D3 SECURITY

NEXT-GENERATION SOAR BUYER'S GUIDE

PRESENTED BY D3 SECURITY

WHITEPAPER

BEFORE YOU AND YOUR TEAM BEGIN TO EVALUATE A SOAR PLATFORM, IT'S IMPORTANT TO ANSWER THESE QUESTIONS:

1. Why do we want orchestration and automation?
2. What do we expect from orchestration and automation?
3. How can we prepare to implement a SOAR tool?

I. GETTING STARTED:
WHY DO WE WANT ORCHESTRATION AND AUTOMATION?

There may be a number of reasons you are considering orchestration and automation, but focusing on two or three is a great starting point.

Narrowing down the "why" will help you set expectations for results, remain focused on problem solving, and ultimately, select the right tool.

But, it's up to you to clearly establish why your company is looking to implement a SOAR tool.

ARE YOU TRYING TO:

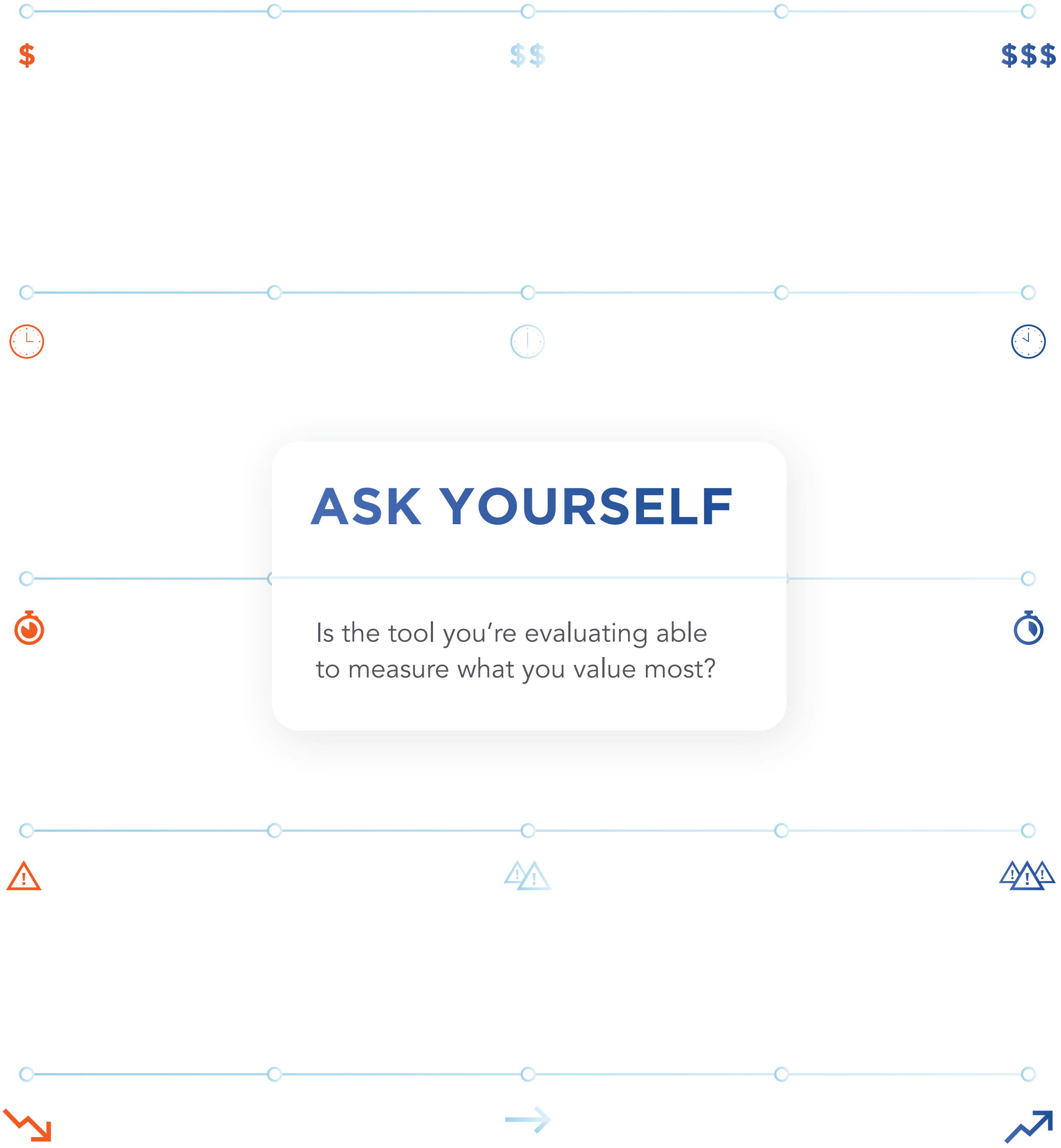
- □ Improve security alert-handling
- □ Streamline analysis and investigations
- □ Guide incident responders
- □ Enhance collaboration
- □ Automate security actions/use cases
- □ Generate SOC and IR metrics
- □ Establish consistent processes
- □ Ease compliance and audit requirements
- □ Reveal gaps and vulnerabilities
- □ Protect against APT groups

II. EXPLORING: HOW WILL YOU MEASURE SUCCESS?

Once you have determined the goal of your orchestration and automation efforts, you need to set expectations. This is also helpful to ensure the tool you select can provide the necessary metrics, trending, and reporting.

DO YOU EXPECT THE SOAR TOOL TO:

- □ Reduce mean-time-to-respond (MTTR)
- □ Generate benchmarks and trending
- □ Automate response to certain incident types
- □ Reduce open and recurring incidents
- □ Reduce manual processing and maximize efficiency of FTEs
- □ Limit investigation/IR costs
- □ Increase SOC visibility for executives



ASK YOURSELF

Is the tool you're evaluating able to measure what you value most?

III. PRE-EVALUATION: QUESTIONS BEFORE VENDOR CONTACT

Now that you have established your expectations and goals, it's time to find, evaluate and select the right tool and vendor for your SOC. Not every tool is alike. And not every vendor has the same capabilities and level of expertise.

Before speaking with a vendor, take a few minutes for a credibility check:

1. DO THEY HAVE A CLIENT BASE OF ENTERPRISE CUSTOMERS?

Look at their website. Do they have client logos and quotes from happy customers? Do they have case studies, whether the customer is identified or anonymized? Do they have a track record of serving customers of your size, in your country or region, and in your industry?

2. IS THEIR PLATFORM "NEXTGEN SOAR?"

What can you tell about their platform? Do they offer codeless integrations and playbooks that enable ease of use and maintenance? Do they leverage a framework like MITRE ATT&CK to support proactive TTP correlation, threat hunting, and gap analysis? Do their workflows support collaboration across departments and user groups?

3. WILL YOU RECEIVE A SATISFACTORY LEVEL OF EXPERTISE?

Is their team staffed with cybersecurity experts? Do they offer 24/7 professional support or do they rely on their user community? Have they been recognized in analyst reports and industry awards? Do they produce expert content regularly?

IV. IN-DEPTH EVALUATION:
QUESTIONS AFTER VENDOR CONTACT

If you determine that a SOAR vendor meets the pre-evaluation criteria, there are simple questions you can ask to dig deeper, in order to see how they match up with your needs:

EXPERIENCE

- □ What is the largest deployment by users/endpoints/integrations
- □ How many clients do you have in my industry
- □ Will a security expert manage my project

ORCHESTRATION & AUTOMATION

- □ How does your tool enable technologies to work together
- □ Is there a codeless playbook editor?
- □ Can human and machine tasks be interwoven
- □ Are incoming events correlated based on tactics, techniques, and procedures (TTPs)
- □ How many integrations are available out of the box
- □ Are my key integrations "certified"

RESPONSE

- □ Is there a full library of incident-specific playbooks
- □ Can I create and edit my own playbooks without vendor support or consultants
- □ Does it support no-code/low-code integrations and playbooks

CASE MANAGEMENT

- □ Can I manage end-to-end forensics and eDiscovery cases
- □ Can privacy, compliance and fraud cases be managed in the tool
- □ Do workflows support collaboration across teams beyond the SOC

REPORTING & DASHBOARDS

- □ Are role-tailored dashboards part of the standard deployment
- □ Can IR processing and SOC metrics be generated
- □ Is there robust trend reporting
- □ Do reports and dashboards include adversary TTPs

AUDIT & COMPLIANCE

□ Can reports be scheduled, or triggered by an event

□ Is there an audit log and chain-of-custody

□ What compliance report templates are built-in

- PCI, SAR/AML, NYCRR, NERC, etc.

PRICING

□ Does pricing increase based on the number of security actions

□ Will future customization result in maintenance or consulting fees

□ Does the product rely on community development and support

ABOUT D3 SECURITY

D3 Security's Next-Generation SOAR platform combines the proactive analysis of MITRE ATT&CK with rapid, end-to-end automation, orchestration and response. Using D3's advanced capabilities, SOC operators around the world have expanded the speed and scale of their security operations, while strengthening their ability to identify suspicious behaviors, conduct efficient investigations, and remediate critical threats.

D3 SECURITY

www.d3security.com

SALES CONTACT

1-800-608-0081 (Ext. 2)
sales@d3security.com

FOLLOW US