Forensic Driven Detection and Response (FDR) Solution

Building Cyber Resilience using forensics-based intelligence

SISA FDR - A Forensics Driven Cyber Resilience Solution for Managed Detection and Response

With the proliferation of digital transformation initiatives, and the nascent arrival of 5G and edge computing, CISOs are left scrambling to protect a rapidly expanding risk surface. Besides, the known shortage of cybersecurity talent coupled with rising cost of cyber attacks is further challenging the ability of businesses to respond to the evolving threat landscape.

What businesses need is a holistic and ***advanced intrusion detection solution*** equipped with ***actionable intelligence*** to enable a shift from a reactive to a proactive threat response.

What's on your mind?

- How do I determine whether I'm subject to attacks?
- How do I distinguish between real threats and false positives and take timely action?
- How do I contain a breach to minimize its effect and damage?
- What's the right way to respond to a specific cyberattack?

With ***SISA ProACT*** – SISA's comprehensive MDR offering that provides an integrated monitoring platform and a unified incident response solution, answers to these questions are just a breeze.

*"Data breach costs have increased from **$3.86 million** to **$4.24 million** in 2021, the highest in the past 17 years"*

*"It is estimated there will be **3.5 million** unfilled cybersecurity jobs worldwide through 2025"*

The intelligence to detect sooner. The context to respond effectively.

SISA's Forensic Driven Detection and Response (FDR) solution goes beyond traditional solutions that work on rules and signatures. Our solution is powered by forensic intelligence to enable context-aware detection and response.

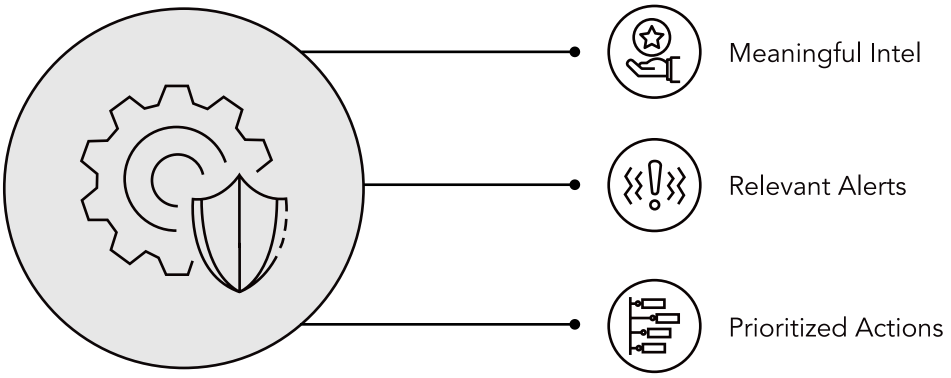
Inherent **AI & ML** capabilities for swift actions

Built-in threat intelligence and **automation** capabilities leveraging SISA's world-class, invaluable forensic data

Delivers **10x value** by accelerating time to multi-vector threat detection and response.

Forensic powered Detection and Response Solution

Context Aware Security Intelligence Powerhouse



Meaningful Intel

Relevant Alerts

Prioritized Actions

The 3 Pillars of FDR

Knowledge	People & Process	Technology
• SISA is one of the top 4 Global PCI Forensic Investigators with 10+ years of accumulated forensic knowledge. • Threat intel from major card brands. • Continuous learning from past and current investigations.	• Integration of MITRE ATT&CK Framework into MDR offering. • SISA-specific frameworks such as Threat Hunting Framework & Forensic Frameworks. • Trained investigators for monitoring.	• Dhi ML, a predictive analytics engine, powered by AI/ML technologies to automatically detect anomalies. • Automated Response to counter threats faster. • Strong analytics & correlation engine trained on threat intel feeds and forensic learnings.

