SYNCURITY
Built by Analysts, For Analysts

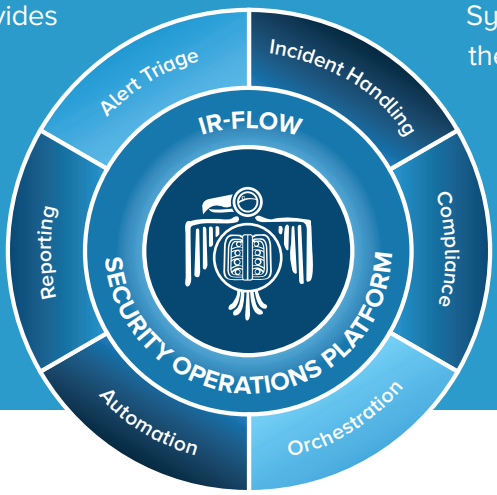
SYNCHRONIZE YOUR SECURITY OPERATIONS

Syncurity's IR-Flow is the only security operations platform built by security analysts for security analysts that combines alert triage and incident handling, security automation and orchestration, and reporting and compliance. Syncurity helps CISOs and SOC managers reduce risk, improve analyst efficiency and deliver consistent cybersecurity outcomes.

IR-FLOW: SECURITY OPERATIONS PLATFORM

SEPARATE ALERTS AND INCIDENTS

Unlike other platforms, Syncurity provides separate queues for alert triage and incident response. IR-Flow improves analyst efficiency and effectiveness by automatically adding context to incoming security alerts and only escalating critical alerts to the incident response team.



BRING YOUR OWN ENTERPRISE

Syncurity allows organizations to adapt their security operations platform to the needs of their enterprise. IR-Flow's customizable security workflows, extensible data model and built-in integration framework easily connects with existing security and IT systems.

INCORPORATE HUMAN INSIGHT

Unlike other security solutions, Syncurity balances analysts and automation to ensure true positives are not missed and false positives are not escalated by a pre-defined incident response algorithm. IR-Flow allows analysts to automate manual, repetitive tasks and focus on critical alerts first by defining custom workflows for each alert and incident type.

IMPLEMENT A SYSTEM OF RECORD

IR-Flow is the only security operations platform purpose-built to serve as an auditable security system of record. Syncurity captures all human and machine-generated events, actions and timestamps for every alert and incident, allowing analysts, managers and executives to generate pre-built reports, reduce risk and demonstrate compliance.

SYNCURITY
Built by Analysts, For Analysts

SYNCHRONIZING SECURITY OPERATIONS

SIEM Alerts, Emails, APIs

1. Detect

- Integrate Data Sources
- Auto-Enrich Alerts
- Shared Work Queue

MANAGE ALERTS IN A CENTRAL LOCATION

IR-Flow helps analysts move beyond e-mail and spreadsheets by ingesting alerts from SIEMs, security tools, and/or ticketing systems via APIs or email into a unified triage queue. Alerts are automatically enriched with relevant context from security tools without requiring analysts to open multiple browser tabs or run command line queries.

Tier 1 Analyst

2. Triage

- Intelligent Prioritization
- Triage Scoring Engine®
- Triage Checklists

PRIORITIZE CRITICAL ALERTS IN SECONDS

Alert handling accounts for more than 80% of all SOC activity. IR-Flow rapidly identifies critical alerts and filters false positives with a patent-pending Triage Scoring Engine.® Analysts validate remaining true positives against pre-defined triage checklists and escalate critical alerts into incidents for investigation.

Tier 2 Analyst

3. Investigate

- Incident Handling
- Custom Playbooks
- Chat & Collaboration

ENFORCE CONSISTENT SECURITY WORKFLOWS

IR-Flow ensures that all analysts implement consistent, repeatable incident response workflows. Quickly codify best practices, policies and procedures into custom playbooks for phishing, malware or ransomware attacks. Syncurity force multiplies your security team, allowing even junior analysts to rapidly adapt to new use cases.

Incident Responder

4. Contain + Remediate

- Case Management
- Threat Intelligence
- Ticketing Systems

RESPOND TO INCIDENTS WITHIN MINUTES

Syncurity allows analysts to manage the entire incident response lifecycle and respond to urgent threats immediately without leaving the IR-Flow interface. Push actions to or pull information from leading threat intelligence, endpoint security and ticketing systems to dramatically reduce time to containment and remediation.

CISO/SOC Manager

5. Report

- Incident Timelines
- Analyst Performance
- Risk Reduction

ENABLE A NEW LEVEL OF VISIBILITY

Unlike most security automation tools, our workflow engine records all event and activity timestamps, enabling IR-Flow to act as an auditable system of record. CISOs and SOC Managers can focus on optimizing operations, demonstrating improvement and reducing business risk while simultaneously enabling better security outcomes.

Syncurity Corporation,
3100 Clarendon Blvd, Suite 200
Arlington, VA 22201 USA

Phone: +1 703 570 4220
E-mail: info@syncurity.net
Website: www.syncurity.net