Cyware Security Orchestration Layer (CSOL)

A Universal Any-to-Any Security Orchestration Gateway

The ever-increasing complexity and variety of cybersecurity tools has resulted in analyst burnout and slowed threat response for organizations. Security operations teams are often burdened due to a large number of repetitive processes in their daily workflow. To counter this and improve the pace of threat response, organizations are adopting Cyware’s security automation and orchestration platform as a means to automate their security operations leveraging security tools deployed across different environments.

Cyware Security Orchestration Layer (CSOL) is a universal and dedicated security orchestration gateway for executing on-demand or event-triggered tasks across deployment environments at machine speeds. CSOL allows security teams to create customized automation playbooks to execute various manual, repetitive tasks in a reliable machine-driven manner. CSOL enables machine-to-machine (M2M), human-to-machine (H2M), and machine-to-human (M2H) security orchestration through integrations with a wide range of deployed security tools and technologies.

CSOL helps organizations streamline and automate their security operations by enabling disparate tools and technologies to talk to each other without having to rely on any manual effort for data normalization, enrichment, and analysis. By deploying CSOL, organizations can significantly reduce mean time to respond (MTTR) and increase operational efficiency along with overall return on investment (ROI) in cybersecurity.

Capabilities and Benefits

Seamless Security Orchestration
- Custom Security Playbooks
- Flexible RESTful API
- Third-party Integrations
- Visual Playbook Editor
- On-Demand and Scheduled Orchestration

Process Automation and Standardization
- Automated Standard Security Processes
- Consistent Repeatable Results
- Fine-tuned Logical Workflows
- High Service Availability

Save Time and Increase Efficiency
- Increased Efficiency through Custom Playbooks
- Reduced Analyst Burnout by Automating Manual Tasks
- Dashboards and KPI Tracking
- Respond Faster and With More Accuracy

Playbook Use Case Examples
- Automated Phishing Analysis & Response
- Malware Detection and Containment Automation
- Automated SOC Event Handling
- Automated SIEM Incident Case Management
Custom Automation Playbooks

- Leverage manual as well as fully-automated playbooks to dynamically meet process and procedure-specific demands.
- Gain access to hundreds of easily click-and-drag, customizable, out-of-the-box playbooks with multiple integrations and custom embedded code.
- Create nested playbooks with dynamic logic to address a wide variety of use cases.

Cross-Environment Automation

- Create seamless automation interoperability between cloud operations and on-premise deployed technologies.
- Integrate CSOL with existing technology stack by utilizing over 250 pre-built application integrations and RESTful API.
- Standardize repetitive security processes to achieve consistent results in security operations.
### Deployment Environments
We provide multiple deployment options for our products, giving our customers the flexibility to utilize all our product features by choosing the model that best suits their business needs.

- Public and Private Cloud
- On-Premise
- Hybrid
- Air Gapped

### System Requirements
System requirements will change based on the considerations of high availability and backups.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>CPU Cores</th>
<th>Memory</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>32 GB</td>
<td>100 GB</td>
<td></td>
</tr>
</tbody>
</table>

### Flexible API:
Utilize a rich, RESTful API to easily build interoperable integrations with custom or third-party tools, cloud-deployed resources, or on-premises technologies.

### Pre-Built Playbooks:
Jumpstart automation and orchestration efforts by utilizing our vast library of pre-built playbooks and customize them to your specific workflows.

### Powerful Customization:
Harness the power of a secure development environment built upon and supporting Python 3, to manipulate and normalize data by easily and efficiently creating custom functions directly in the visual playbook editor.

### Audit Playbook Executions:
Quickly review detailed runtime information to assist in playbook debugging and enhancements.

### Export and Import Logic:
Maintain version control and harness the ability to move playbooks between instances by importing and exporting playbooks directly in the interface or automate the process by leveraging our API.

### Nested Playbooks:
Deploy a nested playbook methodology to create efficient subtask workflows and dynamic logic to address a plethora of use cases.

### Application Extensibility:
Install applications built by third-parties to create technology integrations or create your own connectors and actions directly in the platform.

### Schedule Playbooks:
Make use of playbook scheduling features and take control of playbook actioning by utilizing cron expression.

### Granular Access Control:
Gain granular control over platform features by assigning user privileges based on group memberships.

### Visual Editor:
Quickly and easily create powerful automation capabilities by developing logical workflows from the user-friendly visual playbook editor.

### Multi-Instance Support:
Utilize our platform’s integration flexibility by creating multiple instances of each connector to address different use cases.

### About Cyware
Cyware provides threat intelligence sharing and cyber fusion products to security teams across the world. Cyware’s innovative solutions include capabilities for strategic and tactical threat intelligence sharing, cyber fusion, security orchestration, and incident response. Cyware’s solutions make secure collaboration, cyber resiliency, and enhanced threat visibility a reality for customers.

Cyware
1460 Broadway New York NY 10036
cyware.com | sales@cyware.com | 855-MY-CYWARE