

THREAT HUNTING

SERVICE OVERVIEW

Legato Security Threat Hunting discovers less obvious threats to client networks and digital assets. Legato security execute a hypothesis-based objective-driven hunt to actively search for signs of compromise. Threat hunts are often a planned and organized engagement with scheduled tasks and produce a findings report at the completion of all threat hunting tasks. This actionable threat intelligence is vital to filling gaps and planning for customers' cybersecurity future.

SERVICE CAPABILITIES



LOG ANALYSIS & MONITORING

Analyze firewalls, intrusion detection systems, and endpoint security solutions.



CREDENTIAL MONITORING

Seasoned security professionals explore dark-web markets for compromised credentials.



PLANNED & ORGANIZED ENGAGEMENT

The threat hunt process follows a structured approach and scheduled tasks.



FINDINGS REPORT

Comprehensive findings report delivering identified threats and recommended actions.

BUSINESS OUTCOMES



ENHANCED AWARENESS

Awareness about emerging threats, attack techniques, and indicators of compromise.



BOOST INCIDENT RESPONSE

Gain a better understanding of the techniques and tactics of the threat.



EARLY THREAT DETECTION

Finding threats early on allows you to take prompt action and prevent further infiltration/data breaches.



REDUCED RISK OF COMPROMISE

Equipped with actionable threat intelligence, customers can reduce their risk exposure to outside attack.

ONBOARD

Legato Security's vCISO will work with the customer to gain a full understanding of the customer's existing environment, resources and security strategy

STRATEGIZE

With the customer's desired outcomes in mind, Legato Security's vCISO will help build a forward-looking security strategy to help organizations combat evolving adversaries and attacks.

EXECUTE

Legato Security's vCISO will implement and execute a security strategy that will improve customer defenses and minimize the chances of a security breach.



Contact Us:

P: 385.301.8388

www.legatosecurity.com

WHY LEGATO THREAT HUNTING?



FULL SERVICE SOC

Legato Security's SOC operates 24x7, ensuring that our customers are protected from cyber attacks every, of every day. Designed to augment and support a customer's existing security team, the Legato Security SOC will:

- Detect, triage and correlate every alert
- Prioritize threats for remediation, saving customer's time and money
- Respond and remediate threats on behalf of the customer



LEADING TOOLS AND PROCESSES

Legato Security's vendor agnostic approach means that our SOC will manage and optimize a customer's existing set of security tools, eliminating the need to rip and replace their original investment.

- Immediate ROI by leveraging existing tools and pairing them with a team of security experts to streamline operations
- Flexible architecture and system integrations
- The ability to select best-of-breed technologies to compliment your existing security solutions



WE SCALE WITH YOUR ORGANIZATION

Legato Security's open security platform allows us to build and scale a security solution that fits your business now, and in the future.

- With services that range from strategic and advisory services through fully managed network security, Legato Security has a service for any size organization
- Select the appropriate tools and solutions for your organization current needs
- As your organization matures, Legato Security will be with you every step of the way by creating a tailor made security plan that scales with your needs

THE VALUE OF MANAGED THREAT HUNTING

PERSONALIZED

Tailored to the needs of each organization, Legato Security ensures that each service meets the needs and required outcomes of each customer.

CUSTOMIZED

Each Legato Security service accounts for the unique resources and parameters of a customer environment, helping create a custom and results driven engagement.

ACTIONABLE

Post-service reports provide actionable intelligence and recommendations to further harden the customer's security posture.

"Having Legato Security's SOC help with Threat Hunting has saved our team hours and hours of time that we've been able to reallocate to other tasks.

- CISO, Retail Industry



Contact Us:

P: 385.301.8388

www.legatosecurity.com