ProtectedIT White Paper

Presenting: Complete SIEM Event Source Integration: A 5 step approach

JUNE 2020

ProtectedIT

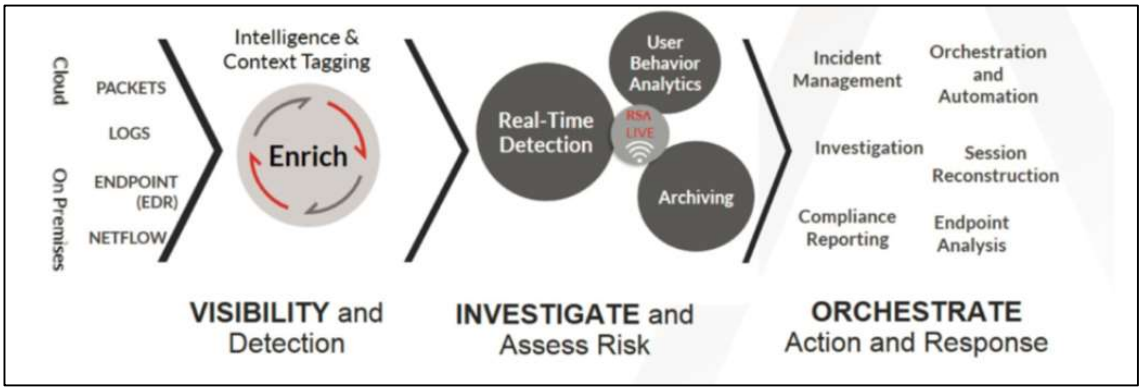
Elevating & Unifying Security Technologies

Complete SIEM Event Source Integration: A 5 step approach

June 2020

A White Paper exclusively produced and presented by the ProtectedIT Engineering Department

The ProtectedIT Engineering Team is committed to providing factual, useful technical content for educational purposes. We hope you enjoy learning and look forward to sharing more soon.



