SOLUTION BRIEF

Respond Quickly to Cyberattacks with IBM Resilient

The cybersecurity landscape is getting more complex. Hackers continue to innovate and business technologies generate increasing amounts of data. These trends are steadily making legacy security monitoring solutions obsolete as they struggle with an inability to scale and ineffective rule-based threat detection techniques.

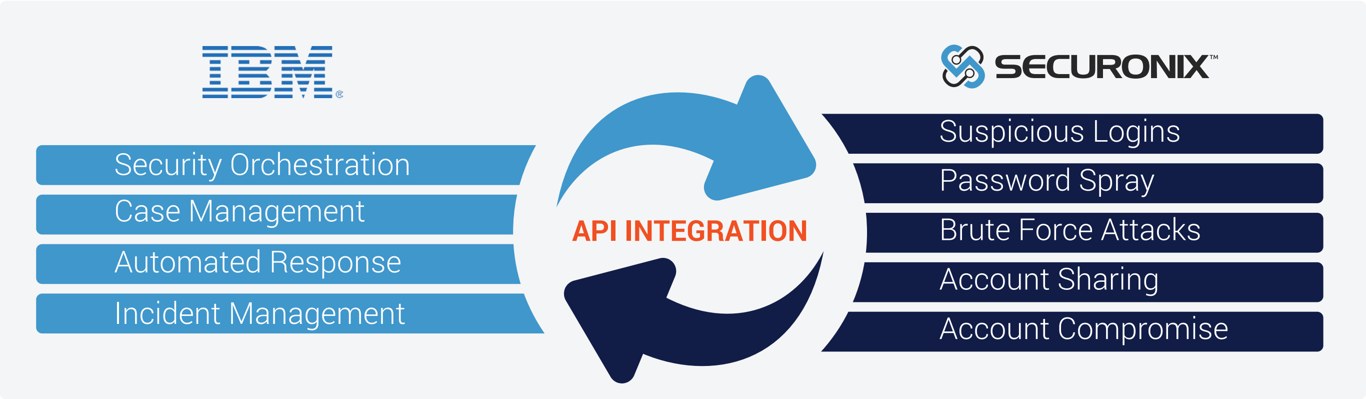
Securonix Next-Generation SIEM transforms big data into actionable security intelligence. It integrates log management, security incident and event management (SIEM), user and entity behavior analytics (UEBA), and intelligent incident response in a single solution that can be deployed in its entirety or in flexible, modular components. It collects massive volumes of data in real time, uses patented machine learning algorithms to detect advanced threats, and provides actionable security intelligence for quick response.

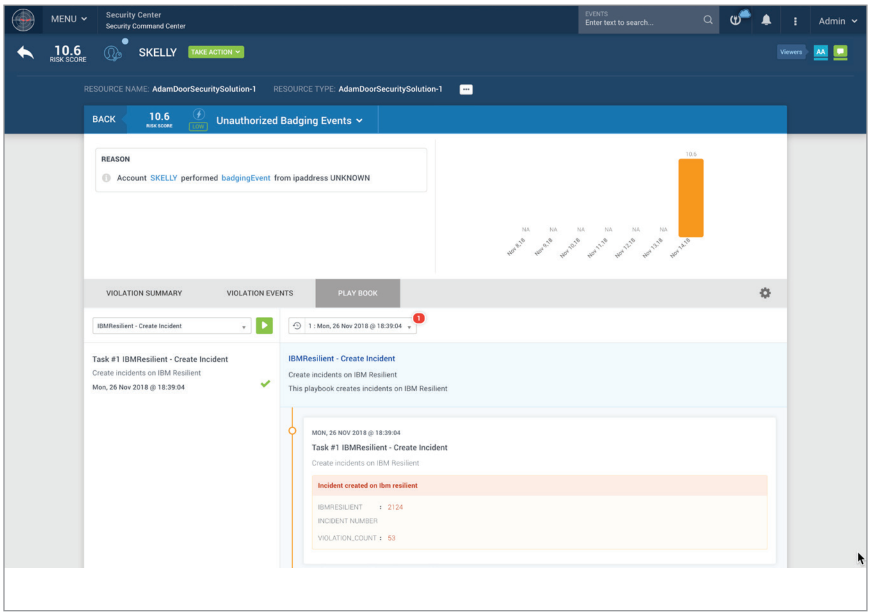
The IBM Resilient Incident Response Platform (IRP) with Intelligent Orchestration seamlessly combines case management, orchestration, automation, and intelligence into a single platform – enabling security teams to deliver a fast, agile, and laser-focused response to complex cyberattacks.

When integrated, Securonix and IBM Resilient deliver world-class comprehensive protection, prevention, and orchestration to handle your organizations' cybersecurity needs. Together, this solution provides you with actionable intelligence on your highest risk threats in real-time, so you have the contextual information you need to take action. Securonix also consolidates all events associated with a threat into a single incident, reducing the noise so you can focus on the threat.

