

SECURITY OPERATIONS CENTER



Our next generation security operations center provides continuous monitoring and response capability. Our mission is to be an extension of the clients' own internal team, covering – not duplicating – internal capability needs.

TECHNOLOGY AGNOSTIC

We begin by ingesting available telemetry from all available endpoints, network appliances, applications and clouds to gain visibility over your entire network. We bring a technology agnostic approach and will work with whatever the client has - or provide recommendations to cover any visibility gaps.

REAL-TIME ANALYSIS

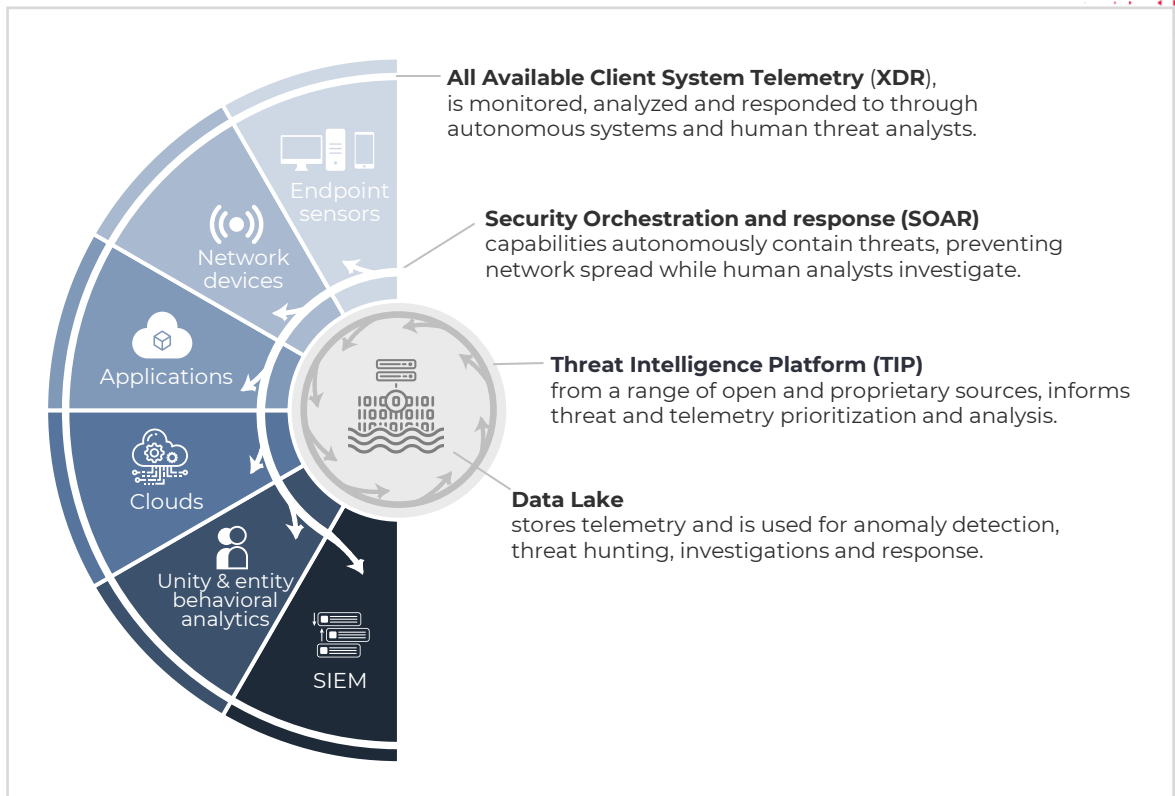
Our SOC infrastructure includes advanced automation, designed to ensure rapid containment and notification of suspicious behavior. However, we also provide the next step: human touch. Cybersecurity analysts review and validate all threats within defined service level agreements. Notifications to clients are customized to their communication preferences, and human analysts coordinated responses directly with the client team.

SECURITY OPERATIONS CENTER SERVICES

- 24 x 7 x 365 security operations center
- Managed threat hunting with human analysts
- Next generation endpoint, network sensors, and cloud application monitoring options
- Sandbox
- Online & mobile dashboard
- Vulnerability scanning



LOKI LABS



POSTURE EVOLUTION

We work with our clients to progressively move their cybersecurity posture upwards and to the right. Monthly account meetings not only review historic behavior, but discuss relevant emerging threats, discuss discrete elements of the clients' overall security strategy, and provide an opportunity for clients to seek expert advice.

THREAT NOTIFICATIONS

Threat notifications feeds, customized to the clients' environment and security stack, ensure clients are quickly informed of exploited and discovered vulnerabilities that could impact them.

HYBRID SOCS

For clients with some internal SOC and threat hunting capacity, we provide surge support, providing coverage overnight, weekends, and holidays, providing clients with peace-of-mind that their network is being monitored out of hours.

SIEM-AS-A-SERVICE

Clients integrate their technology with our security incident and event management (SIEM) infrastructure, but have their own customized access to enable them to monitor and conduct their own threat hunting.

Loki Labs Inc

13431 Heswall Run, Orlando FL 32823
888.565.4522 / 888.LOKI.LABS
info@lokilabs.io

A service-disabled veteran owned small business.



LOKI LABS

©2022 Loki Labs, Inc. All rights reserved. Loki Labs is a registered trademark of Loki Labs, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners.