SENTINELONE AND SYNCURITY IR-FLOW SOAR PLATFORM INTEGRATION

SOC and IR teams find themselves drowning in constant streams of alerts, logs, and data in managing alerts and escalated incidents. Establishing repeatable process, and layering in automation and orchestration, supported by robust case management is becoming a “must have” for enterprises and MSSPs/MDRs grappling with the increasing attack surface (e.g., cloud, mobile) and sophistication of attacks.

Leveraging the SentinelOne EPP and Syncurity IR-Flow SOAR Platform, analysts can leverage the pre-execution, on-execution, and post-execution threat convictions and response actions of SentinelOne with the workflow, automation, orchestration, and case management capabilities of the award-winning, patent-pending, Syncurity IR-Flow SOAR Platform, resulting in a seamless, scalable and dynamic architecture that dramatically reduces the time to detect, validate, contain and remediate threats.

The partnership enables joint customers to easily integrate autonomous endpoint protection into existing security architectures. The joint solution empowers enterprise Security Operations Center (SOC) and Incident Response (IR) teams to detect, assess risk and automatically block validated attacks on endpoints from a single view in conjunction with their other tools. SentinelOne provides more than 200 APIs – the most of any endpoint company – enabling customers to integrate and unify security assets within their environment.

The Syncurity IR-Flow SOAR platform integrates existing security and IT technologies, using repeatable, auditable workflows that provide a dynamic layer of connectivity between them. IR-Flow enables automation for time-consuming and/or repetitive tasks, as well as orchestration across multiple disparate systems and human-required intervention.

SentinelOne uses artificial intelligence to deliver autonomous endpoint protection and automatically eliminates threats in real time. The joint solution helps customers dramatically reduce the security risk lifecycle to identify, validate and stop damaging cyber attacks.

In addition to the robust number of APIs, the SentinelOne Syncurity IR-Flow integration provides support for more than ten proactive actions that empower security teams to better protect their environments. These actions are uniquely independent of the applications calling them, and support alert ingest, data enrichment and risk containment/remediation actions, and enable Analysts to dynamically run endpoint scans, blocking hashes, and quarantining endpoints.

Benefits

- Easily define dynamic workflows for a variety of cyber and IT ops (e.g., patching) use cases
- Ingest and triage activity, event, and alert data from SentinelOne into Syncurity IR-Flow
- Enrich Alert and Incident facts like IP, hashes, filenames, URLs, process detail, machine status, etc. using SentinelOne Deep Visibility telemetry from within Syncurity IR-Flow Playbooks
- Compress Alert triage time using automated playbooks, actions and interactive input
- Ensure Analysts focus on for priority risks using dynamic risk scoring on every enrichment, either human or machine-initiated
- Reduce containment and remediation time using orchestrated and automated Playbooks when one or more Alerts are validated and escalated to an Incident
- Address real-world organizational constraints for Incident response using a combination of direct integration actions to security and IT solutions, human input, and IT ticketing
- Check security policy actions from SentinelOne using easy-to-configure playbooks in Syncurity IR-Flow's Visual Playbook Editor
- Orchestrating SentinelOne convictions, including system rollback, leveraging re-usable Playbooks Tasks, tracked, managed and measured using Syncurity IR-Flow's robust case management

