Trends in Technology: Orchestrators

Published on August 2, 2017

Orchestration. It's the new hot topic in cybersecurity interoperability and automation. This handout provides you with a quick analysis of some of the common characteristics and operationally critical features of these rapidly maturing technologies. Whether you're interested in purchasing orchestration products or just trying to keep up with the latest trends in technology, take a few minutes to see what many of them can offer.

Centralized Dashboard

Orchestration products provide a user interface that enables users to navigate the features of their products. These user interfaces vary in their design: some orchestrators provide simple drag-and-drop boxes to build workflows, while others just provide workspaces for developers to code. These centralized dashboards vary greatly in their appearance, but their purpose is the same: to monitor cyber events and mitigation status.

Performance Metrics

Metrics are captured and used to compile summary reports displayed on the dashboard. These analytics vary in what they report, such as open versus resolved incidents, ROI metrics, and SLA status. Orchestrators vary greatly in what performance metrics they display and how they calculate them.

Integration Frameworks

One of the most important features that orchestration products offer is their ability to interoperate and connect with other products. All orchestration products enable connections through an Application Programming Interface (API) or plug-ins that are product specific. Some orchestration products even allow developers to create and use their own plug-ins. Integration frameworks support the IACD tenet of "Bring Your Own Enterprise" by allowing your organization to make the most of their product investments by integrating across them using an orchestration service provider.

Community Support

Some orchestration products also offer valuable resources such as the support of a community that shares documentation and code. It is also important that the vendors participate in this support. Because everyone's environment is configured differently, sharing information can help organizations to tailor their orchestration products more efficiently. Communities that operate in open forums, on blogs, and on other social media platforms also enable users to ask questions and receive prompt feedback. Additionally, open-source platforms support code sharing that enables collaboration on code as well as the ability to download usable code and apply it to specific environments.

Workflow Designer

Orchestration products provide the ability to design and customize workflows tailored to your local environment. This feature also enables you to implement dialable levels of automation based on your comfort level. Whether you're eager to completely automate responses to a cyber threat or just want to get your toes wet, the workflow designer puts you in control. By giving you control to decide where you want "human-in-the-loop" intervention, you'll gain confidence in the execution of automation.

Workflow Tester

Once you've built your workflow, it's important to verify that it executes in the correct manner and validate that it produces its intended results before putting it into operation.

Prioritization

Orchestrators respond to cyber events by using a queue or a scoring schema to prioritize incoming data. Orchestration products that have focused on developing a scoring system determine which events to respond to first based on your organization's policies and processes.

Security Function

Because orchestrators inherently become targets due to their centralized functionality, it's important that they implement standard security practices.

Role- and Attribute-Based Access Controls

Orchestration products categorize users with roles such as administrator, developer, and analyst. While the names and associated privileges vary across products, they all acknowledge that there are different intended users of the product. Depending on your requirements, you may need attribute-based access controls as well.

Authentication and Credentials

Orchestrators need to authenticate using credentials and accordingly need to store or access these credentials safely. You need to apply local authentication, access control, and authorization policies appropriately to non-human entities such as sensors and cybersecurity products.

Auditing

Orchestrators need to provide the ability to audit by logging actions taken in response to cyber events. This enables users to examine how the orchestrator responded and to verify and validate that it acted as intended. It also assists in assessing the state of the system in the event of system failure or shutdown.

Recovery

It is important that workflows developed in orchestrators be stored in a way that is recoverable. There are many mechanisms for storage, such as databases, version control systems, and flat files. The system should return to a defined state after a service restart or upgrade.