REDLEGG

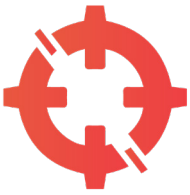
MANAGED DETECTION & RESPONSE SERVICE

YOUR ADAPTABLE MDR SOLUTION FROM AN MSSP THAT VALUES LONG-LASTING, COLLABORATIVE RELATIONSHIPS & A HANDS-ON APPROACH TO SECURITY.

- ☑ Level of remediations & host isolation upon agreement
- ☑ Monitoring of network connections, file integrity, process creation, registry edit, and running services
- ☑ Expertise in IR, Incident Triage/Analysis, Network & Forensic security analysis, & Automated Response
- ☑ Leadless Threat Hunting
- ☑ Onboarding time in hours, not days or weeks
- ☑ Flexibility – option to use LimaCharlie, Palo Alto Networks Cortex XDR, or your existing tool
- ☑ Continuous centralized recording of all telemetry activity
- ☑ Remote delivery and includes tuning phase
- ☑ Option of integrated Threat Intelligence from our threat research team
- ☑ Option of integrated network sensor
- ☑ Custom threat detection use cases
- ☑ Custom automation and detection rules
- ☑ Ala carte SOC-as-a-Service offerings with an MSSP who knows your network as good as you do

WHAT IS MDR BY REDLEGG?

RedLegg's MDR Service provides a skilled team monitoring critical hosts around the clock, looking for abnormal behavior or other indicators of attack, and offers expertise in the areas of Threat Hunting, Automation Development, Incident Triage and Escalation, and Remediation Response. With RedLegg's MDR service implemented and enhanced by our methodology, our data enrichment, and automations, your overall security posture is greatly improved as is the mean time to detect and respond to advanced attacks.



Grow Your Detection Capabilities

Reduce Your Time To Detect & Respond

Monitor Your EDR Tool 24x7

PROACTIVELY DEFEND YOUR NETWORK FROM ADVANCED ATTACKS

Reduce the impact (and damage) of threats by preventing lateral movement in your network.

MDR SERVICE

- In combination with SIEM, use EDR as a second layer of coverage to help you fill in detection gaps by offering more insight into host activities.
- Go beyond high-confidence alerts with agreed-upon terms for triage, investigation, and remediation that allows our experts to protect your network on your behalf.
- Whether you prefer to use our tool or your existing investment, we have the experts to adapt to your staffing needs with all the capabilities of a SOC-as-a-Service operation.
- For even deeper insight into network traffic, you can add our network sensor to the MDR service.

877.811.5040
DOTELL@REDLEGG.COM
REDLEGG.COM