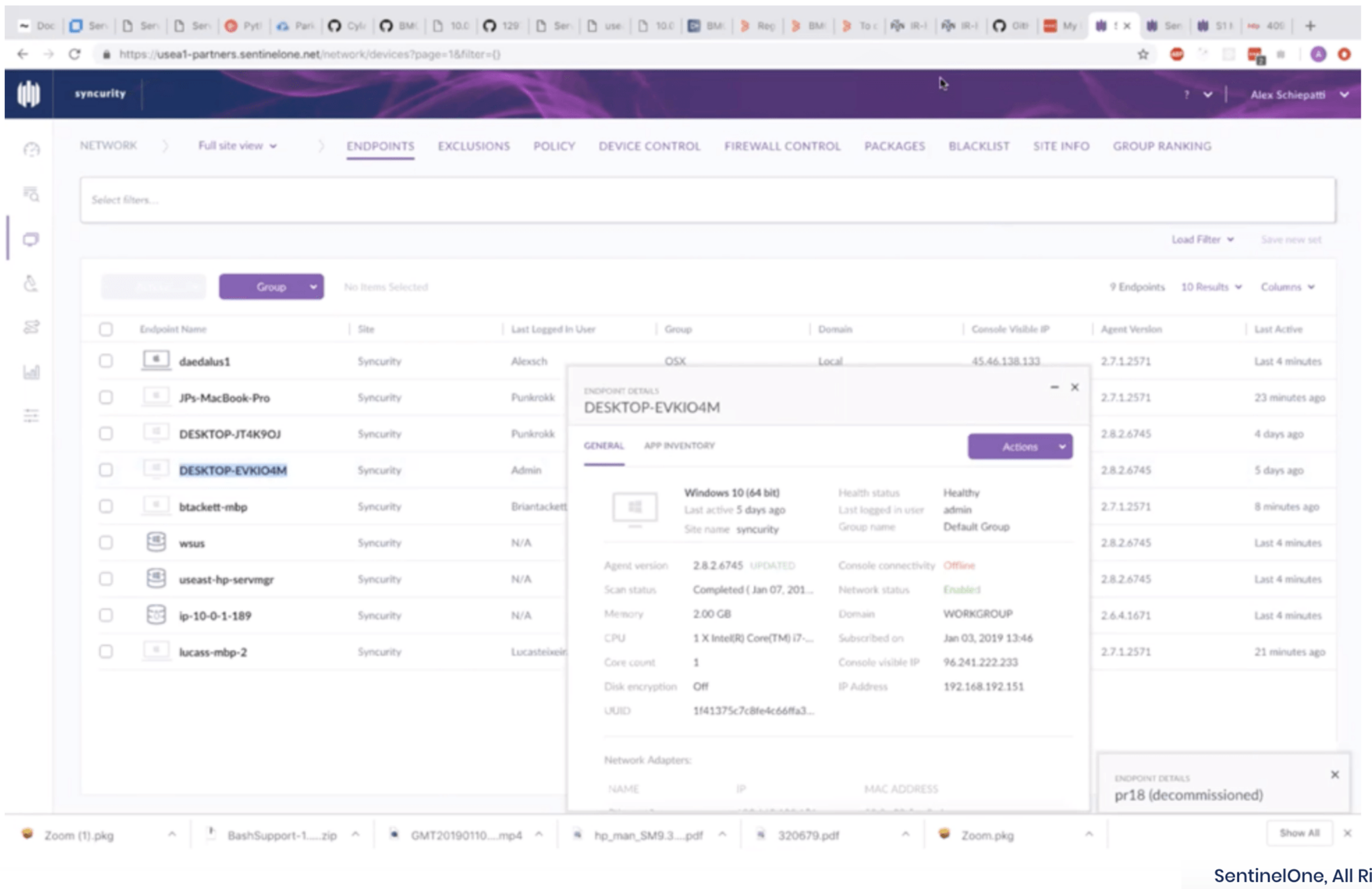
Actions

The SentinelOne IR-Flow integration enables the following actions to perform prevention, detection, remediation, and forensic endpoint management tasks:

- Hash Blocking – Block or unblock a file hash, or check to see if already blocked
- Get Endpoint Info – Discover if an endpoint has SentinelOne agent installed, get useful metadata about host
- List Processes – List the running processes on an endpoint
- Quarantine – Quarantine, or remove from quarantine one or more endpoints
- Scan endpoint – Scan an endpoint for dormant threats
- Mitigate threat – Mitigate identified threat
- Assign or update group to apply different policy

The SentinelOne IR-Flow integration is easy to make operational. All you need is:

1. An instance of Syncurity IR-Flow (private cloud or on-premise)
2. SentinelOne deployment
3. SentinelOne Integration Actions from the secure Syncurity Repository



Fire Action

Actions SentinelOne Get Agent Info

agent daedalus1

Advanced Options

Close | Fire Action

Save Agent Info [redacted] Closed

Steps Add Step

SentinelOne Get Agent Info (SentinelOneGetAgentInfo)

⊢ Active Threats	0
⊢ Agent Version	2.7.1.2571
⊢ Group Name	OSX
⊢ Is Active	False
⊢ Is Up To Date	True
⊢ Mitigation Mode	protect
⊢ OS Name	OS
⊢ OS Version	10.14.1
⊢ Registered At	2018-10-24T20:35:53.659908Z
⊢ User Name	alexsch alexsch