ėkasha

zeronsec

Ekasha helps

Conduct Context-driven Investigations

enrich incidents with assets and network information and drive granular investigations with more context, less time and more efficiency..

Efficient stakeholder Collaboration

Stake holder collaborate, share information and participate on live incident investigation and remediation on War room.

Orchestrate SOC through Workbooks & Playbooks

Investigate and remediate incidents by using out-of-the-box, pre-configured workbooks and playbooks to orchestrate SOC from single, easy to use console.

Focus on what is important

Transforms textual data into meaningful details through enrichment, orchestrated artifacts gathering and automatic artifacts analysis resulting in making important, actionable information available.

SOC Cohesiveness

Ekasha platform serves as a workbench for all security operations activities, facilitating real-time communication and collaboration through case assignments and escalations and a war room.

Reduce Alert Fatigue

automate multiple alerts aggregation into individual incidents allowing users to group the alerts based on incident types and affected assets which results in a smaller number of incidents to work on and get rid of multiple alerts producing duplicate information.

Continuously Measure SOC Performance

Measure SOC performance using various dashboard views and reports and work on improvisation to run the efficient operations.

Incidents Categorization and Auto-Prioritization

Automatic categorization and prioritization of incidents reduces the MTTR and helps analyst perform quicker analysis and attending critical asset incidents with higher priority

Significantly Reduces the manual workload

Ekasha gathers additional contexts from across the ecosystem to group the related alerts into incidents into manageable incidents for analysts resulting less number of incidents per analyst.

ekasha

Features

Incident Analysis

- ✓ Artifacts / Evidence gathering
- ✓ Incident lifecycle timeline
- ✓ Data Enrichment
- ✓ Cyber Kill Chain visibility
- ✓ Triage
- ✓ Affected Asset Visibility
- ✓ Algo-based Incident Auto-prioritization

Incident Handling

- ✓ Workbooks
- ✓ Playbooks for Automated Triage
- ✓ Investigative Actions
- ✓ Response Actions
- ✓ War room for Stakeholder Collaboration

Integration

- ✓ Reputation check platforms
- ✓ IT & Security Infra.
- ✓ Sandbox
- ✓ ITSM
- ✓ IAM
- ✓ LDAP
- ✓ Cloud Services

Reporting

- ✓ Executive reports
- ✓ Custom reports

General

- ✓ Custom dashboards
- ✓ Alert Ingestion Engine
- ✓ Support for variety of alert formats
- ✓ Intelligent Case Management
- ✓ Role-based access control

SLA Mgmt.

- ✓ Incident SLA tracking

Playbooks

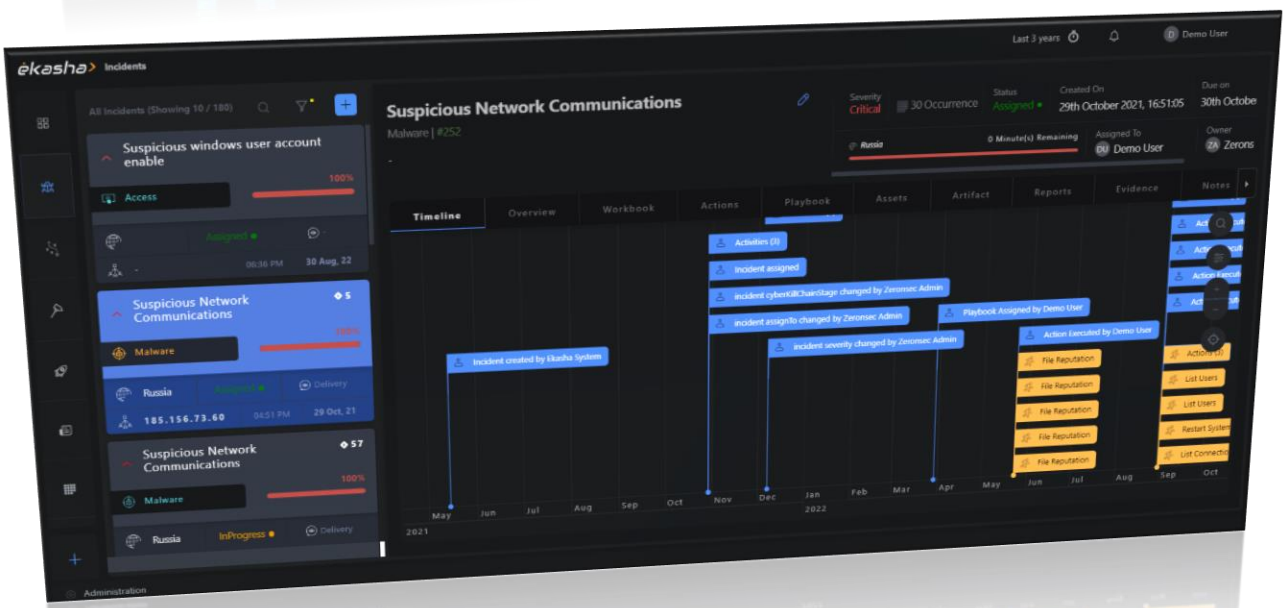
Ekasha offers 100+ playbooks including:

