Orchestration “Test Drive” Guidance

Why Perform a Test Drive?

NOBODY KNOWS WHAT YOU NEED BETTER THAN YOU DO. A HANDS-ON TEST DRIVE OF ORCHESTRATION PRODUCTS IS THE BEST WAY TO EVALUATE HOW WELL THEY SUIT YOUR NEEDS, IN YOUR OPERATIONAL ENVIRONMENT.

The IACD Orchestration Thin Specification defines a minimum set of services that orchestration services should provide, but most vendors offer more. The different products and services are designed – and often optimized - for particular types of environments, which may differ from yours. Here are some guidelines to help you identify suitable products, and then evaluate how they will help *you* meet your Security Automation and Orchestration (SA&O) needs.

Pick Your Products

There are many options available for security orchestration, and your choices are increasing every few months. **To help narrow down those choices, start with identifying what you are really looking for.** Are you looking for high-availability orchestration to support 24/7 operations with a high level of reliability? Or are you trying to automate some repetitive tasks to gain more consistency and/or free up personnel to perform deeper analysis? What tools and processes do you need your orchestrator to integrate with? Are you willing or able to adapt your processes to make better use of SA&O? Once you’ve answered a few of these questions, you can identify key features that you need an orchestrator to support and select products for your test drive that have the best fit for you.

What type of organization are you supporting?

Is it a fairly large, well-resourced SOC with tens of people working around the clock? Is it a smaller organization that is unlikely to buy a high-end SA&O solution, but needs some degree of automation to better use the tools you have? Are you geographically co-located or dispersed? Do you outsource some or all of your security services and need to better interface with your suppliers?

What do you want to automate?

Are you trying to automate repetitive tasks within your organization? Are you looking for better integration and coordination across some or all of your suite of tools? Are you looking for better use of your external data sources and threat intelligence? Are you inundated with data and looking for a more efficient way to make sense of it?

How well-defined or extensive are your current processes?

Do you have well-maintained, rigorous Standard Operating Procedures (SOPs)? Do you have associated training packages or on-line help modules that operations personnel use regularly? Do you have processes that span many parts of your organization? Do you have procedures for most tasks within an organizational unit? Do you have procedures for interactions with elements of your organization? Outside organizations?

Does the product integrate with your operational environment?

Is the product able to natively integrate with desired information sources? If not, are adapters readily available to do so? Does the product natively integrate with other tools used? If not, are adapters readily available and do they provide all of the functionality required? How many of your current or planned tools can you integrate with the product?

What data or services do you want to use?

Do you need to integrate with internal data feeds and services? External data feeds and services? Do your selected products have adapters or connectors that you can use directly? Do they have support to develop custom adapters if you need them? Do you have a playbook to exercise those data feeds and services? Does your product vendor have playbooks you can use?

What type of support do you need?

Do you have technical support staff that will provide the primary support for your tool suite? Do you need an on-demand 24/7 support line? How are patches distributed? Are you part of, or interested in joining, an established community of interest like an ISAC or ISAO? How actively can you participate in community forums? Will you be able to use (and share) documentation and code? Do you want process and playbook examples to use?

Planning Your Test Drive

Once you've decided on a few products, you'll need to think through what resources you'll need to test drive them. Think about what you'll need to evaluate, and also what you think will be different about the products you're evaluating. **By lining up your support and identifying the resources you'll have available ahead of time, you'll be able to maximize what you do once your products are installed and ready for you.** Who in your organization really needs to evaluate them? Do you need to schedule their time or can they do the evaluation as part of their normal workday? Do you need support from system administrators? Do they also need to weigh in on your product selection? What are the key features you need to evaluate? What is unique/different about each orchestrator? What features might be nice to have? Be sure to think about future plans for your organization, too.

How much do you want to put into a test drive?

Are you evaluating just one product? Or 3 or 4? Are you limited to just one or two tasks? Or can you evaluate end-to-end workflows and complex playbooks? What's your test drive timeline? How many resources can you afford to dedicate to the test drive? Have you considered using non-company expertise?

What will you evaluate?

Which workflows will you automate? Can you use/modify existing playbooks or do you need to develop new ones? Are they simple tasks or can you use an end-to-end playbook? Are you evaluating just the product's capabilities? Performance? Or will you also evaluate other factors such as ease of installation? And ease of use?

Who needs to participate?

Who needs to evaluate the product? Will additional personnel be available to support? Which operational personnel need to exercise the product? What support personnel need to be included? Do your support personnel need to evaluate the product as well? Who will you need to coordinate personnel availability with?

How will the product integrate into your operational environment?

If access to tools or information is controlled, can the product use appropriate credentials for accesses? How are those credentials protected? What changes can you make to support integration? How will you transfer information to or from those that can't be integrated?

What support will you need?

What help will the vendor(s) provide before, during, and after your test drive? What internal support will you need to plan, set up, execute, and evaluate your test drive? Will these personnel be directly participating in the test drive? or are they additional?

How will information be exchanged between the vendor(s) and your internal personnel? Who will be evaluating the results?

What are your metrics?

What is most important to you? Do you need to process high volumes of data? Does the workflow have to execute absolutely correctly all of the time? Do you need to ensure that operational personnel can follow what the automation is doing? Ensure that they are not inundated with status messages and alerts? What metrics do your selected products monitor and do those fit your needs?

Setting Up for Your Test Drive

Now you're down to the nuts and bolts of your test drive. You'll need to work out how the products will be tested in your environment. **The more realistic you can be, the better you'll be able to identify benefits and shortfalls.** You will need to set up a test environment, either within your operational environment or separate from it, where you can evaluate all of the features that are most important to you. Focus on the key features you want and how to evaluate them--what data will you use and how will it be segregated from normal operations? Do you need to protect your data? Where will your products be installed? You'll also need to be sure you have evaluation licenses that don't expire until you're finished with your evaluation. Will the test drive require modifications to existing policies and procedures? Keep an objective focus; some results may not come into clear focus until after your test drive is complete. Strive to ensure that your experiments are repeatable.

