RSA NetWitness Orchestrator

The modern cyber threat landscape is defined by automated actors such as commodity malware, crimeware, insider threats, and the generic actions of “hacktivists”. Dealing with such innate cybersecurity threats which are churned out in large volumes requires a high-level of orchestration which enables security teams to deal with more important issues. RSA NetWitness Orchestrator provides the comprehensive monitoring and investigation technology needed to iteratively track repetitive threats and prevent them breaching enterprise networks.

RSA NetWitness Orchestrator is a comprehensive orchestration tool that combines complete case management, collaborative investigation, and leverages the RSA NetWitness Platform to discover and mitigate threats. Its capabilities include:

- Incident Management
- Automated Threat Detection and Auto-documentation
- Threat Mitigation and Response
- Intelligent Automation and Orchestration

Incident Management – RSA NetWitness Orchestrator enables security teams to delve deeper into cybersecurity incidents with a view to providing context to specific incidents. The orchestrator takes into consideration repeat offenders when dealing with insider threats, scans system IPs and networks, and track related incidents to provide detailed reports for cybersecurity teams to act upon. Its approach to incident management ensures every node and asset within an enterprise network is continuously tracked and accessed to discover threats.

Automated Threat Detection and Auto-documentation – RSA NetWitness Orchestrator takes orchestration to the next level through the use of 500 applications, integrations, and its’ leveraging of “ThreatConnect” to automate the threat detection process. With the Orchestrator, cybersecurity teams get preconfigured playbooks and documentation templates to automate the detection of both known and unknown threats. Security experts are also provided with the tools to customize specific playbooks to enhance auto detection and documentation playbooks to speed up threat detection and response activities.

Threat Mitigation and Response – Detecting threats or cybersecurity incidents is one half of every comprehensive cybersecurity plan. The second important aspect is responding to discovered threats in real-time to either eliminate or limit the damage they could cause. RSA NetWitness provides automated response tools to alert, block, and quarantine threats based on its intelligent detection system. Piggybacking on ThreatConnect also ensure an accurate response is provided which means you can automate the orchestration of the response procedure with confidence.

Intelligent Automation and Orchestration – At its most basic level, RSA NetWitness Orchestration is a comprehensive orchestration tool as its name suggests. It is designed to support deployments within multi-tenant, single-tenant, and on-premise IT environments. It provides scalable security detection and response orchestration for growing enterprise environments and assists security teams with the intelligence needed to prioritize response initiatives.

RSA NetWitness Orchestration Features

The key features of an intelligent security orchestration tools include real-time executions, automating decision-making processes, support collaboration across security apparatus. RSA NetWitness Orchestrator meets these requirements and adds a few more features to provide comprehensive security orchestration capabilities. Its features include:

- **Dashboard and Reporting Tools** – The Orchestrator provides increased visibility into IT architecture and the context behind cybersecurity incidents using intuitive reporting and a comprehensive dashboard. The dashboard enables security teams to easily visualize the threats, understand their source, and view detailed security metrics on specific incidents. RSA NetWitness reporting tools support the creation of custom playbooks and templates to automate response or simplify documentation.
- **Real-time Response –** The success of every response to a cybersecurity incident depends on the speed at which specific actions were taken. RSA NetWitness delivers the speedy response, as well as, the accuracy needed to ensure threats are comprehensively managed. Security teams can also adapt orchestration strategies according to the changing threat intelligence landscape which makes it easier to detect previously unknown threat actors.
- **Flexible and Scalable Deployment –** RSA NetWitness Orchestrator is built to provide the flexibility required to automate incident detection and response for enterprise fluctuating security requirements. The Orchestrator guarantees security extensibility and growth with

increasing security operations. It provides scalability options for both vertical and horizontal scaling depending on how your enterprise architecture is setup.

RSA NetWitness Orchestrator and the RSA NetWitness Platform

The RSA NetWitness Orchestrator is an extension of the RSA NetWitness Platform as it brings precise orchestration and security automation to the table. The Orchestrator leverages the visibility RSA NetWitness Platform and its advanced security information and event management (SIEM) provides across all endpoints. This adds to the scalability of the Orchestrator and the context it brings to threat analysis.