IBM Security Resilient Security Orchestration, Automation and Response (SOAR) Platform, MSSP add-on

Highlights

- Delivers full multi-tenancy support and multi-tier management
- Provides security orchestration and automation at scale
- Segregates client data, integrations and configuration
- Allows analyst visibility of incidents across multiple clients

Delivering Scale, Visibility and Automation for MSSPs

Managed Security Service Providers (MSSP) are looking to provide their customers with detection and response capabilities as part of a wider service offering. As the number of customers they support grows, and the security incidents they need to investigate increases, managed SIEM and managed detection and response (MDR) providers need to scale their approach to incident response to meet these demands. In order to continue to grow their business and better support existing customers, MSSPs need to scale and automate their response process to reduce the burden on their security analysts and deliver a more predictable level of service for their customers.

An extension of the market leading IBM Security Resilient SOAR Platform, the MSSP add-on has been designed to meet the specific requirements of Managed SIEM and MDR providers. The MSSP add-on gives security operations teams the ability to segment individual client data, playbooks and integrations into siloed, protected environments, all managed via a single Resilient platform to ensure scalability. MSSP security teams are able to quickly and easily review the incident status across multiple clients using new dashboards, and to update response playbooks either across their entire customer base, or for an individual client. The Resilient SOAR platform MSSP add-on delivers the scalability, visibility and predictability that Service Providers need to grow their security business.

The IBM Security SOAR Platform provides customers with case management, orchestration and automation, and human and artificial intelligence to help them to improve their security operations processes, reducing their time to respond to security incidents by automating previously manual processes. SOAR solutions assist with a number of Security Operations Center (SOC) use cases, such as Incident Response and SIEM alert triage. The Resilient MSSP add-on extends these benefits to Systems Integrators and Service Providers who are providing managed security services to their customers. By deploying the Resilient SOAR platform as part of their operational stack, MSSPs are able to address common SOC challenges.

MSSPs need to evolve their services to meet stringent customer service level agreements (SLA) and expectations despite the growth in the number and severity of the alerts they have to manage. They also share the industry-wide challenge of hiring and retaining skilled personnel to staff and maintain their security operations function. The Resilient MSSP add-on is designed to help meet these requirements by delivering the following main elements:

- **New MSSP deployment model** – Clients are able to deploy the MSSP add-on as a single, scalable Resilient system with isolated tenants known as Child orgs. These Child orgs house client-specific configuration information, incident data and integrations, but are managed as part of a single Resilient instance, this has significant scalability advantages as an MSSP can grow their customer base without having to set up and provision additional systems.
- **Global Dashboard** – The Global Dashboard allows the MSSP analyst team to have visibility of incidents across multiple clients. This functionality allows analysts or SOC managers to quickly assess the current state of their entire customer base and drill down into a specific child org in order to work on an individual incident. Granular role-based access control allows the administrator to configure the dashboard settings so that different analyst teams can only see incidents related to clients they are authorized to support.
- **Configuration Manager** – MSSPs need to be able to provide playbook updates across their entire customer base in order to react to emerging threats, as well as to be able to deliver bespoke client customizations. The new Configuration Manager provides the MSSP with this functionality. Playbook and rule updates are configured centrally and can then be pushed selectively, or to all clients as a global playbook update.
- **Metrics and Reporting** - MSSP security teams can track KPIs across the whole system or on a client by client basis. Relevant reporting information such as meantime to respond (MTTR) can be tracked and information can be shared with clients either by exporting it outside of the Resilient platform or by the MSSP providing client access. All data managed by the Resilient platform is tracked and time-stamped, and can be used to create reports and dashboards.

The MSSP add-on for the IBM Security Resilient SOAR platform helps clients meet their service delivery commitments while reducing their operational overheads. Through the use of security orchestration and automation, MSSPs can reduce the manual burden around incident

investigation and enrichment on their analysts, allowing them to manage greater volume.

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations stop threats, prove compliance, and grow securely.

IBM operates one of the broadest and deepest security research, development and delivery organizations. It monitors more than two trillion events per month in more than 130 countries, and holds over 3,000 security patents. To learn more, visit ibm.com/security.

For more information

To learn more about the IBM Security Resilient SOAR Platform MSSP add-on, please contact your IBM representative or IBM Business Partner, or visit the following website(s): https://www.ibm.com/security/intelligent-orchestration/resilient

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.