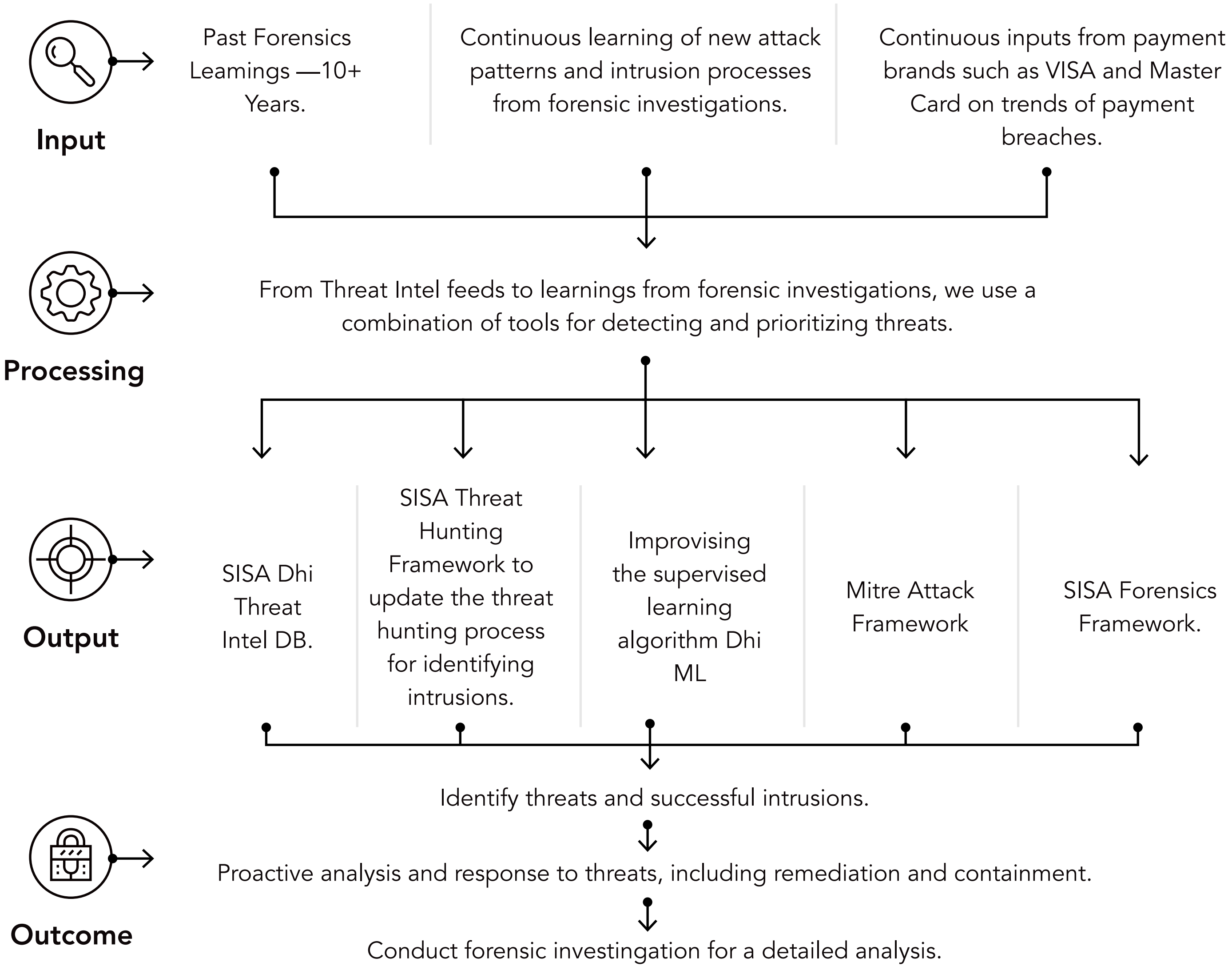
SISA FDR in Numbers

50% reduction in cost from current Total Cost of Ownership (TCO)

1,500+ Use Cases covering all devices and cloud platforms

1.5 million threat values with intel from live forensics analysis

Realize an impeccable process of threat hunting and containment.



Input

Past Forensics Leamings —10+ Years.

Continuous learning of new attack patterns and intrusion processes from forensic investigations.

Continuous inputs from payment brands such as VISA and Master Card on trends of payment breaches.

Processing

From Threat Intel feeds to learnings from forensic investigations, we use a combination of tools for detecting and prioritizing threats.

Output

SISA Dhi Threat Intel DB.

SISA Threat Hunting Framework to update the threat hunting process for identifying intrusions.

Improvising the supervised learning algorithm Dhi ML

Mitre Attack Framework

SISA Forensics Framework.

Outcome

Identify threats and successful intrusions.

