Security Onion Report Automation Architecture with Skedler

www.skedler.com

Contents

Introduction

Security Incident Management is a crucial part of any MSP or MSSP. It utilizes a combination of appliances, software systems, and human-driven investigation and analysis. The security incident management process typically starts with an alert that an incident has occurred and the engagement of the incident response team. Incident responders will investigate and analyze the incident to determine its scope, assess damages, and develop a mitigation plan.

Preparing reports based on these incidents reported by any SIEM or NSM tool is one of the daily activities of a Security Operations professional. Reports such as Vulnerability Management, Threat Intelligence, etc., can maintain a high level of transparency by showcasing the progress these organizations make by implementing mitigation strategies. Reports also reveal the improvements your efforts brought about and showcase the problems and worst-case scenarios that were prevented.

Report Automation

MSSPs are pressed to deliver seamless, scalable, and automated security services to demonstrate their ability to enforce higher protection standards. The MSSPs need a high degree of automation in their security offerings to protect their clients in the ever-evolving threat landscape.

SOC professionals provide daily summary reports to businesses and clients based on security event analysis such as firewalls, IDS/IPS systems, and security operations, including Incidents and Alerts. It takes a lot of time and effort to manually generate and share reports using code from different sources every day. Another downside is that manual labor can include inconsistency or mistakes. These take out available time from your resources, which would better fit development opportunities such as innovation and remediation. Thus, it is a no-brainer to employ tools such as Skedler to automate high-impact-high-effort tasks such as reporting.

Providing unique solutions such as sharing request status and activity reports can help you establish your expertise. By automating the process, you can ensure that reporting will be done quickly and correctly no matter what happens to your team.

Automating the reporting process for your clients is a no-brainer. It will save your team time, improve your remediation impact, increase employee satisfaction, and provide a new service offering.

Skedler can put your Security Onion, Kibana, and Grafana reports on auto-pilot!

Risk Management

Risk management is a process that seeks to mitigate risk by acknowledging the existing risks, assessing their impact, and planning a response. As organizations understand more and more about the importance of risk mitigation, MSSPs are adding third-party security risk management services to their portfolios. These tools or services simplify risk management information and help with compliance efforts.

Security Onion is a Linux distro for Intrusion Detection, Network Security Monitoring, and Log Management. The Ubuntu-based distribution contains many security tools such as Snort, Bro, OSSEC, Sguil, Squert, etc. It allows an analyst to configure and run an intrusion detection system with complete monitoring and reporting capability in a few minutes. Security Onion uses Kibana for data visualization. Kibana is a free and open-source interface that lets you visualize your Elasticsearch data and navigate the Elastic stack.

Skedler with Security Onion

Skedler Reports offers the most powerful, flexible, and easy-to-use data monitoring solution that companies use to exceed customer SLAs, achieve compliance, and empower internal IT and business leaders. By using Skedler Reports, you can enjoy the following benefits:

- Simple installation, quick configuration, faster deployment
- Send visually appealing, personalized reports
- Send PDF, PNG, HTML Inline, Excel, or CSV reports on-demand or periodically via email or slack channel.

With Skedler, MSSPs can generate compliance reports (e.g., PCI ASV reports) quickly and efficiently to save countless man-hours, deliver reports 10x faster, and enable their customers to mitigate vulnerabilities more quickly. You can use filters to create specific reports for specific projects, allow users from high-level executives to technicians, and schedule reports to be delivered at any time.

Connect Skedler with Security Onion

Connecting Skedler with Security Onion can be completed in a matter of seconds. As Security Onion uses Kibana for visualization, we can use Skedler's integration with Kibana to automate the reports. The steps include adding Elasticsearch and Kibana URL and the credentials for Security Onion, ELK, and Kibana. You can choose if you would like to allow embedded access to every user or use the prompt user option to implement role-based-user-access. The steps include

1. Open Data Sources, select 'Create Datasource,' and select 'Kibana.'
2. Enter the Elastic Search URL and Kibana URL.
3. Choose Security Onion under Authentication Type and enter credentials for the same.
4. Enter Elasticsearch and Kibana credentials
5. Search Limit, Ping configuration, and Request timeouts can be changed under Advanced Option.
6. Click 'Save and Test'

The Security Onion data source is connected and ready to generate reports.

Generate reports from Security Onion using Skedler

To generate reports from the added Kibana dashboard, we can start at 'Reports,' select 'Create Report,' and select 'Visual Report.'

Next, I can connect the Kibana data source and add the Space. I can choose the report and layout types and add the dashboard's load time.

Once the data source is selected, the next three steps will ensure that the report automation is completed:

Report Designing

With Skedler, you can design the report with text, parameters, elements, and images. You can add your company logo to these reports and create more credibility among your customers and other stakeholders. Other options available at the design stage are:

Adding Burst Filter: This filter can use one dashboard and send reports to multiple customers simultaneously based on different dashboard queries.

Selecting Time Window: You can choose between selecting any particular time frame or using the dashboard time window.

Report Scheduling

Once the report design is completed, we can set the Schedule. Here, you can select the recurrence and frequency. You also get the option of adding holidays. The export options include PNG, HTML Inline, Excel, and CSV.

Report Distribution

Skedler allows seamless distribution via Email as well as Slack channel. For the email channel, you can add the recipients and use parameters to customize the subject or body of the email. Similarly, you can select the channel or the direct recipient for Slack to receive these reports upon generation.

These reports can be generated, downloaded, and mailed irrespective of the schedule. You can share the report with any user within the organization. You can also edit the report design or schedule and check the history of these reports.

Conclusion

This document provides users with a reference architecture for Security Onion users to automate Kibana reports using Skedler.

Security Onion is an excellent tool for network security monitoring, and Kibana is a user-friendly open interface for visualizing Elasticsearch data and navigating the Elastic Stack. Connecting Skedler to Security Onion and Kibana enables users to make the best of both worlds.

Customers and other stakeholders can get automated personalized reports hourly, daily, weekly, or monthly using Skedler. All of these are without a single line of code. Skedler allows its users to save time on manual error-prone reporting duties and focus on areas of innovation and development.