eSuraksha *by* RAJIVIHAAN

A Fully Managed AI-Powered SaaS Security Solution

What is eSuraksha by Rajivihaan

RAJIVIHAAN's **eSuraksha** security platform is a service that leverages and enhances your existing investment and tools to uncover previously unknown and advanced threats. **eSuraksha** analyzes enterprise log data to detect unknown threats and create enriched, prioritized, **actionable cases while removing noise and false positives, enabling your security staff to focus on business requirements vs. time** consuming investigations. **eSuraksha** retains and exposes transferred logs allowing users to see, search and correlate data via reports and dashboards from a single pane of glass.

eSuraksha by RAJIVIHAAN

A true force multiplier, powered by AI and an industry leading level of advanced security analytics, proven to strengthen compliance initiatives and identify unknown threats existing security tools just do not catch.

- Increases Efficiency
- Far Less Noisy; Removes Alert Fatigue
- A Force Multiplier
- Replaces Tier -3 Services with Automation
- Provides True Situational Awareness

Why eSuraksha by RAJIVIHAAN *:*

- Addresses the problem of advanced adversaries making their way through perimeter defenses by combining multiple **modes of Machine Learning (ML) with an advanced Artificial Intelligence (AI) engine.**
- **Indexes and analyzes logs from your existing tools to find previously unknown, advanced, and insider threats while dramatically reducing the number of false positives generated by more traditional solutions. These findings are presented in a consolidated** and intuitive user interface.
- **Cases are automatically created with an AI engine considering a range of variables including behavior severity rating (risk), analytic (behavior) confidence, network priority and critical servers.**
- **Delivers high-fidelity, actionable cases with suggested remediation steps.**
- **Leads the industry in the number of continuously evolving streaming analytics, designed to detect unique behaviors, enhancing your existing security tools, network devices, servers and endpoint AV/AM tools. The AI engine evaluates all of the** components of a case to ensure validity. This step, that is normally accomplished by an experienced cyber analyst, ensures our false positive rate of less than 5%.
- Leverages custom analytics to detect a wide range of anomalous behaviors including:
  - **Data Exfiltration**
  - Advanced beaconing
  - DGA detections
  - Credential misuse
  - Unusual user behavior
  - Web attacks
  - P2P communication
  - Network Enumeration
  - Suspicious downloads
  - Unauthorized user activity
  - Malware
  - **Misconfigurations**
  - Suspicious Process Spawning
  - **Insider threats**
  - Unauthorized Vulnerability Scans
  - Cryptomining
  - **Intrusion attempts**

eSuraksha *by* RAJIVIHAAN

A Fully Managed AI-Powered SaaS Security Solution

Powered by ML and AI, eSuraksha can:

Expedite/Expand Detection

- eSuraksha**, automatically aggregates related information and malicious activities into high-fidelity, actionable cases, and covers** the multitude of cyber-attack methods and vectors an organization faces.

Increase Efficiency

- **eSuraksha** is a force multiplier for your security team.
- Standard detection solutions typically inundate security teams with alert overload, from un-validated, raw alerts with **limited useful threat data; each alert requires extensive time to uncover the real incident and provide anything actionable.**

eSuraksha is*:*

Comprehensive

- **eSuraksha** provides a wide breadth of threat coverage ensuring your entire environment is comprehensively secure by **combining multiple modes of ML with sophisticated AI to find unknown, advanced and insider threats and delivering** these results via a customized console.

Easy

- **eSuraksha's** cloud-based service is far superior to legacy **solutions that are complex, costly and notoriously difficult to** install and manage.
- **eSuraksha's** advanced capabilities can be deployed and online with just a few hours of setup work; results can be produced within hours of deployment.
- **eSuraksha** provides full-stack visibility of your current security tools and infrastructure without the aggravation and cost of deploying and managing your own infrastructure.

Proven

- **eSuraksha** provides a 95% true positive rate and is already handling hundreds of thousands of observations for customers.
- eSuraksha **has uncovered and prevented many of (but not limited to) the following: production outages, expensive PII** breaches, insider threats/attacks, compromised medical/life sustaining devices, voter/election database compromise, data **exfiltration, and catastrophic business failure.**

ORGANIZATION	THREAT	CAPABAILITIES
National Agency	**UNAUTHORIZED ACCESS** Current SIEM and SOC may have no "rule" monitoring for multiple, automated failed administrative logons to a critical data base server	**eSuraksha PREVENTS PII BREACH** Unsupervised analytics can immediately discover an ex-contractor, maintaining access to this critical server with an automated logon script. Expensive PII records breach can be averted.
Real Estate	**INSIDER THREAT** Very unusual communication with several thousand external IP addresses on ephemeral ports. Lots of log evidence but no skilled analyst watching or manually hunting for threats.	**eSuraksha CAN SPOT UNAUTHORIZED ENCRYPTED VPN** Machine learning & the AI engine can contain with firewall, DNS, and AD logs, to detect an unauthorized VPN and proxy server installation on a workstation made by a sysadmin to conduct personal business, bypassing security controls and exposing the enterprise to the internet.
Building Services	**BANKING TROJAN** A brand new variant of a banking credential scraping malware could be installed on a Wire Transfer Financial Server. Malware likely to blow past signature based AV tool and firewalls	**eSuraksha CAN STOP UNAUTHORIZED WIRE TRANSFERS** Analytics can detect low, slow unauthorized P2P behavior to different countries within first day of service. This new malware variant would not have been spotted by corporate security tool stack, or alerted on by well- known MSSP nor recognized by any tool in Virus
Large Oil and Gas Provider	**CRITICAL IOT DEVICE COMPROMISE** Wellhead device maybe compromised with targeted malware and would be capable of issuing unauthorized commands and downloading additional payloads	**eSuraksha CAN PREVENT PRODUCTION OUTAGE** Advanced Nextgen stateful firewalls can log activity but may not natively detect or drop traffic with random beacons to Command and Control servers outside the country. Analytics monitoring firewall and DNS logs can create a case and remediation steps that keep production online and uninterrupted.

www.rajivihaan.com

Contact: sales@rajivihaan.com