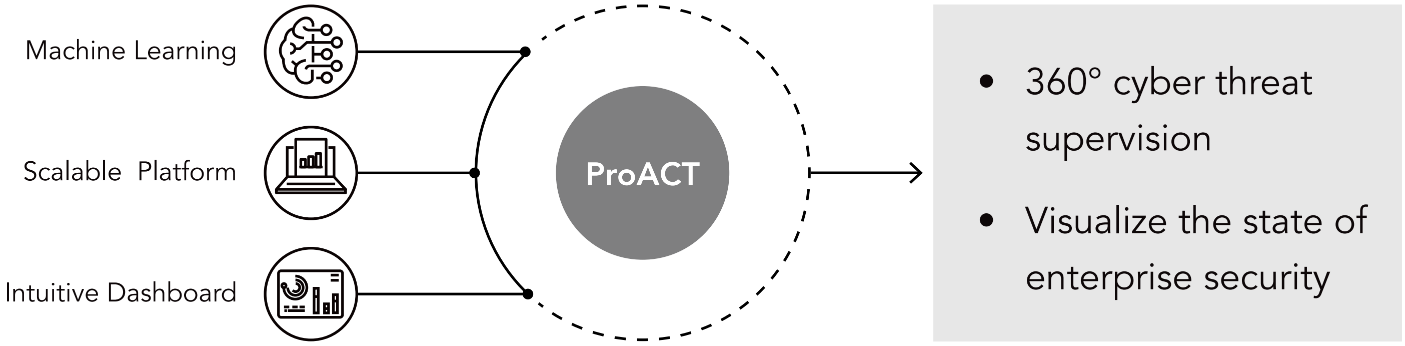
Proactive analysis and response to threats, including remediation and containment.

Conduct forensic investingation for a detailed analysis.

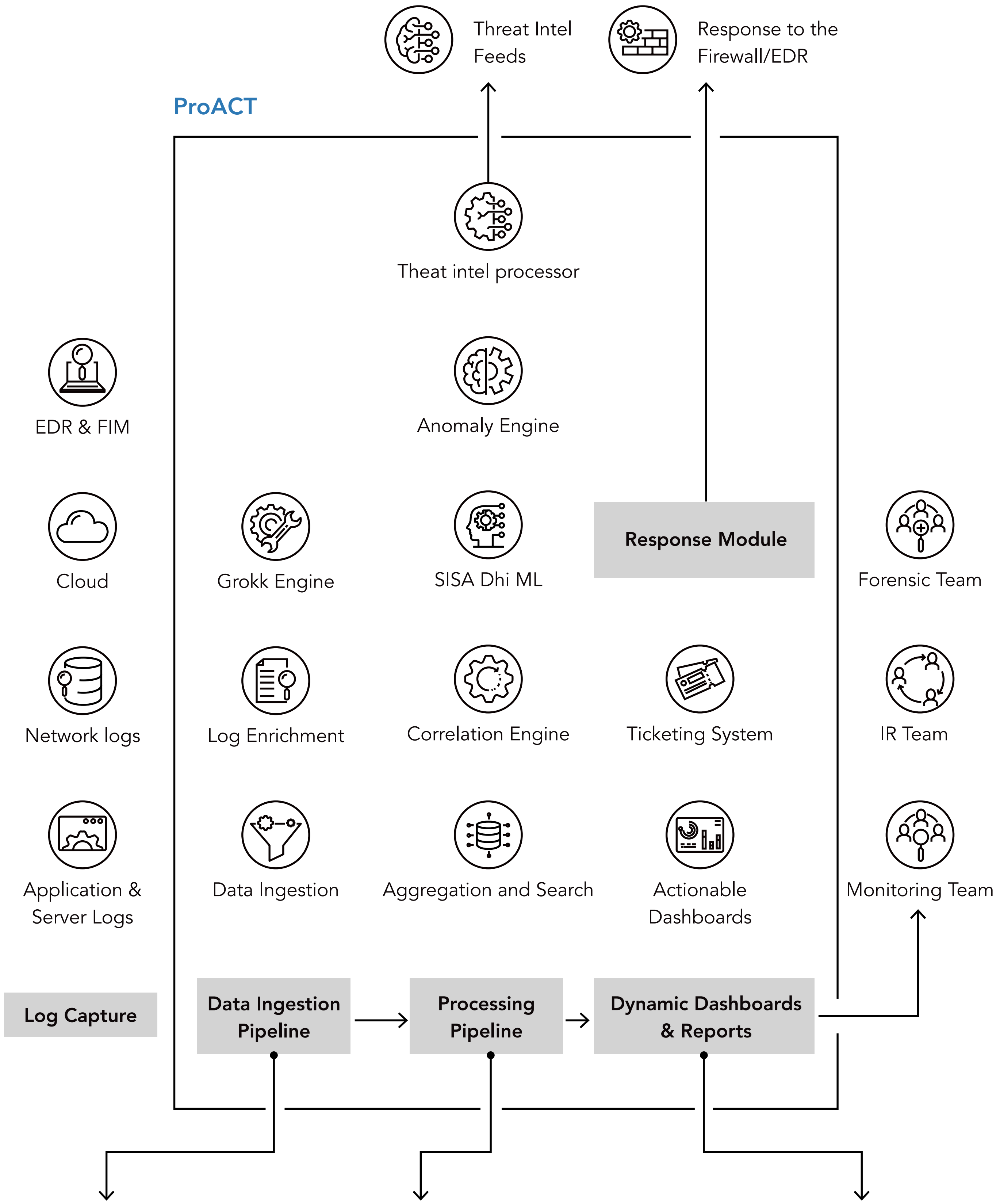
Faster identification of intrusion, immediate analysis and triaging, threat intel gathering and containment.