Integration Benefits

- Automated incident creation lets you see threats quicker, so you can act faster.
- Intelligent orchestration, incident case management, and audit trail tracking in one, integrated solution.
- Incident response automation lets you take automated action to respond to security incidents.
- Reduce mean time to respond when you have access to real-time actionable intelligence.





RESOURCE NAME: AdamDoorSecuritySolution-1 RESOURCE TYPE: AdamDoorSecuritySolution-1

REASON

Account SKELLY performed badgingEvent from ipaddress UNKNOWN

Task #1 IBMResilient - Create Incident
Create incidents on IBM Resilient
Mon, 26 Nov 2018 @ 18:39:04 ✓

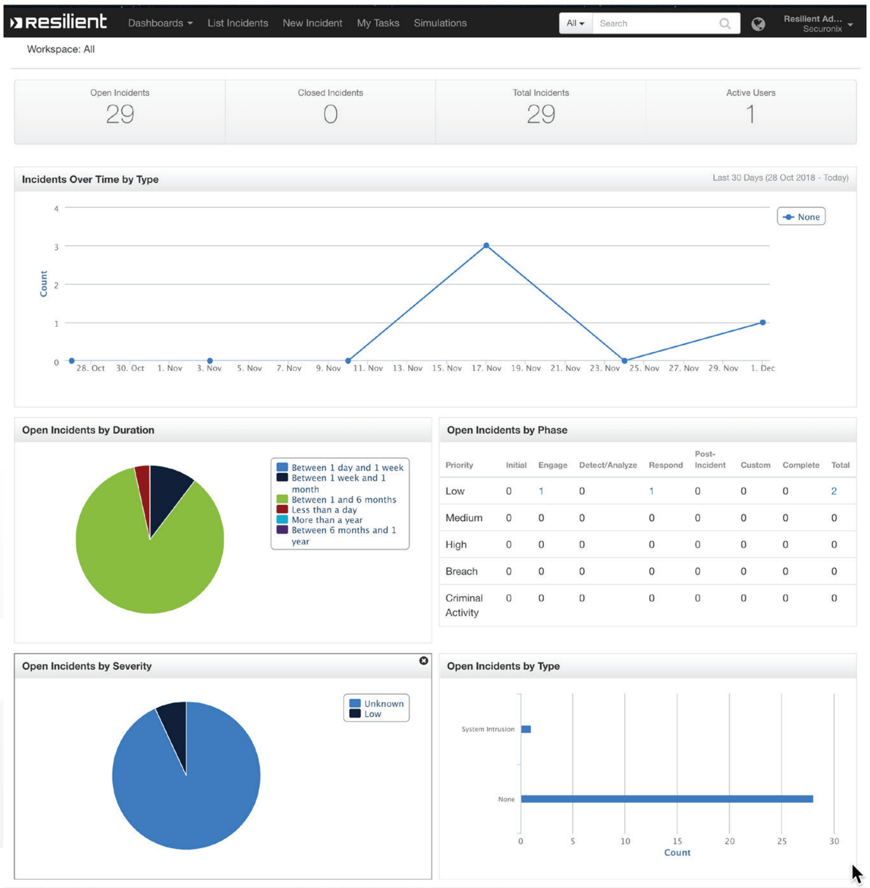
IBMResilient - Create Incident
Create incidents on IBM Resilient
This playbook creates incidents on IBM Resilient

MON, 26 NOV 2018 @ 18:39:04
Task #1 IBMResilient - Create Incident
Create incidents on IBM Resilient

Incident created on Ibm resilient

IBMRESILIENT INCIDENT NUMBER : 2124
VIOLATION_COUNT : 53

Securonix API integration with IBM Resilient provides a playbook to quickly create an incident response case.



Workspace: All

Open Incidents	Closed Incidents	Total Incidents	Active Users
29	0	29	1

Open Incidents by Phase

Priority	Initial	Engage	Detect/Analyze	Respond	Post-Incident	Custom	Complete	Total
Low	0	1	0	1	0	0	0	2
Medium	0	0	0	0	0	0	0	0
High	0	0	0	0	0	0	0	0
Breach	0	0	0	0	0	0	0	0
Criminal Activity	0	0	0	0	0	0	0	0

The IBM Resilient dashboard provides a high-level overview.

How it Works

- Securonix behavior analytics uses self-learning to baseline normal behavior patterns in your user data and detect account misuse and anomalous behaviors.
- With direct API integration, Securonix can be configured to automatically create a ticket in IBM Resilient.
- The IBM Resilient Intelligent Orchestration Engine further centralizes operations while streamlining incident response and automation.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information, visit www.securonix.com.

About IBM

IBM Resilient is the industry leader in helping organizations thrive in the face of any cyberattack or business crisis. IBM Resilient's proven Incident Response Platform (IRP) empowers security teams to analyze, respond to, and mitigate incidents faster, more intelligently, and more efficiently. For more information, visit www.resilientsystems.com

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000

14665 Midway Rd. Suite #100, Addison, TX 75001 | ©2018 Securonix