SOURCE: RSA®

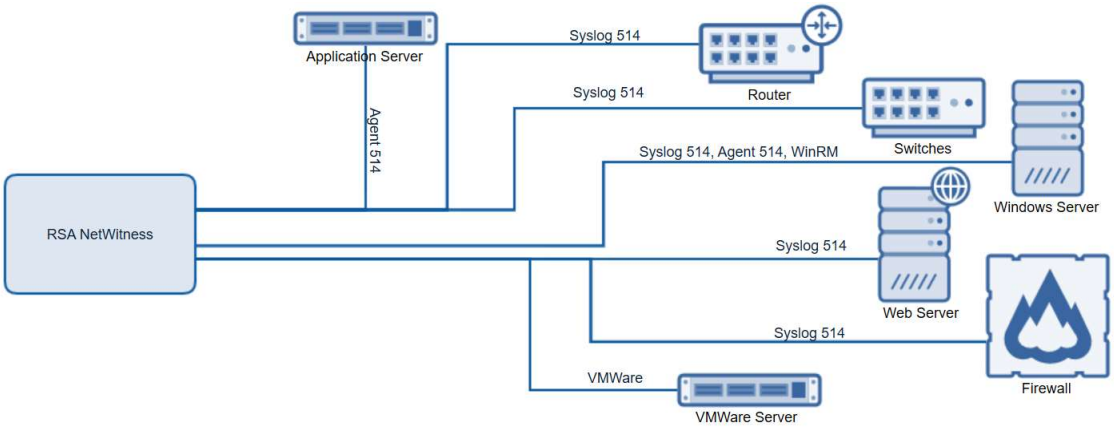
AT-A-GLANCE

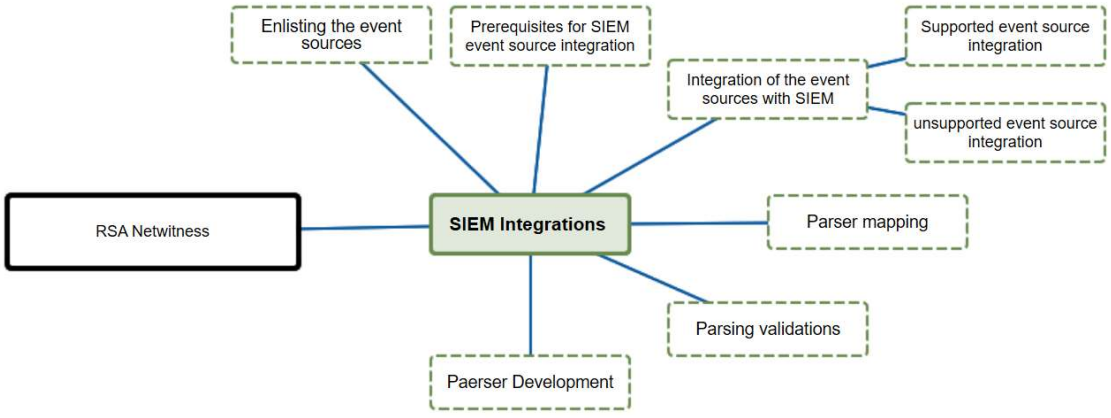
Challenges	**Results**
• Client has SIEM solution, but lacking visibility into logs for all devices. • Custom integration of RSA NetWitness® unsupported event sources. • Device mapping issue for integrated event sources. • Use case development	• Integrated all the event sources with SIEM. Now log visibility is available for all event generators. • Successfully integrated RSA NetWitness® unsupported event sources by custom integration method and built parser to parse collected logs. • Completed device mapping for all integrated event sources. • Developed and deployed use cases based on integrated event sources.

One of the largest government clients of ProtectedIT is utilizing RSA NetWitness® as their Primary Security Information and Event Management (SIEM) solution for their Enterprise-wide security monitoring platform. They are on Version 11.3 of RSA NetWitness®.

The client has a vast variety of Event generators in their environment including Switches, Routers, Firewalls, Application Servers, Virtualization Devices etc. ProtectedIT is providing services to the client for complete SIEM Event Source Integration. ProtectedIT's Senior Security Engineers chalked out a holistic plan for the completion of tasks in 5 detailed phases.

1. Enlisting all the Event Sources
2. Communicating pre-requisites for SIEM Event Source integration
3. Integration of the Event Sources with SIEM for the following types:
    a. Supported Event Source integration
    b. Unsupported Event Source integration
4. Validating out-of-the-box supported parsers
5. Parser development – Required if the Event Sources are not supported Event Sources of RSA NetWitness®





1. **Enlisting Event Sources**:

Client team enlisted all the Event Sources that are required to integrate with RSA NetWitness® Platform and segregated this information based on the type and number of devices.

Client team also shared the sanitized information of the device scope with ProtectedIT along with priority of the Event Sources to be integrated with SIEM. This was to help understand which devices were required to be integrated first. Based on this input from the client, the initial SIEM integration plan was created.

2. **Communicating prerequisites for SIEM Event Source integration to client**:

The detailed scope of the Event Sources which was prepared by the client team helped ProtectedIT team to understand the type of Event Sources available in the client environment. The team then prepared and shared a set of prerequisites and integration guidelines for each device type available in the scope with the client. The prerequisites given to the client talks about the port opening requirements, installation of dependent software like sftp agents and user creation wherever required. For example, Cisco router can be integrated via syslog method and it requires communication over port 514 from Event Source to Log Collector. It also requires syslog destination to be configured on the device in order to forward the logs.

The client environment had a vast variety of Event Sources and not all the Event Sources were officially supported by RSA. Prerequisites were dependent on the type of the Event Source, type of the integration method and whether it was supported by RSA NetWitness®. Once the pre-requisites were completed, the team proceeded to the next phase which was to integrate the Event Sources with the SIEM.

3. **Integration of the Event Sources with SIEM**:

Integration of Event Sources depends on RSA NetWitness® compatibility. Based on this we segregated all the Event Sources in below categories

- RSA Supported Event Sources
- RSA Unsupported Event Sources

RSA NetWitness® supported Event Sources are those for which the supported integration methods as well as the parsers are available by default in RSA NetWitness®.

On the other hand, unsupported Event Sources are those which don't have any parsers developed nor are there any integration methods provided by RSA. Hence, the team had to validate the possible integration of these Event Sources and it required custom parser development as well.

Once the prerequisites for the SIEM integration was completed, the team started with the next phase which is the integration of the Event Sources.

Based on the list of Event Sources in the client environment, supported devices were integrated using different integration methods supported on RSA NetWitness® like Syslog, VMWare Collection, File, ODBC, checkpoint OPSEC LEA, Windows collection using WinRM, SNMP trap.

Client team integrated some of syslog-based Event Sources with the support of device owners. In this case, the team needed to validate the parser mapping and log availability of the integrated Event Sources. The team saw one peculiar issue with the integrated Event Sources without proper parser mapping in place. Logs from one Event Source were getting parsed with several different parsers, creating an ambiguity and parsing issue. So, the team ensured each device that was integrated with client SIEM solution was mapped with appropriate parser in the log decoder.

