eGyanam PARHAM - Automation Broker

Specially Designed for SOAR Solutions

eGyanam PARHAM - for SOAR Solutions

About Parham

eGyanam Parham is Industry's first multifunctional Security Automation Broker solution which plugs the Security Gaps in a traditional enterprise wide security environment where multiple security solutions work in silos.
It communicates with key security solutions including SOAR, SIEM, Firewalls, Threat feeds, non-standard log sources in a cohesive manner delivered as a customised combination of Software Product & Consultancy solution to address the Cyber Security Automation & Analytics needs of an Organisation.

Parham Achieves Customized Security

Every Organization faces very specific and unique Security challenges and so the solutions should be customized. The product focused approach does not take the exact Security needs of the Organisation and only achieves General Purpose Security.

eGyanam Parham Automation broker covers these gaps and provides a customised solution for Automation requirements of the Organization.

Key Features of Parham

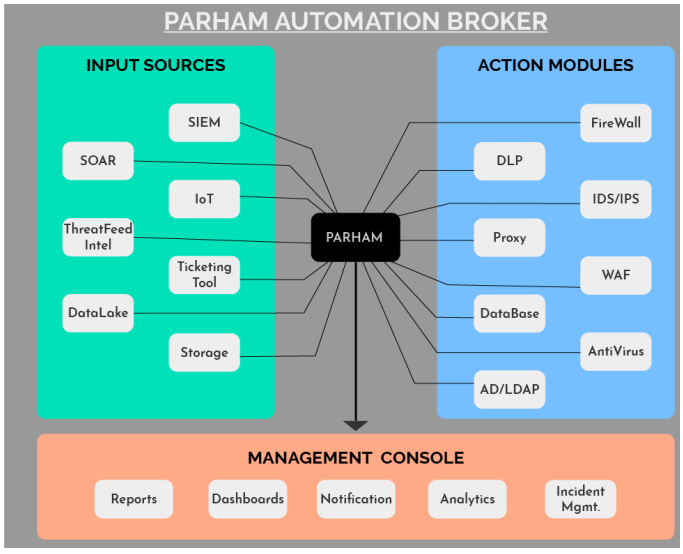
- Provides Automation & Orchestration capability for any Cyber Defence Center.
- Can be used with any SOAR solution to address the integration and compatibility limitations being faced currently.
- Can be used with any SIEM solution for customized Dashboards, Use cases & Reports which is quite limited currently.
- Can integrate with most Modern SIEM solutions including IBM Qradar, RSA NetWitness, Splunk, LogRhythm, ArcSight & McAfee Nitro.
- Can integrate with both IT & Non-IT solutions like IOT, Scada etc, based on feasibility.
- Works in a non-intrusive manner where no Parham component is installed on any SIEM or SOAR platform.
- Automated Response for select Security Alerts based on predefined rulesets and intelligence.

Why is Parham needed?

Current Security Operation Centres (SOC) have an inherent design challenge, the absence of automation.

- Most SOCs fail to remediate any Security incidents in real time as they are detection controls only.
- Parham can provide Automation Capability required to respond to Security Incidents in near real-time mode.
- Dependence on human intervention through SOC teams results in a delay of at least 15-60 minutes for closure of Security Incidents.
- Any hacking or other advanced cyber attack attempt usually needs only a maximum 1-3 minutes to perpetrate the disaster scenario.
- Most SOCs have a SIEM and/or a SOAR solution, still struggle to cover key Security Solutions and Business applications in the current Detection & Response framework because of the inherent integration limitations.

