RedLegg for Cortex by Palo Alto Networks

REDLEGG

REDLEGG & CORTEX

Today's cybersecurity landscape is increasingly complex and fragmented. Disconnected tools reduce visibility, delay response times, and drive up costs. Palo Alto Networks Cortex provides a unified, AI-powered solution - but realizing its full potential takes the right expertise.

That's where RedLegg comes in. We deliver fully managed detection and response services for Cortex, combining expert-led operations, seamless integration, and around-the-clock monitoring. This enables organizations to operationalize Cortex quickly, respond to threats more effectively, and strengthen security - without added complexity.

For mature organizations, out-of-the-box functionality isn't enough. RedLegg enhances Cortex with customized runbooks, tailored automations, and proactive threat hunting - all aligned with specific business risks.

REDLEGG MDR

- Palo Alto Networks Managed Security Partner since 2020
- Chicago-based, veteran-owned
- Est 2008

WHY REDLEGG - CYBERFUSION

A Smarter Approach to Security Operations

RedLegg integrates platform management, cyber threat intelligence, expert threat analysts, and advanced data analytics into a seamless security ecosystem.

Our Cyberfusion approach bridges gaps between security tools, data sources, and response actions for faster, more effective security outcomes.

- **Micro-Practices That Matter**
  Expertise in Threat Analytics, Automation, and Detection Engineering to enhance Cortex capabilities.
- **Proven Results, Not Just Promises**
  Delivering fully operationalized security with white-glove service.
- **Cost-Effective & Scalable**
  A smarter alternative to traditional professional services, with a focus on efficiency and value.

redlegg.com
(312) 757-4941
dotell@redlegg.com

RedLegg for Cortex by Palo Alto Networks

REDLEGG

GO-TO-MARKET OPTIONS

Full Platform Management
Complete oversight, tuning, and response.

Professional Services
Deployment, integrations, and optimization.

Channel Partnerships
RedLegg works with major VARs globally.

Expanding Palo Alto Networks Exposure
Integrating Cortex with existing customer environments.

CORTEX XSIAM, CORTEX XDR + REDLEGG MDR

Smarter, Faster, More Effective Threat Detection

Human-Led Investigations

Pair AI-driven detection, with human lead investigation for high-fidelity alerts.

Custom Detection Logic

Fine-tune detection rules based on your environment.

Threat Disruption

Real-time containment guidance and automated response actions allow customers to act fast before threats escalate.

CORTEX XSOAR + REDLEGG MANAGED AUTOMATION SERVICES

Optimize and Transform Your SOC

- **Playbook Optimization**
  Refine playbooks to align with real-world security operations, preventing automation misfires and inefficiencies.
- **SOC Workflow Integration**
  Integrate Cortex XSOAR across the customer's security stack, ensuring seamless response across endpoints, network, and cloud.
- **Automation Architects**
  Prioritize, plan, and execute your unique automation projects.

CORTEX CLOUD + REDLEGG MDR

End-to-End Cloud Security

- **Cloud Optimization**
  Tailor security controls to fit agile development environments, ensuring protection without slowing innovation.
- **Unify Security Across Cloud and SOC**
  Achieve full security coverage across multi-cloud environments while streamlining SOC operations.
- **Runtime Threat Detection**
  Contextualize detections, distinguishing between legitimate activity and potential compromise.
- **Cloud Threat Hunting**
  Identify misconfigurations, privilege escalations, and suspicious activity across multi-cloud environments.

redlegg.com
(312) 757-4941
dotell@redlegg.com