Special Note: Engineers are advised that they need to ensure that the correct parser mapping is done before the Event Source integration. SIEM integration can be validated by checking the log availability in the SIEM

solution. In this phase, we can see some challenges if the prerequisites are not met – for instance - the required ports between Event Sources and Log Collector are not open.

Once the Event Sources SIEM integration is successful the next step is to verify the parsing.

4. **Validating the parsing**:

In this phase, the team started validating the parsing of all the Event Sources that were integrated with SIEM. If the team noticed any parsing issue with RSA supported Event Sources, they raised a content case with RSA's content team, as RSA creates, upgrades, and manages the supported Event Source parser. One can modify the RSA created parsers; however, it is recommended and a best practice to approach RSA content team for assistance on the supported Event Sources.

For RSA Unsupported Event Sources this step (validating the parsing) will come after the Custom parser development and deployment of the custom parser

5. **Parser development**:

Parser development or UDS (Universal Device Support) activity is required for the Event Sources not officially supported by RSA. At our client site the team noticed more 15 Event Sources that were not supported by RSA.

To develop the parser, there are several steps as mentioned below -

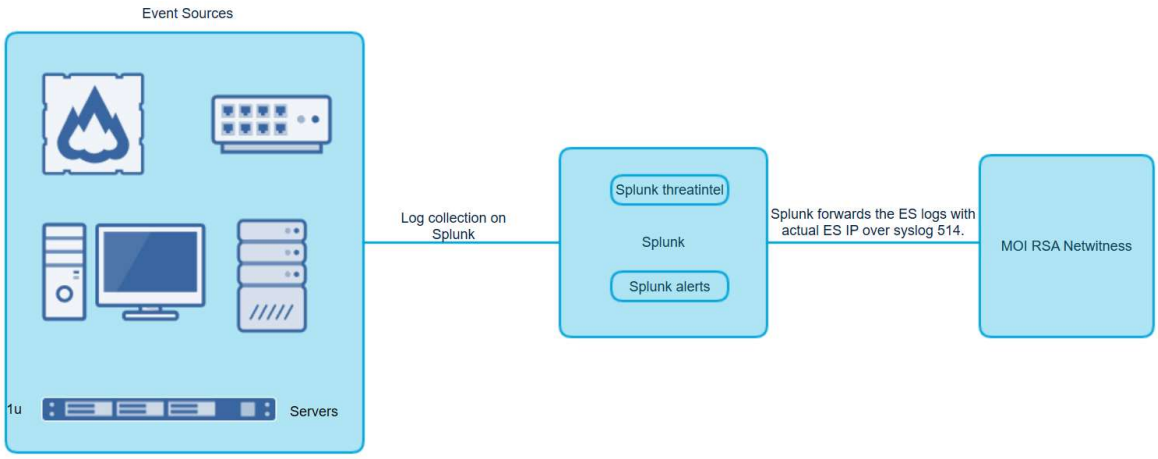
UDS activity steps:

I. Requirement gathering for the UDS activity. That includes below
    a. Sanitized sample raw logs from all Event Sources for parser development.
    b. Discussion with client SOC team to understand the meta mapping requirements.
    c. Documentation about the Event Source log format
II. Developing parsers as per the inputs received from SOC team
III. Testing the parser on the Dev setup or the test bed
IV. Deploying the parser in the client's RSA NetWitness® environment
V. Reviewing the parsing and reiterate from step 1 if required

Future Requirement - Splunk integration with RSA NetWitness®:

The team observed several unsupported Event Sources in the client's environment which were required to be integrated with RSA NetWitness® and Splunk is one among that list. Splunk integration, which is an ongoing UDS integration ask, has the following requirements

1. Event Source Logs received on Splunk solution need to be forwarded to RSA NetWitness® with actual Event Source IP details.
2. Alerts generated on Splunk solution need to be forwarded to RSA NetWitness®.
3. Threat Intel data of Splunk solution needs to be forwarded to RSA NetWitness®.



To accomplish meeting the client requirements, ProtectedIT engineers are reviewing multiple paths to success and will publish findings shortly.

Contact:

ProtectedIT

Manny.chadha@protectedit.net President of India

Karen.bertoli@protectedit.net Chief Marketing Officer +1 305 216 4190