

BREAKING  
**DEFENSE** / *GAME CHANGER*

**Making DoD Security  
Operations Centers  
More Effective:  
Security Automation**

splunk>





# Making DoD Security Operations Centers More Effective: Security Automation

Security orchestration, automation, and response (SOAR) software frees DoD analysts to apply cognitive skills to actually fixing problems.

The Defense Department's most recent National Defense Strategy (NDS) describes a complex military environment characterized by increased global disorder, a decline in the long-standing rules-based international order, myriad threats from rogue states like Iran and North Korea, great power peers like China and Russia, malicious hackers, and terrorists in places like Yemen. One of the military domains where this dynamic is most evident is cyberspace, where bad actors arguably have comparable or better cyber capabilities than us.

"This increasingly complex security environment is defined by rapid technological change, challenges from adversaries in every operating domain, and the impact on current readiness from the longest continuous stretch of armed conflict in our nation's history," the NDS states. "In this environment, there can be no complacency—we must make difficult choices and prioritize what is most important..."

More cybersecurity threats mean more cyberattacks on DoD networks. Essye Miller, former principal deputy for the DoD CIO, said recently that attacks on department networks are surging and that the attack surface is expanding as adversaries target DoD employees working from home during the coronavirus pandemic.

This surge in cyberattacks means that analysts working in DoD information security operations centers (SOCs) are being bombarded with security alerts. With so many events, it's hard for them to differentiate true alerts from false ones, and to determine which events are priorities to address immediately. Through no fault of their own, they end up chasing their tail when their time could be better spent on mission-critical activities that directly support warfighters.

The solution for this domain is automation. While popular in commercial software segments for years—including Salesforce automation, marketing automation, human resources automation, and IT automation—DoD security teams are just beginning to realize the benefits of what's known as security orchestration, automation, and response.

## The Value of Security Automation

"Automation is nothing new to the military. The Defense Department is making great inroads into DevSecOps, for example," explained Drew Church, senior security advisor at Splunk, referring to an agile software development process where software is quickly developed, tested, and improved over weeks and months rather than years. "A key, fundamental concept of DevSecOps is automation. The point of automation in DevSecOps is to bring together different technologies, tools, people, and processes to develop code and get it out to the war fighter more rapidly.

“Automation provides that same capability inside IT operations procedures, security operations procedures, and other business processes,” said Church. “It does this in a reliable and repeatable fashion every time, and at speed and scale.”

Splunk’s SOAR solution is called Phantom. It helps security teams work to identify, analyze, and mitigate threats facing their organizations. It can be used to improve efficiency, shorten incident response times and reduce the growing backlog of security incidents, even when there’s a shortfall of DoD security personnel to analyze the volume of daily security alerts.

### **“Focusing on the bureaucracy of security rather than the actual doing of security limits the effectiveness of security analysts,”**

Phantom does so by integrating teams, processes, and tools, and by automating tasks, orchestrating workflows, and supporting a range of SOC functions to include event and case management, collaboration, and reporting.

In essence, it frees SOC analysts of the usual Tier I-type activities of gathering data from the security information and event management (SIEM) platform, prioritizing these alerts, performing triage to determine if an alert is real or a false alarm, configuring and managing security monitoring tools, and generating trouble tickets.

Instead, Splunk Phantom lets them spend more time on the value-added work of Tier II SOC analysts. This includes actually investigating the trouble tickets, responding to incidents, and leveraging threat intelligence to better understand the threat and be proactive rather than reactive.

“Focusing on the bureaucracy of security rather than the actual doing of security limits the effectiveness of security analysts,” said Church. “Better to free them of the tasks that can be easily automated like reviewing IP addresses, domain names, and URLs so that they can be force multipliers in conducting the thoughtful work needed to protect DoD networks.

“That automation is done for them in Phantom. It let’s analysts focus on investigating and taking remediation or mitigation steps as appropriate. Where humans excel is in actually thinking through a problem. Copying and pasting

from websites, emails, and reports is not the most effective use of a highly paid, resource-limited talent pool.”

### **Integration With Existing SOC Tools**

SOC analysts make their decisions by gathering information. They sometimes review classified military intelligence, but usually they look at a lot of open-source information and data from commercial off-the-shelf products from myriad providers of cybersecurity threat intelligence products.

Some of the common ones that are relevant to the Defense Department include: McAfee’s ePolicy Orchestrator, which the DoD refers to as Host Based Security Systems (HBSS); and Tenable’s Security Center, which is known inside the DoD as Assured Compliance Assessment Solution (ACAS).

Splunk Phantom has more than 300 out-of-the-box integrations with products like HBSS and ACAS.

“Being integrated with each of those products permits the analyst to get the information they need without having to go to another browser window, or another tab, or a different computer,” said Church. “Phantom automatically brings all that data to the analyst. That takes somebody who spends most of their time copying information from page A into system B and lets them make more rapid and accurate determinations about the threat.”

Through the use of APIs (application programming interface), that same integration is also found with government off-the-shelf (GOTs) solutions that haven’t before been integrated with Splunk Phantom because there was never a request to do so. The same goes for a custom app created by a DevSecOps shop like the Air Force’s Kessel Run project in Boston, for example.

Automating these vital but drudgerous processes also pays dividends during both staffing shortfalls and times of surge, and brings consistency to SOC activities. Military service members are constantly rotating and changing duty stations; senior leadership turns over regularly. Contractors have to be relied upon to provide continuity from tour to tour.

That means that SOC processes that were well oiled on a Monday may no longer be operating smoothly on Friday because of a change of command. Or maybe there is a compelling event that grabs everyone’s attention. Or





possibly there are legal or policy requirements that need to be addressed, and though they don't add mission value they still must be completed.

Automation by Splunk Phantom smooths out the bumps associated with those all-to-common scenarios by keeping the flow of vital data moving to where it can be acted upon best.

"The computer's running the marathon for you so that you are free to sprint and swarm on the problems that need the most resources at any particular time," said Church.

### **The Takeaway**

For security analysts, incident handlers/responders, IT operations managers, security operations managers, and forward-leaning business process experts, Splunk Phantom is all about removing barriers so people can

get back to accomplishing the mission, maximizing productivity of skilled personnel and organizations. "For anybody that has a business process, a mission process, an IT operations process, or a security process and wants to free those skilled workers to get back to what you brought them onboard to do, we can help you with that," said Church. "We do that through orchestration, we do that through automation. We bring in collaboration, and we're able to do that at scale because of the value that a company like Splunk brings to the table. By being able to have a rich ecosystem of partners and support across the board, we're able to do that even with differences from organization to organization."

Splunk Phantom addresses technology-based processes, and orchestrates and automates those processes to get people back to doing what they do best.