REDLEGG

THREAT INTELLIGENCE SERVICE

WHY A SERVICE

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.

EMPOWER YOUR INFRASTRUCTURE TO DO MORE

Operationalize threat intelligence data, stop known attackers in your systems, & get ahead in your threat landscape.

Invest In Quality Data

Ingest & Action On IOCs

Stay Ahead Of Threats

MORE THAN A FEED

High-confidence data, diversified streams, & what you need to make it actionable.

QUALITY DATA

Don't put all your eggs in one basket. With data from multiple feeds, including our own original threat research, the data you receive is guaranteed to be high-confidence and relevant.

DELIVERY PLATFORM

Once you buy a threat feed or subscription, you need someone to get that data into your systems – enabling rules, tuning out false positives. Our Threat Intelligence Service handles it all.

THREAT RESEARCH TEAM

Know a threat when you see its fingerprint and stop it in its tracks. Our threat research team has the bigger picture in mind, assisting in identifying attacks and associating them with larger campaigns.

877.811.5040
DOTELL@REDLEGG.COM
REDLEGG.COM

REDLEGG

THREAT INTELLIGENCE SERVICE

YOUR TRUE INTELLIGENCE SOLUTION

- RedLegg's Threat Intelligence Platform
- Correlated customer attack data
- Third-party premium threat intel feed
- Original threat research from our honeypots, malware research, & threat hunting
- High-confidence, up-to-date, and categorized data
- Creation, implementation, & tuning of new TI alarms and alerts
- Installation of only those alarms and alerts necessary for your environment, creating a more reliable SIEM
- Feeds updated, reviewed, & tuned every 24 hours
- Your threat intelligence security team includes automation strategists, malware researchers, threat researchers, senior incident responders, senior forensic specialists, & threat analysts
- Ala carte SOC-as-a-Service offerings with an MSSP who performs incident response, forensics, MDR, & automation

THREAT ECOSYSTEM

CUSTOMER ALARM

An alarm is generated from a monitored customer environment. The alarm is sent directly to our central engine as an Alert.

XSOAR

Within the Alert, our central engine identifies and extracts observables: IP address, domain, URL, or file hashes. These observables are considered as potential Indicators of Compromise.

THREAT ANALYSTS

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.

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).

877.811.5040
DOTELL@REDLEGG.COM
REDLEGG.COM