- Email Notification For Malware
- C&C Investigate And Contain
- DNS Hijack Enrichment
- Investigate
- Compromised Email Containment
- IP Investigate And Report
- Hunting
- Malware Hunt & Contain
- Malicious Insider Containment
- Malicious Blacklists
- Phishing Investigate And Respond
- Ransomware Investigate & Contain
- SSH Endpoint Investigate
- Rootkit Investigate
- Simple Network Enrichment
- Wannacry Hunting
- Suspicious Email Attachment Investigate And Delete
- Wannacry Investigate
- Wannacry Prevent
- Wannacry Remediate

Platform Highlights

Executive KPI Dashboard

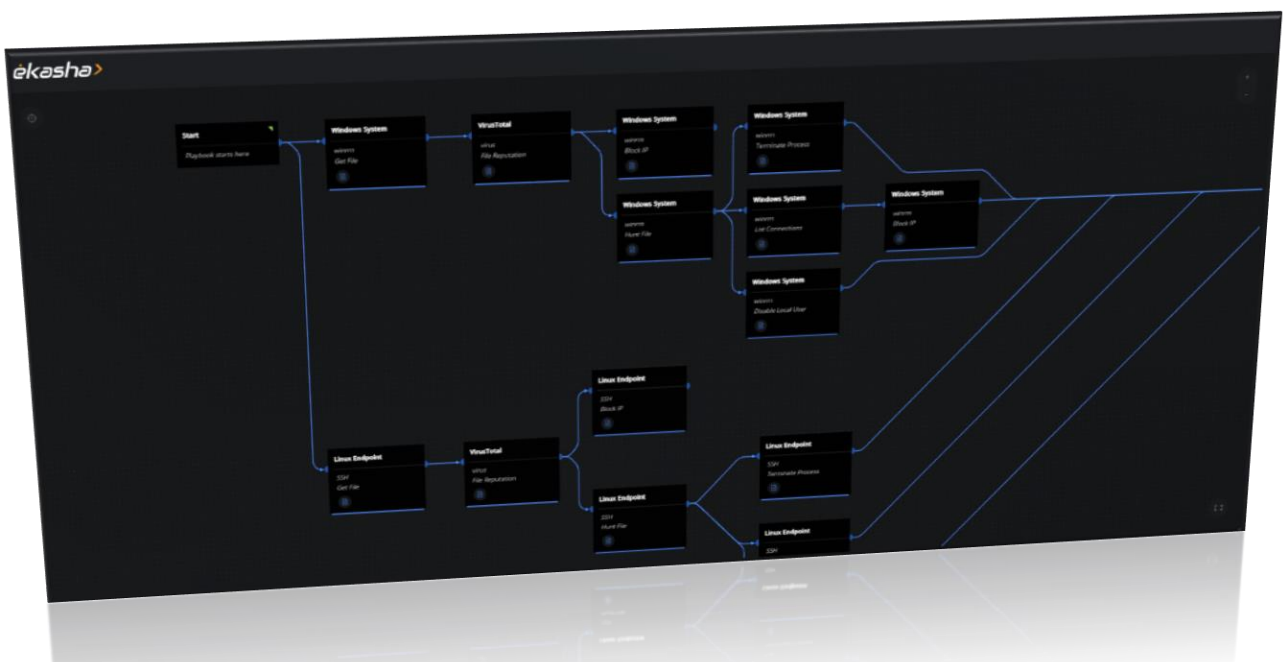
Incident Progress Timeline



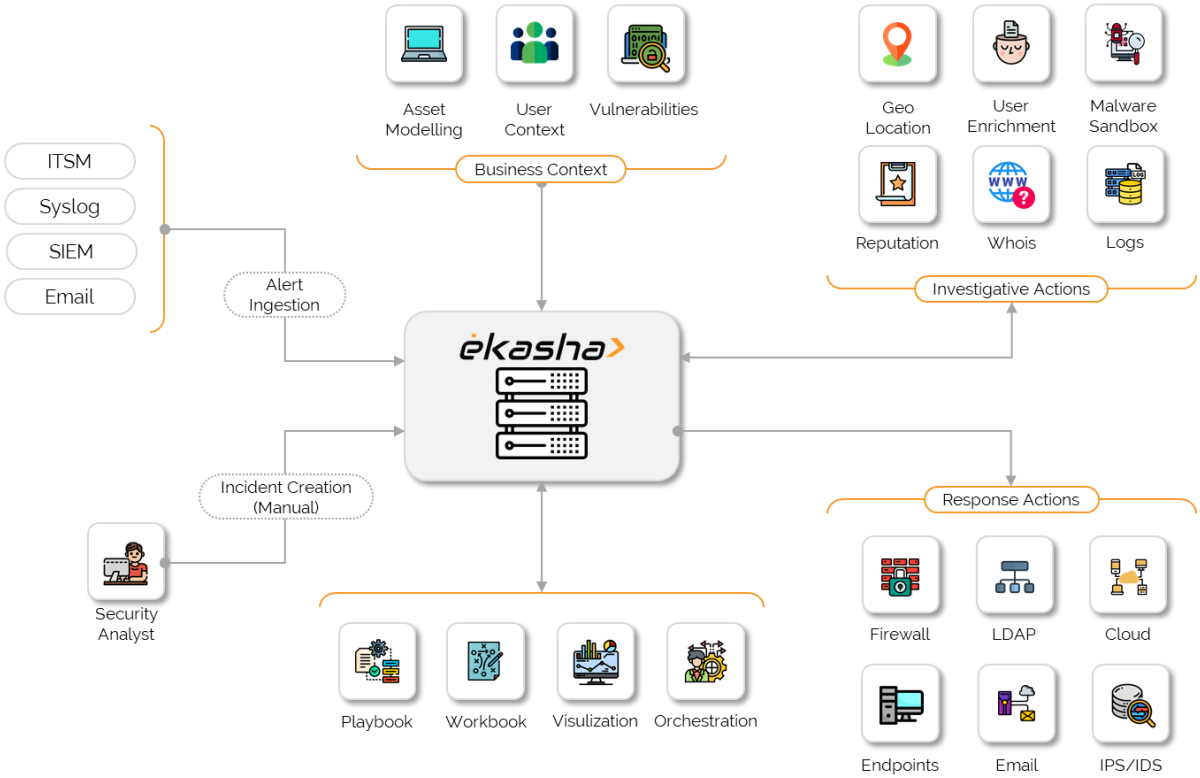
Platform Highlights

Platform Integration

Automation Playbook



Architecture



ekasha

Analyse, Prioritise, Investigate & Orchestrate

Need Help? We are happy to help you.

zeronsec

Reach us :

USA: 1(470) 681-1220 | India: +91 92214 49423 / +91 93244 59861 / +91 96196 25096 | UAE: +971 568 01 4765

info@zeronsec.com www.zeronsec.com

About Zeronsec

Zeronsec is a customer-centric Cyber Security company. Our core business activities include threat research, develop niche cyber security products and provide advance consulting services. The combination of our self researched threat intelligence and products along with consulting services and seasoned professionals helps us create and deliver greater as well as differentiated value. Customers trust us for their need like Managed Security Operations, Cyber threat Hunting, Security Assessment, Compliance consulting (ISO 27001, PCI, etc.), Cyber Forensic investigation and many more specialized consulting services.