more than 15 years of experience building industry–leading intelligence operations, delivering insights to the world's largest companies and government agencies. Visit **www.intelfinder.io**