REDLEGG

THREAT INTELLIGENCE SERVICE

Service Description

While threat intelligence feeds and platforms introduce new data into a SIEM, EDR solution, or other technical controls, without the expertise to correctly operationalize the data, this new information is simply excess noise. When you purchase a third-party feed or platform, you are purchasing additional contextual information about potential activity in your network.

To be truly effective, you must take that contextual information and successfully implement it into a platform. To put it to work, you will need to build alarms and rules around the ingested threat intelligence, and properly tune the rules. RedLegg's Threat Intelligence Service not only provides your organization with a threat intelligence platform that supplies valuable threat research to your SIEM and other controls, but also brings a team of subject matter experts to operationalize that data within your enterprise.

Products Included

RedLegg's Threat Intelligence Service includes the following:

- RedLegg Threat Intelligence Platform
- Correlated attack data gathered across all RedLegg TI customers
- Third-party premium threat intelligence feed
- Original threat research
- Third-party, open-source threat intelligence feeds

Services Included

Threat Intelligence provides important enhancements to the correlated logs generated by the SIEM. However, that data can hold little value if it is not operationalized effectively. As part of operationalization, RedLegg reviews the various IOCs and observables in the threat feed, compares them to the monitored log sources, and creates rules and alarms based on this information, helping to detect and respond to threats and attacks quickly.

RedLegg's Threat Intelligence Service differentiates itself from typical threat intelligence feeds and platforms as follows:

- RedLegg operationalizes your threat intelligence by creating, implementing, and tuning new alarms and alerts.
- RedLegg installs only those alarms and alerts that are necessary to the customer environment, creating a more reliable SIEM.
- RedLegg consistently reviews and curates the intelligence to ensure its continued relevance.

Feed Information

RedLegg's Threat Intelligence Service implements a custom-curated threat intelligence platform to augment our Clients' current SIEM deployments, providing up-to-date, high-confidence intelligence.

Unlike most threat intelligence feeds and platforms, which are singularly focused on threat research, RedLegg collects data from the following sources:

- **Correlated attack data** – Unique to RedLegg's Threat Intelligence Platform, RedLegg extracts IOCs and observables from confirmed cases across our customer base, providing actual attack data to the platform.
- **Third-party premium threat intelligence feed** – This is threat research performed by various third parties and distributed in various premium feeds that are ingested into the RedLegg Threat Intelligence Platform.
- **Original threat research** – This is threat research conducted by RedLegg and provided through honeypots, malware reverse engineering, and threat hunting.
- **Third-party, open-source threat intelligence feeds** – This is threat research provided by various organization and made available to the public.

Collection Features

RedLegg aggregates this collected data and assigns reliability scores based on threat and presence. Data is de-duplicated to maintain performance and efficiency. The data set contains potential threat actors and domains that have achieved a low reputation due to detected and reported activity, as well as malicious hosts, URLs, IPs, file hashes, and other observables identified by the RedLegg Managed Security Services team; these items are added to the Intelligence Feed as well.

High Confidence	Objects collected for the RedLegg Threat Intelligence Service have been actively observed participating in malicious behavior and have been correlated to reduce the possibility of false positives. Hosts that have not demonstrated bad activity after a period of time will have their risk ratings lowered, but not removed altogether.
Up-to-Date	It is important to always use current data, as new bad actors appear daily. To stay ahead of the game, RedLegg utilizes data that is updated multiple times per day to ensure that lists contain the most currently identified risks.
Categorized	Understanding the type of activity that a bad host or site represents is key to understanding the potential threats within a network. To this extent, the RedLegg Threat Intelligence Service contains entries in many categories, allowing constant vigilance of bad actors. This setup grants RedLegg the ability to assist customers with keeping control of the areas containing the highest levels of risk to an organization's network.

Threat Intelligence Categories

The Threat Intelligence Categories below represent a small sample of the different types of behaviors of over 84,000 various entities and the risks they pose, generated from real attack data as well as original and third-party research included in the RedLegg Threat Intelligence Platform. This list is reviewed and curated monthly, removing outdated information and adding new relevant data.

WATCHTOWER

Watchtower is a tool designed by the RedLegg Threat Research Team to allow RedLegg Managed Security Services to better manage, investigate, and contextualize intelligence around security threats identified in live, real-world environments. MSS Security Analysts provide next-level Threat and IOC management, while utilizing automated and on-demand analyzers to quickly identify the nature of a potential security event. Watchtower feeds into and receives live data from the RedLegg Threat Intel Ecosystem. Watchtower is a Value Add for all customers who subscribe to RedLegg Threat Analysis-based MSS Services.

Watchtower Functions:

- **Case Management System** – Correlate tasks, observables, and alerts into a single investigation (case) to better track and document an event.
- **Threat Analysis Tools** – Built-in automated and on-demand analyzers allow analysts to quickly and easily gather information and intelligence on the observables identified.
- **Cross-Customer Correlation** – High-level visibility into potential threats that may be affecting multiple customers.
- **Observable Management** – Automatic extrapolation of key data points that direct an analyst to quickly identify a security alert.
- **Work flow Standardization** – Tasks and workflows are automatically presented to analysts in playbooks when new cases are created. This assures consistent and thorough research.
- **Asset Management** – Critical customer assets are tagged by engineers with context so that they can be quickly identified in subsequent events.
- **Malware Sandboxing** – Malicious files and IPs forwarded to Watchtower can be detonated safely in our sandbox environment and results/intel gathered to provide a more thorough investigation.
- **Security Focused** - Security and operational alarms are separated to keep staff focused on the alerts that pose the biggest risks to a customer's business.
- **Threat Intel Ecosystem** – The observables are gathered and curated before being and submitted to the RedLegg Threat Intel Feed for use in subscribing customers' SIEM environments.

Key Differentiators

Correlation – Watchtower is unique from an MSS perspective because it allows us to not only perform case management and threat analysis from a centralized tool, but also allows us to correlate across our customer base. This key information exposes potential threats that may be new and developing, or even targeting specific customer verticals.

Intelligence – We put the threat data that our analysts gather from investigations back to work in our Threat Intelligence Service. This gives our subscribing customers a leg up on staying current with real-world potential risks that may affect their business verticals. The Watchtower/Threat Intel Ecosystem is unique in Managed Service Providers, as we use real threat research to make the process smarter.

Observables and Asset Management – Part of the challenge in identifying a security threat is to know which hosts are participating in the activity. With our observable analyzers and our custom asset management, we can notate known customer hosts and gather quick intel on potential external threats. All of these differentiators serve to provide a better customer deliverable by enabling our analysts to provide better analysis, quicker identification of threats, and the ability to be proactive when identifying and mitigating known threats through threat intelligence.

Threat Ecosystem

1 **Customer Alarm** – An alarm is generated from a monitored customer environment. The alarm is sent directly to Watchtower as an Alert.

2 **Watchtower** – Within the Alert, Watchtower identifies and extracts observables: IP address, domain, URL, or file hashes. These observables are considered as potential Indicators of Compromise.

3 **Threat Analysis** – Analysts review the Alert data and run investigations on the identified observables. Analysts report their findings to customers and submit observables to the Threat Research Team for review.

4 **Threat Intelligence Service** – Observables are reviewed by the Threat Research Team to verify their validity as bad actors. These items are included in our Threat Intel Service as known Indicators of Compromise (IOCs).