What data will you use?

Will you be using live data? Do you need to separate it from normal operations data? Do you need to save it so you can repeat the same evaluation (i.e., for different products or different configurations)? Do you need to protect the data? Do you need to create supplementary test data?

What information will you collect?

What information do you need to evaluate? What information (interim and final) will be produced? Where will it be saved? How much space will you need? Does it need to be protected? How will it be segregated from operational information? Is it time sensitive?

How will you measure/compare your products?

What does "good" look like? What features are most important to you? Which ones are "nice to have", but not essential? What measurements/monitoring will you need to have to make a comparison? How will you account for product uniqueness?

What security do you need?

What security is required (for products and data)? How will it be integrated with current security practices? What security features should be test-driven? Can they be tested with existing security infrastructure?

Where will products be installed and what resources will they need?

Who will install and integrate the product(s) with existing tools? What computing and storage resources are needed and can they be allocated? For how long? Are any approvals required?

Test Driving Your Selected Products

Now you're ready to test drive your products. If possible, you should test a wide range of capabilities, including workflows for simple repetitive tasks, end-to-end workflows resulting in a particular response action, and handling/use of information from external sources. **Orchestration is most effective when it can completely automate from input all the way through to end action.** But we know that's not always possible, so test both fully automated workflows as well as those that need a human to perform some actions. Also, be sure to look at features that may differentiate orchestrators for your environment –what makes one better than another? Be sure to engage with your product vendors while you're test driving—they know the most about their product and can help you make the most of it.

Can you comfortably manage workflows?

Are workflows reasonably straightforward to set up? Are sufficient help/support resources available? Is a catalog of available workflows maintained? Can workflows be tested before deployment? How straightforward is it to modify a workflow? Does the product keep track of changes to workflows? Does the product log workflow activity?

Do workflows execute efficiently and correctly?

Do the workflows work properly? How easy is it to monitor/review workflow execution? If a workflow is unable to execute properly, are appropriate alerts generated so corrective action can be taken? When multiple workflows are executing, can they be prioritized? Does the product scale to support the anticipated workload?

Are reporting/auditing mechanisms sufficient?

What statistics are gathered? Can these be tailored augmented if desired? What reports are generated? How difficult is it to add additional reports? What logs are generated? How easy are they to review? Are they in a standard log format that can be monitored using existing tools?

Does the product perform satisfactory response and recovery actions?

Are desired COAs executed correctly? If unable to execute a COA, or to determine which COA to select, are appropriate alerts generated and useful for appropriate operations personnel? If a response action cannot be executed, are the appropriate personnel notified? If a response action is determined to be inappropriate, can it be rolled back completely? Does the product maintain a history of response actions taken? Can that history be adequately accessed, searched, and filtered when required?

Do security and access control mechanisms work properly?

Is information protected as expected? Do access control mechanisms for external tools and information sources operate as expected? Are you able to properly configure identity and authentication features for both people and host platforms/servers/systems for your organization? Can you adequately monitor and audit these features and their configuration?

Can you adequately monitor the operational state of the SA&O solution?

If a service interruption occurs, is it detected? Can the product be restarted from a previous state? And can it be rolled back to a specific state? If an information source or external tool is unavailable, are the appropriate personnel (including current users) notified and able to take appropriate action?

Evaluating Your Test Drive

After you've completed your test drive, it's time to evaluate your results. **Compare the product(s) to your previously defined criteria.** How did the product(s) perform? Did you like them all, but still can't determine what's best for you? Perhaps you need to take a deeper look at other features provided by each one—maybe you can get more than you hoped for. Did you like none of the products? Maybe you need to think about alternative workflows. Did you consider modifying your processes and procedures to better utilize SA&O? Maybe you need a different set of products. Based on what you learned, do you want to look at another product or two? Were you able to evaluate everything you wanted to look at? If you couldn't actually test drive a feature, can you get information about it in some other way?

What did you like?

Were you able to look at all of the features you wanted to? Were you able to exercise the product in an operationally realistic setting (number of users, quantity of data)? If not, can you get information about its performance in similar environments? Did you have conditional likes? Are those conditions insurmountable?

What didn't you like?

Were these "deal-breakers" or just nice to have? Is there another way you could organize your workflows or configure the product that might work better? Are there realistic alternatives available? How willing is the product vendor to work with you? What upgrades are already planned and when will they be available?

What other features are available?

Are there more product features that will assist you in the future? Is the product vendor supporting a number of organizations similar to yours (similar size, similar mission/business needs)? Are product upgrades coming out regularly?

How is the support?

Was the support provided by the vendor as expected? Better or worse? Were help features (on-line tool tips, FAQs, etc.) useful and comprehensive? Is there a community sharing information about this product? How active is the community? How much information useful to your organization is available?

Evaluate Before You Buy

> *THERE ARE MANY SECURITY AUTOMATION AND ORCHESTRATION PRODUCTS AND SERVICES ON THE MARKET. TEST DRIVING BEFORE YOU BUY IS A CRITICAL STEP IN SELECTING THE BEST PRODUCT FOR YOUR ORGANIZATION.*

Determining the appropriateness of an orchestration product to your organization is critical, but not easy. Taking advantage of trial versions and evaluation licenses is one way to find the products that are the best fit for you, but it takes planning to make the most of any test or evaluation. The guidance provided in this document is intended to help organizations plan for, and execute, successful evaluations of orchestration products.