SISA ProACT for Forensic Driven Detection and Response

SISA ProACT's proprietary Security Information and Event Management (SIEM) platform delivers outcome-based security across networks, applications, and endpoints in cloud, hybrid, co-location, and on-premises environments.



- 360° cyber threat supervision
- Visualize the state of enterprise security



Ingestion Pipeline

Grokk Engine autodetects the source and structure of logs.

Log Enrichment module translates log information into human readable format and adds meta data such as user role device categorization etc. for further analysis.

Processing Pipeline

Treat Intel Processor: Logs are compared with the Threat Intel feeds for any threats and alerts.

Anomaly Engine: Looking for patterns and deviations from data.

SISA Dhi ML: It's the predictive analytics engine powered by ML which detects anomalies and notifies the analyst

Response Module

Risk Ranking: Response module based on the risk score can automatically block the IP's. If the score is medium or low further analysis is carried out to block the IP.

Log Monitoring and Threat Hunting

An applied Forensics-based, reverse-engineered threat hunting solution on an integrated platform for advanced persistent threat detection that puts streams of logs and alerts from network devices, applications, servers, and cloud into context.

Data Ingestion Pipeline

Using the NLM feature, the Autogrokking engine autodetects, analyses, normalizes, and structures the raw log data – the log enrichment module of SISA FDR translates log data into a human-readable format and tag metadata for effective and accurate analysis.

Threat Intel Processor

The Threat Hunting Engine of SISA FDR has a subscription to 70+ threat feed sources and accesses SISA's Forensic investigations to identify the latest threat vectors.

Advanced Analytics

SISA Dhi is the advanced analytics engine powered by machine learning capabilities that detect true positives to reduce the alert volume. Some of the key features of SISA Dhi are User Entity Behavior Analysis, DNS Threat Hunting, Weblog, etc., resulting in faster detection of abnormality.

Response Automation

Response module can directly initiate automated response and block respective IPs in the firewall based on the risk score generated.

24x7x365 monitoring and response	**On-demand security orchestration**	**Intuitive security analytics dashboards**
Scalable virtual appliance and all-in-one agent	**Unified incident response solution**	**Proven deployment with virtualised appliance**

Do what matters the most, as we help you secure 24X7

Forensic Grade Threat Hunting:
Our analysts are trained in forensic investigation techniques and frameworks and use Forensics-based intelligence for threat hunting.

Advanced Analytics & Automated Response:
Machine Learning models are used in ProACT's key features for prioritized threat detection and automated, proactive responses.

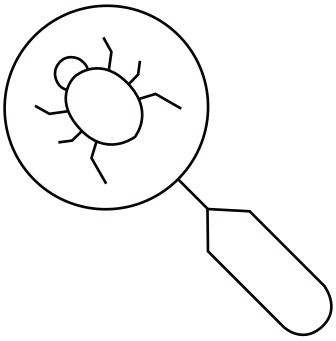
Standby Team for Incident Response & Forensic Investigation:
FDR by SISA includes Incident Response (IR) and Forensic Investigation as a part of the overall solution.

Improved ROI & TCO:
Single layer of accountability and ownership of Product, Process, and People hosted in purpose-built Infrastructure resulting in better ROI and TCO.

Improved Security Posture:
Simulated attacks every quarter using new attack patterns identified as part of forensic learning.

Training on IR:
Ongoing CIDR workshops for training your teams on incident response and containment.

