# SYNCHRONIZING MSSP SECURITY OPERATIONS

MSSPs today face fierce competition for new business, resources and talent in their efforts to monitor thousands of organizations that lack the resources to properly manage the security of their IT environments. Despite advances in technology, MSSPs continue to struggle with an ever-changing threat landscape and a severely-limited talent pool that reduces response times, increases customer churn and shrinks profit margins. These operational challenges have led MSSPs to search for effective, affordable and profitable strategies in order for them to differentiate their services from competitors, manage costs, gain market share and scale security operations.

INTEGRATED SECURITY OPERATIONS PLATFORM

Syncurity IR-Flow is the only Security Orchestration, Automation & Response (SOAR) platform built to help MSSPs address these challenges, reduce risk, improve analyst efficiency and deliver consistent cybersecurity outcomes for their clients. IR-Flow automates time-consuming, manual alert triage and incident response processes, to help analysts identify true positives faster, while significantly reducing false positives. IR-Flow helps analysts move beyond e-mail and spreadsheets by integrating with SIEMs, security tools, and/or ticketing systems to shorten the time it takes to escalate incidents, assign tickets and orchestrate containment and remediation efforts.
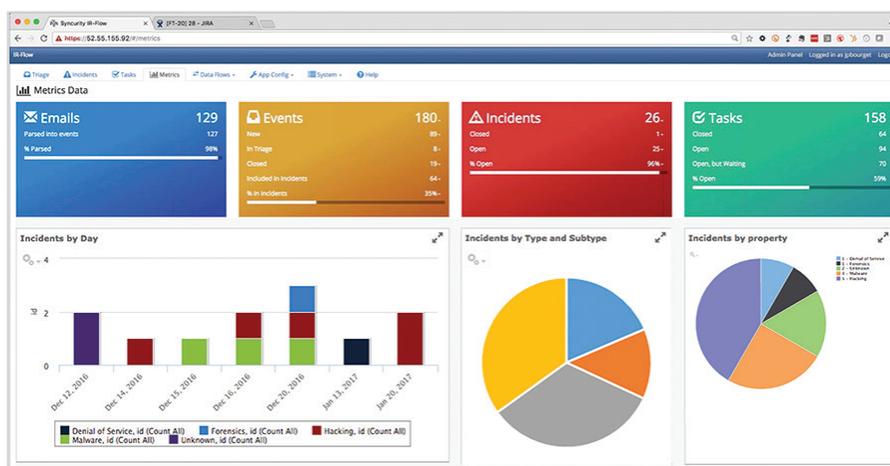
Syncurity's IR-Flow security operations platform helps MSSPs automate and orchestrate incident response to improve analyst efficiency and improve client security outcomes.

BENEFITS

- Increase visibility into client's security and IT environment

- Reduce time-consuming, manual alert triage efforts

- Identify true positives faster and reduce false positives

- Escalate incidents through security integrations not e-mail

- Demonstrate SLA performance with reporting audit trail

FEATURES

- Extensible Data Framework

- Role-Based Access Controls

- Scalable System Architecture

- Segregated Client Data

- Shared-Risk Pricing Structure

1. EXTENSIBLE DATA MODEL AND INTEGRATION FRAMEWORK

Unlike some platforms that require the development of custom Python scripts for each integration, IR-Flow's patent-pending Cyber Translation Framework allows MSSPs to add new integrations with an easy-to-use GUI that simplifies the process of creating new actions through our API. This extensible data model and integration framework allows MSSPs to quickly adapt IR-Flow to each client's unique security stack and IT environment, dramatically simplify ongoing maintenance and support and significantly reduce the time it takes to onboard new clients.

2. GRANULAR, ROLE-BASED ACCESS CONTROLS

IR-Flow's granular, role-based access controls allow administrators to easily assign permissions, create custom fields and display data columns based on each analyst's roles and responsibilities. This allows MSSPs to separate clients, segment users and filter workspace views based on the level of access each analyst has been assigned. Admins can control user access for every field, view, task, alert, incident, report or integration by default or dynamically update privileges as needed to enforce compliance with specified policies and procedures.

3. SCALABLE SYSTEM ARCHITECTURE

IR-Flow's system architecture leverages parallel processing, elastic search and VMWare's ESX environment for 1+n clustering, storage virtualization and backup/recovery services. This setup ensures reasonable response times for hundreds of concurrent users accessing very large data sets. IR-Flow's immutable system of record also provides MSSPs with the confidence that their client data is protected from inadvertent or malicious modification/deletion or unauthorized access that could break chain-of-custody evidence in the event of an audit or legal action.

4. SEGREGATED CLIENT DATA

IR-Flow is available on-premise (VM), in a private cloud (AWS, Azure, GCP, etc.) or in a hybrid approach. This flexibility allows MSSPs to adapt to unique client data residency and multi-tenancy requirements, while maintaining a single pane of glass for operations, integrations, dashboards and reporting. For example, some MSSPs deploy IR-Flow with all client data persistent within the same instance of the database, physically located on-premise in their data center, while other MSSPs deploy IR-Flow in separate private clouds to physically segregate data for each client.

5. SHARED-RISK PRICING STRUCTURE

Unlike some competitors, Syncurity's shared-risk pricing structure allows MSSPs to minimize risk and focus on mutual business growth. Syncurity billing is based on the number of IR-Flow users with credentials and login authorization, not based on the size and number of an MSSP's customers or any other variable. This simple pricing structure provides MSSPs with a stable, predictable cost model that allows for more accurate business and financial planning, without forcing MSSPs to incur undue licensing costs that cause margins to erode when scaling the business.