How Parham work

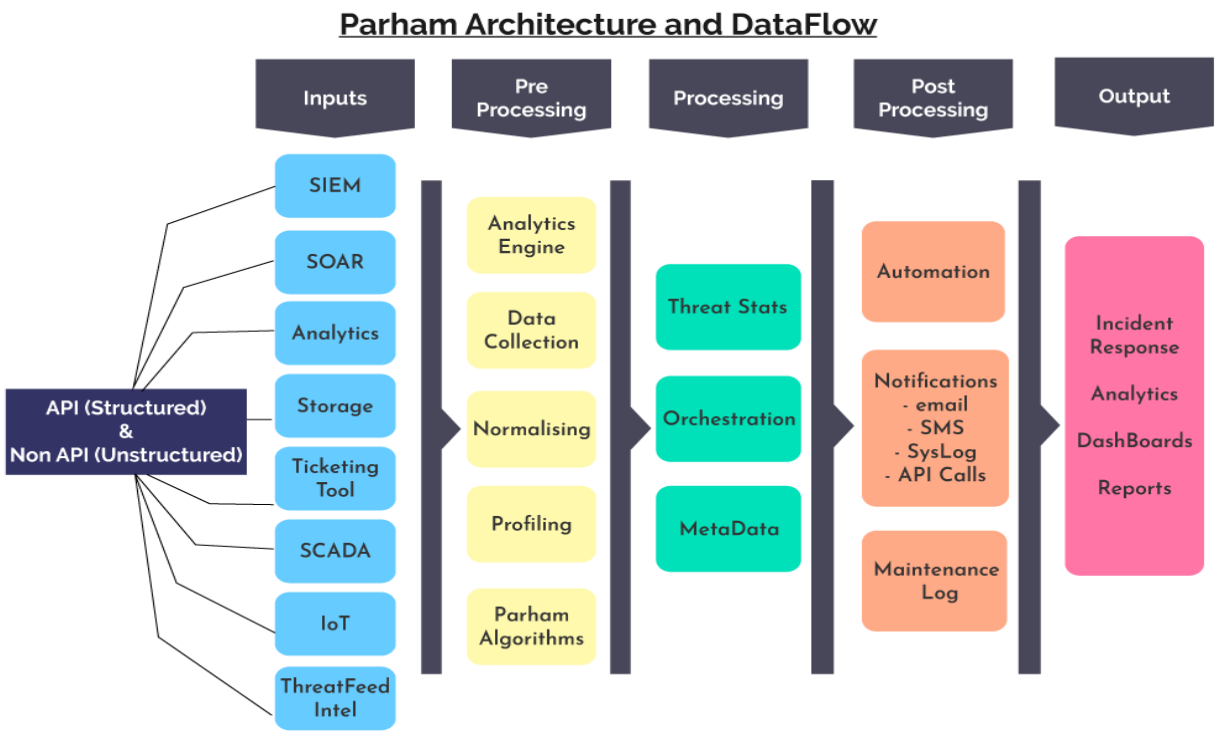


Please contact for more details / Demo / PoC.
We would love to hear your feedback and try to incorporate your requirements for Cyber Security Automation and Analytics.

Multi Threat Feed Integration

- Parham can consume multiple threat feeds available from Commercial & Open sources.
- Provide rich visualization & dashboards for various unaccounted threats based on the intelligence contained in the threat feeds.
- Automation Scenarios can be enabled at network perimeter devices like Firewalls based on inbuilt Threat Scoring engine.

Parham Block Diagram Representation



Parham Unique Features

1. Curated Threat-Information-Feeds
2. Can connect to a wide range of Security Technologies including (vendor agnostic) SIEM, Firewall, IDS/IPS, SOAR etc.
3. Notifies via Email, Slack, WebHook, API
4. Supports Machine Learning & Predictive Analysis with advance contextual visualisation with customised & user friendly dashboards and reports.
5. Big-Data enabled platform with compatibility to connect SQL & No-SQL databases
6. Customised Use-Cases for every environment with Recent-to-Last Known Threat & Vulnerabilities
7. Easy to setup and run.
8. Parham THREAT SCORE ENGINE generates Threat Scores by correlating Threat-Feed-Source with Threat-Category

Other Important & Critical Features

- Console & Dashboards - completely customisable.
- Available as Add-on for any existing SIEM/SOAR or a standalone Security Solution for environments without SIEM.
- Can integrate with existing ITIL compliant Ticketing solution based on feasibility.

Parham Hardware Requirement Details:

List	Specifications
CPU	8 physical cores
Memory	16 GB [Min]
Disk	1000GB HDD
System Type	Virtual/Physical
Network	1 GB/10GB Ethernet

Parham - Compatibility Matrix

SOAR	IBM Resilient, Demisto, Splunk Phantom
SIEMs	QRadar, RSA NW, Splunk, ArcSight, McAfee
Firewalls	Cisco, Checkpoint, Fortinet, Juniper, Palo Alto

Parham Framework works as a combination of Consulting, Product & Support