**Main View as Left pane**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Info** | **Description** | **Submodule** | **Owner** | **Document page links** |
| **Elysium Product Info** |  | 1. Company, focusing on security, Analytics, operations and BI use cases. 2. Brief comparison with other tools and considerations, cost effective Models, deliverables in terms of AI/ML/Cybersecurity 3. Supporting partners and Integrations | @Satish Abburi ,@Christopher Berry | [[^Linking to attachments.pdf]](https://sstech.atlassian.net/wiki/spaces/ELC/pages/883982432/Elysium+Analytics+Deployment+Document)  [[PDF document about linking to attachments|^Linking to attachments.pdf]](https://sstech.atlassian.net/wiki/spaces/ELC/pages/883982432/Elysium+Analytics+Deployment+Document) |
| **Overview** | **All main features** | 1. log management and analytics services, leverage machine-generated big data to deliver real-time IT insights, Alerts and Actions. | @Satish Abburi @Christopher Berry |  |
| **Quick Start** | **Setup Client Installation, cloud access, demonstration** | 1. After filling the client form 2. Setup Client access using UI 3. Setup cloud access 4. Setup Installation, Services offering 5. 10 days trail run if any 6. Request a Demo | @Maxim Dashenko |  |
| **ODM Supports and Log Types** | **Operational data sources support as matrix form** | 1. Different vendor sources 2. Cloud sources 3. AWS , Apache, Kubernetes Monitoring and Observability etc | @Vladimir Shlyakhtin |  |
| **Visualization and Dashboards or Dashboards and Analytics** |  | 1. Major Dashboards same as Apps Integration dashboards | @Satish Abburi  @Aravind  @Rajesh.Pasupuleti |  |
| **Alerts** | **Monitors continuously query your data to monitor and send notifications when specific events occur.**  **thresholds, critical, warning, and missing data** | 1. Alerts monitor 2. Scheduled searches 3. Alert rules 4. Alert creation 5. Alert action 6. Alert Notification 7. Alert Dashboards 8. Drill Down Alerts | @Aravind |  |
| **RoadMap** | **Over all Architectural view** | 1. Over all architecture , DFD, USE CASE Diagrams | @Aravind |  |
| **Profile (User/Entity anomaly Scores)-UEBA** |  | 1. Endpoint Indicators of Compromise 2. Privileged Account Usage 3. High Volume File Access 4. Bandwidth Usage by size and count 5. VPN Connections 6. File Downloads 7. Bot Attack 8. Unusual Domain | @Rajesh.Pasupuleti |  |
| **Advanced analytics ML** |  | 1. Algorithms/ Accuracy (DGA, Isolation Forest, one class SVM) 2. AI/ML/Cognitive parts 3. Anomaly Detections 4. ML Pipelines | @Aravind |  |
| **Security** |  |  |  |  |
| **ITD** |  | 1. Risk score of User and Entity**(Day wise and aggregation)** 2. Anomaly count 3. Threat User’s and Entity 4. 360 User view 5. Daily Risky Behavior – Zscores 6. MITRE-ATTACK 7. Event level Risk Trend 8. Event List 9. Alerts 10. Risk score trend analysis for User/ Entity 11. Filters | @Rajesh.Pasupuleti | <https://sstech.atlassian.net/wiki/spaces/AN/pages/1257111777/IP+VIEW> |
| **SIEM** |  | 1. Hosts 2. Network 3. Endpoint Activity 4. Authentication logs 5. DNS Traffic 6. NetFlow |  |  |
| **API** |  | 1. Kiabana 2. Logstash 3. Snowflake 4. Filebeat 5. Metricbeat 6. Ingestion Management API 7. Collector Management API 8. Content Management API 9. Role Management API | @Anil Reddy Donthireddy  @Sriraman Krishnamurthy  @Aniket Lad |  |
| **IOT** |  | 1. Thingsboard Open source IOT Platform 2. Device management, data collection, processing and visualization for IoT solution |  |  |
| **APP’S Integration** |  | 1. 360 view 2. Alerts 3. Endpoint 4. ITD 5. Identity Management 6. Operational 7. Search 8. Statistical Data 9. Security Posture 10. Behavior Analytics UEBA 11. Snowflake analytics 12. Source analytics 13. SOC Dashboard 14. NIST,HIPAA,SOX |  |  |
| **Cloud Integration** |  | 1. AWS 2. GCP 3. Azure |  |  |
| **Manage and Monitoring** |  | 1. Ingestion and Volumes 2. Users and Roles 3. Connections and Integration 4. Data Forwarding | @Satish Abburi @Thomas McCroskey @Charles Lo |  |
| **Search** |  | 1. Search basics 2. Export/Import search data 3. Optimize Search Performance 4. Index Management 5. Search query language 6. Search Cheat Sheets 7. TIME Compare 8. Subqueries 9. Lookup Tables | @sannith.bode  @Charles Lo |  |
| **Role-Based Access Control** | **set of permissions and every user is assigned to exactly one role.** | 1. Admin Role 2. Analyst Role 3. Developer Role 4. Manger Role 5. Team Lead Role 6. Dashboard Access control | @Christopher Berry |  |
| **Release Notes** |  | 1. Version release Documents 2. Enhancements in product | @Satish Abburi |  |
| **Pricing** |  | 1. Cost effective 2. Scaling factor- Volumes in GB 3. Time duration 4. Usage service on demand | @Aravind |  |
| **Help** |  | 1. Community help github 2. Product support 3. Virtual assistance chatbot | @Thomas McCroskey |  |
| **Supported Resources** |  | 1. White papers 2. Demo videos 3. Technical Support Documents |  |  |
| **Technology partners** |  | 1. Cloudera and existing cybersecurity platforms, Snowflake, AWS, Azure | @Christopher Berry |  |
| **Customer success Reviews** |  | 1. Ratings and 2. feedback suggestions 3. Reviews | @Charles Lo |  |
| **Industry supported Domains** |  | 1. Business, Banking Financial, Health care, private, public sectors, govt etc |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |