Secureworks

SOLUTION BRIEF

Security Orchestration

The Challenge

Increasingly complex security environments that are comprised of a patchwork of security technologies create a heavy burden for security operations teams trying to respond to threats in a timely manner. An overload of alerts makes it nearly impossible to manually cut through all the noise and take the right action.

The Solution

We work with you to reduce the complexity and improve the outcomes of your security operations. We focus on best practice processes to get the most out of the security investments you've made, reduce the noise your security team faces, and improve your time to response.

Click Here to Learn More and Take a Tour of Our Solution

As threats proliferate and security environments increase in complexity, implementing a security orchestration, automation, and response (SOAR) solution is a high priority for many security leaders today. Yet simply buying a commercial off-the-shelf SOAR product can actually compound the issues that drove SOAR adoption in the first place.

SOAR Adoption

Attackers are accelerating the pace of their activities and security operations teams have more tools than ever to manage. This leads to more alerts, more complexity, and more challenges in many security environments. Teams struggle to manually cut through all the noise and take the right action. Using automation to reduce a noisy stream of incidents, consolidate response actions, accelerate investigations, and pinpoint real threats sounds promising.

SOAR, when done right, can make your team exponentially more effective and efficient in responding to incidents. If done wrong, you risk automating processes that don't take full advantage of the tools you have invested in or the skills of your team. Proper implementation requires a deep understanding of the security operations domain.

Yet implementation of automation in a security environment has its challenges;

- not knowing where or how to start,
- a lack of available time and resources to manage months of manual integrations into existing products, and
- uncertainty as to whether or not you're simply scaling poor practices.

Also, misconceptions exist including SOAR being 1) a 'set it and forget it' effort, and/or 2) a workforce replacement.

Our Approach

Secureworks is a recognized industry leader in security operations and incident response. Our approach to SOAR leverages and builds upon experience gained working with thousands of clients over the last two decades. Extracting the most relevant security information from a wide set of security technologies to drive fast, accurate decisions around security threats is in our DNA. We bring this expertise to

Client Benefits

- Respond rapidly to common threat scenarios via push-button containment actions
- Accelerate incident investigations by having the right data at your fingertips
- Simplify operations by consolidating environmental and threat data from your environment and security tools, as well as Secureworks and third-party intelligence sources
- Reduce the noise and zero in on alerts that matter
- Speed time to response by automating repetitive tasks
- Maximize your existing technology investments

Solution Features

- Up-front consultation on best practices
- Automation of client-approved playbooks
- Access to Incident Response specialists to advise on actions
- Complete visibility into the security data collected and actions taken through portal dashboards
- Mobile app for notifications and approvals
- Ongoing consultative review of workflows

your environment, challenge your existing processes, outline best practices, and align on the best path forward for your business through improved processes and appropriate automation.

Our goal is to simplify the noise, accelerate response and investigations, and take the right actions faster with you – not to add more complexity for you to manage. We reduce the existing alert burden your security team faces to help validate, contain, and eradicate threats through a combination of security orchestration technology, managed services, and incident response expertise. Our team helps to improve your operational efficiency through the careful use of automation. We start by understanding your unique environment to help you identify the right processes and appropriate automation required to make an impact through orchestration.

Overview

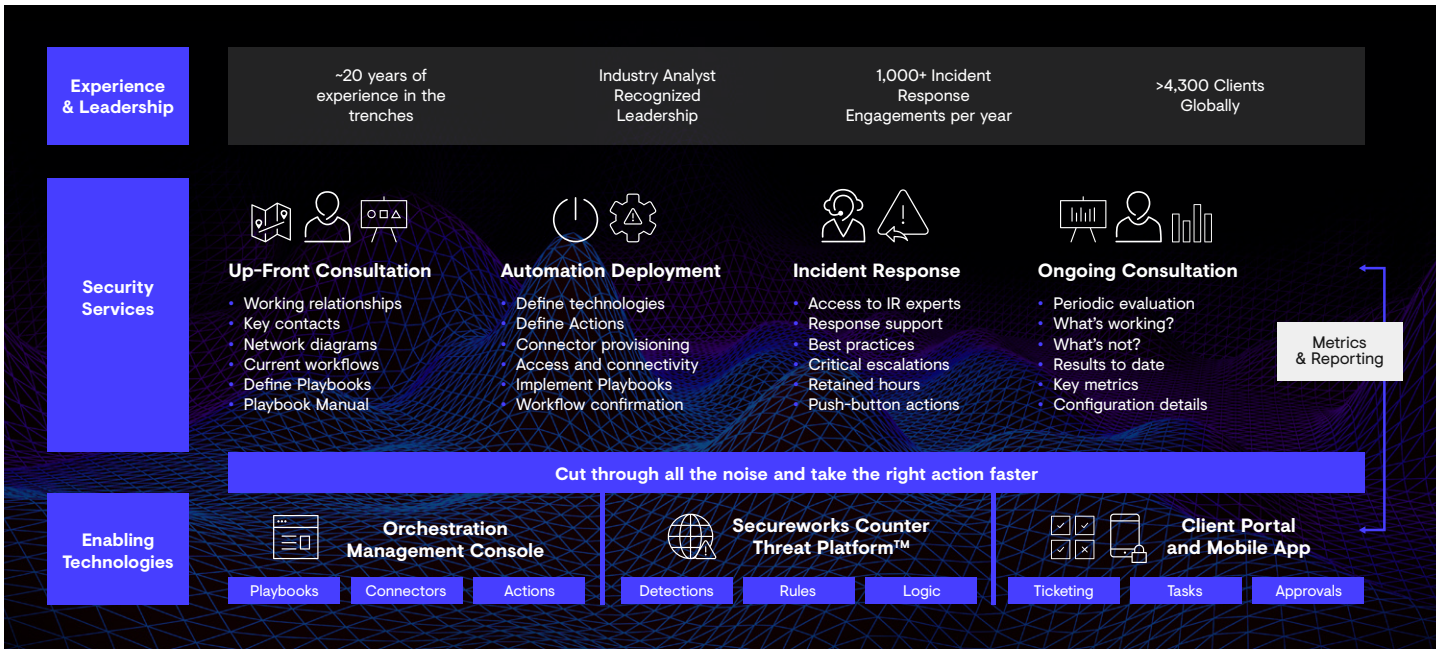
Our technology-enabled managed orchestration solution helps you attain maximum value from your disparate security technologies, ensuring that they are working in concert, and providing your team with the information that matters most. The solution starts with an up-front evaluation of your unique environment and your most common security scenarios. This includes a thorough review of your existing investments in security controls and tooling.

We jointly customize Playbooks to address security scenarios that are tailored to your environment. The Playbooks leverage Connectors and Actions that enrich your security incident data with context from your numerous security tools, track approval workflow before actions are taken, and where desired, automate response to identified threat scenarios. We work with you to investigate and respond to incidents and provide ongoing consultation to measure progress.

All activity is viewable, auditable, and managed from within a set of purpose-built orchestration and automation technologies. With access to our incident response team, you ensure the right actions are taken based on incident types and severity levels. Finally, we provide ongoing support to answer your questions and make improvements over time.

Up-Front Consultation

Orchestration is unique to each client we engage with and success depends on a variety of factors. These include your existing technology and security investments, the nature of Secureworks' Counter Threat Platform™ incidents in your environment, your existing incident response workflows, industry dynamics, and program objectives. At the start of our engagement, we will document your existing procedures and lend hands-on expertise to advise on the best path forward. This engagement ensures you get the most value out of your investment with Secureworks and also allows your direct control over what Playbooks are ultimately deployed.



Automation Deployment

Based on your environment, technologies, processes, and preferences we deploy a set of targeted Playbooks to automate processes across your environment and reduce manual steps that your team conducts today. This phase includes activating the Playbooks that you approve and accelerates the process of investigating, validating, containing, eradicating, and/or preventing the most impactful security incidents. Secureworks Counter Threat Platform incidents trigger Playbooks including malware, exploit attempts, credential compromise, recon scanning, and brute force attempts.

Incident Response

Access to our Incident Response team is included as a critical part of our Orchestration solution. We review your incidents to recommend actions based on our experience. As situations and incidents merit, we will recommend engagement of our incident response team, which is included at no additional cost under a set of retained hours each quarter. Prescriptive response recommendations include push-button actions for you to take based on incident types.

Enabling Technologies

All results and activity such as Actions, Approvals, and Connectors are documented and viewable from dashboards within the Secureworks Client Portal. The Client Portal is integrated with the Secureworks Counter Threat Platform and is accessible from our Mobile App to provide a convenient way to access incident details, take actions, provide approvals, and review outcomes. Metrics and reporting views such as duration of activities help to provide you with an evaluation of your overall return on investment.

Ongoing Value

Secureworks includes a periodic consultative evaluation with our Security Orchestration solution. Not only will we look at your processes and related Playbooks, but we also review new Playbooks, Actions, and/or Connectors. We will focus on reporting results to date based on key metrics and review any changes made to your security environment since the deployment phase. You can also expect ongoing support for service-related questions and configuration details unique to your environment.

Click Here to Learn More and Take a Tour of Our Solution

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com/orchestration

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world. We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Secureworks®