Supplying the capabilities needed to rapidly detect and eliminate cyber threats



- An elite team of researchers, forensic investigators, and responders.
- The proprietary cloud-based data discovery tool – SISA Radar.
- Dedicated Synergistic Security Operations Centre (S-SOC) for 24x7 support.

We provide confidence to businesses using our FDR solutions across banking and finance, e-commerce, transportation, telecommunications, IT/ITeS, and BPO industries by helping them with a stronger security posture.

About SISA Information Security

SISA is a forensics-driven cybersecurity company, with offices in 14 countries, including Bengaluru, India and Irving, Texas. SISA is trusted by organizations across the globe for securing their businesses with robust preventive, detective, and corrective security services, and solutions.

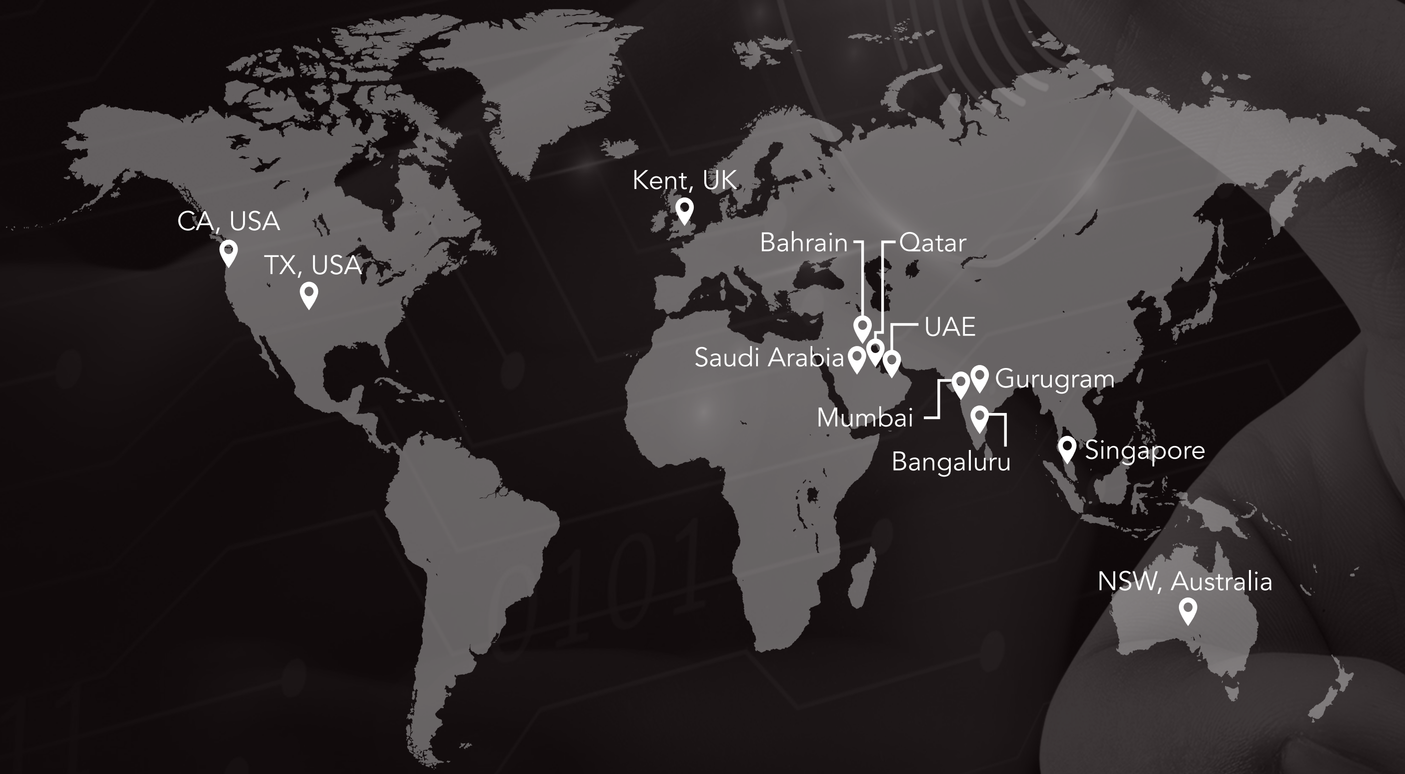
One of the Top 4 Global PCI Forensic Investigators

1,000+
Active engagements

2,000+
Global customers served till date

40+
Countries customer presence

Global Presence



To learn more about SISA's offerings visit us at www.sisainfosec.com or contact your SISA sales representative at contact@sisainfosec.com