opentext™ | Cybersecurity

White Paper

ArcSight SOAR for SOC Analyst and Security Engineers

SOC Analyst Challenges Today

There Are a Lot of Repetitive but Mechanical Activities

Lots of similar incidents come in and lots of similar activities are run one after another manually, in order to respond as described in playbooks. Investigation and response activities almost always include repetitive mechanical steps. In this context, mechanical activities are those that analysts prefer to assume, as they have no requirements for intellect. In most SOCs, analysts spend a lot of precious time running through a lot of repetitive but mechanical activities. Repetitive mechanical work is not just time consuming, but also boring. SOC analysts want to improve themselves and be able to utilize their intelligence to help solve puzzles.

Investigation and response activities almost always include repetitive mechanical steps.

There Are More Incidents than Analysts Can Handle

Typical in-house SOC is expected to investigate and respond to tens (if not hundreds) of incidents per day. ArcSight SOAR by OpenText estimates incident numbers are increasing by at least 20% with every year and staffing is not increasing anywhere close. Properly handling just one incident takes a lot of time, IDC's estimation is around 8 full hours per case; this is more or less, just one case per SOC analyst, per day. There is almost never enough human resource on the SOC floor to cover that. Finding and raising good analysts is getting harder every day, even when SOCs allow themselves the budget to hire more.

Some Attacks Start and Finish Before the Analysts Have a Chance to Respond

Attackers are automating as many of the attack stages with modern malware, so most attacks are almost completely automated today. Such an attack can start and finish in less than 15 minutes. Analysts are not able to respond as fast as they are needed. A typical investigation requires the use of 10-15 different tools (e.g., check the business unit of some person on Active Directory, retrieve running files from a particular computer, check active outbound network connections on the border firewall, confirm if a particular employee is in the building, etc.) and analysts require logging in and out of those tools and then manually, running certain command sequences. Many times, SOC analysts cannot even retrieve this data on their own and need to inquire such data from other business units. More and more cases state that the attack is long over before an analyst starts investigating the case.

Delegation to Less Experienced Analysts Is Tough

Incident investigations require access to a lot of different tools, generally with administrative privileges. Delegating as much of the work to less experienced analysts is a challenge. Many times, socs refrain from giving their privileges to their less experienced analysts as any slight error from their part might cause a catastrophe for the organization. Thus, typically seasoned experts are busier than relatively less experienced SOC analysts.

Collaborative Investigations Are Difficult

Most SOCs use some form of Service Desk software (e.g., BMC Remedy, HP Service Manager, RT, etc.) to manage incident cases. Such service desk platforms allow case management to the extent that SOCs can assign cases to different analysts, analysts can record notes, upload files and close tickets. However, the case history on a typical service desk is as solid as the analysts that behind them. A fellow analyst jumping into a case to help needs a debrief from the initial analyst and in this verbal exchange a lot could have been missed or overlooked. Typically, all the commands run and all the responses that an analyst sees are not recorded into the case history; when this is missing, collaboration is tough.

Typically, all the commands run and all the responses that an analyst sees are not recorded into the case history; when this is missing, collaboration is tough.

ARCSIGHT SOAR FOR SOC ANALYSTS

Comes armed with a lot of features and flexibility around implement at ion, ArcSight SOAR becomes the best-known aid for SOC analysts.

ARCSIGHT SOAR AUTOMATES REPETITIVE ACTIVITIES

ArcSight SOAR comes with a powerful automation engine; ArcSight SOAR automation is second to none in the SOAR industry. The engine is capable of running multiple parallel automation workflows, analysts' approvals and decisions, activities involving end users and a plethora of triggers on what to do and when. Out of the box, ArcSight SOAR comes with 100+ different integrations with security, infrastructure and intelligence technologies. Whether it is a very simple IP investigation from multiple cloud intel providers or as complex as investigating and responding to a malware incident end-to-end, ArcSight SOAR automation is there to offload as much as possible. You can start small and witness your growth as your ArcSight SOAR installation and confidence grows.

ARCSIGHT SOAR CAN HELP DECREASE THE ALERT FATIGUE

Multiple ArcSight SOAR users report that it is easily possible to offload some 30-40% of their investigation and response activities to ArcSight SOAR automation, running full and semi-automation. At ArcSight SOAR, we don't believe in full automation and do not believe in a fully automated future. We believe automation can augment and support analysts for agility. Most incidents come from the SIEM used in the SOCs. By analyzing the Top-10 alerts raised by the SIEM and trying to come up with automated playbooks for 3-4 of them helps a lot in decreasing the alert fatigue.

ARCSIGHT SOAR SPEEDS UP INVESTIGATIONS

ArcSight SOAR sports a purpose-built incident management service desk. Using the ArcSight SOAR frontend, analysts can investigate cases and respond to ongoing attacks far faster than doing everything manually on a variety of tools. Instead of using all of these tools independently, it is possible to invoke them through ArcSight SOAR's web interface; such use helps analysts investigate faster, as they no longer need to login and logout to these apps. With the click of a button, it is possible to invoke a particular data gathering function based on the capabilities of whatever tools the SOC is having. Several ArcSight SOAR users report 15-20 times increase in investigation speed.

ARCSIGHT SOAR ALLOWS SAFE DELEGATION OF WORK TO LESS EXPERIENCED SOC ANALYSTS

ArcSight SOAR works as an access gateway to all the tools and capabilities that are within reach of the SOC analysts. ArcSight SOAR's plugin architecture allows different investigative tools to be commanded and controlled from the ArcSight SOAR web interface. The SOC manager can assign particular access to different tools (and even specific capabilities of these tools) to different analysts. The analysts, then, are able to use these tools and capabilities without knowing the credentials or inner workings of these tools.

Analysts love ArcSight SOAR as it creates more time for personal improvement and focus their efforts on what matters most.

ARCSIGHT SOAR FOSTERS ANALYST'S COLLABORATION

ArcSight SOAR records all investigation and response activities of SOC analysts into 'incident timelines'. Such timelines are available for every incident case. The incident timeline records all activities of the analysts along with outputs of every command or inquiry. This timeline feature not only enables accountability and auditability but also allows collaboration between fellow analysts. A new analyst jumping into a case can very quickly get a proper induction on the case and the whole set of details around the case history.

IN A NUTSHELL

ArcSight SOAR allows repetitive activities to be offloaded, investigations to be sped up 15x, allows delegation to junior analysts without compromising security and allows collaborative investigations. Analysts love ArcSight SOAR as it creates more time for personal improvement and focus their efforts on what matters most.

Connect with Us

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.