Partner Wire

Keeping Partners in the Know

Dear Partner,

The XDR team recently released two much anticipated features—**Custom Alert Rules** and **Alert Suppression**. Also recently released—**two new tenant roles** to complement the existing user roles.

In addition, in this issue you will find troubleshooting information on collecting logs for Linux and Windows Red Cloak Agent troubleshooting (attachment).

Lastly, we have added a few notes about upcoming feature releases.

Custom Alert Rules

Custom Alert Rules allow you to create a custom rule to match your use case and see alerts generated for that rule.

Custom Alert Rules Documentation

Custom Alert Rules (secureworks.com)

Rules FAQ

Will having rules disabled affect new rules?

Having rules disabled by default at time of creation could cause problems. When you click **Create Rule** and see the green information box display “Rule Created Successfully!”, the rule is not live. You will be directed to the Rules table, which includes a column to show enabled and disabled rules.

Can other users edit/modify rules I create?

Yes, users can modify rules created by other users. The user must be an Admin to create, edit, enable, and disable rules.

Is there a limit to which schemas we can reference in the rule definition?

You can limit any of the event schemas. You cannot, however, reference multiple schemas in one rule or generate alerts from another alert.

Can I filter customer-created rules from analyst workflows?

There is now a toggle to filter customer-created custom rules from analyst workflows. See the training videos below for more information.

Alert Suppression

Alert Suppression allows users to create a new suppression rule to suppress false positive alerts or alerts that have been determined to not be a threat.

Alert Suppression Documentation

Alert Suppression Rules (secureworks.com)

Role-Based Access Control

Taegis™ XDR now supports four tenant roles as defined below. The two new roles are **Auditor** and **Responder**. The primary driver for this change is to ensure that customer success managers, partner success managers, non-technical reviewers can be invited as users into customer and partner tenants to review data and generate reports.

Admin: Administrators are the most powerful users in Taegis XDR. They can access and use all features of the application, as well as manage users and security telemetry, such as integrations and CTU Countermeasures. Secureworks® recommends that the Administrator role be assigned to one person whose primary responsibility is to support the platform as a systems administrator. Organizational roles well suited to the Administrator role include: Systems Administrator, Partner/Product Support.

Analyst: Analysts are primarily responsible for investigating alerts, searching for threats, and recommending response actions. Analysts cannot manage users. Secureworks anticipates that most users would be assigned the Analyst role. Organizational roles well suited to the Analyst role include: Security Analyst, Security Manager, Threat Hunter.

Responder: Like an Analyst, Responders can investigate alerts and search for threats, but they can also take response actions on a defined set of assets within the tenant. Organizational roles well suited to the Responder role include: Incident Responder Team Member, SecOps, Threat Hunter.

Auditor: Auditors have the most limited access within Taegis XDR, as they have read-only access to the application. They can create searches and reports but cannot make changes to the data on their sources. Organizational roles well suited to the Auditor role include: Customer Success Manger, Service Delivery Executive.

	Auditor	**Analyst**	**Responder**	**Admin**
Description	Read-Only Role that can search and build reports but **not** make changes to the security telemetry	Security Analyst primarily responsible for searching and investigating alerts	Security Analyst with added authorization to take response actions (e.g., isolate host)	IT administrator responsible for adding security telemetry (e.g., endpoint, cloud, network data)
View XDR - all data and views	Yes	Yes	Yes	Yes
Update / Download	Download Reports only	Yes	Yes	Yes

Delete	No	Yes	Yes	Yes

Collecting Logs for Linux and Windows Agent Troubleshooting

See the attached *RedCloak Logs for Agent Troubleshooting* document. Also, see this new page on the documentation site regarding Red Cloak Agent Troubleshooting.

Upcoming Feature Releases

Partner Multi-tenancy: Partners will soon have the ability to have their own parent tenant and nest their customers as child tenants. The next Partner Wire will contain release information regarding this feature.

Orchestration: XDR Orchestration recently left beta status and more materials will be available for the next Partner Wire release. Read more on the documentation site.