



Red Hat
Ansible Automation
Platform

Automatizovaná bezpečnost

Plně automatizovaná security a compliance vo svete
hybridného cloudu

Jakub Veverka

Senior Solution Architect

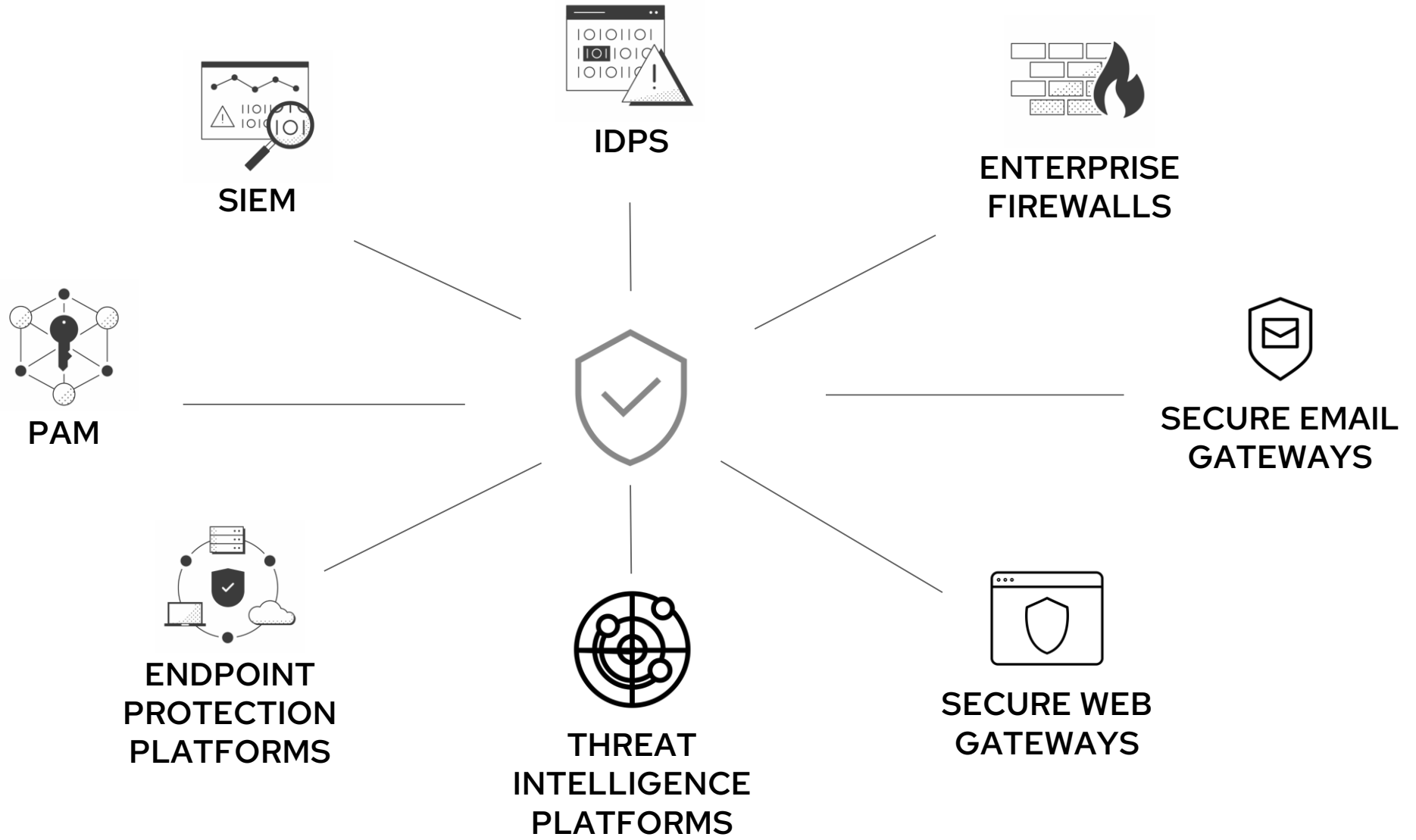
jakub.veverka@redhat.com

“ ”



63% of respondents say their leaders understand that **automation, machine learning, artificial intelligence and orchestration** strengthens cyber resilience.

Ponemon Institute



splunk >

IBM



SIEM



IDPS



FORTINET



ENTERPRISE FIREWALLS



FORTINET



PAM

IBM



Red Hat Ansible Automation Platform



SECURE EMAIL GATEWAYS



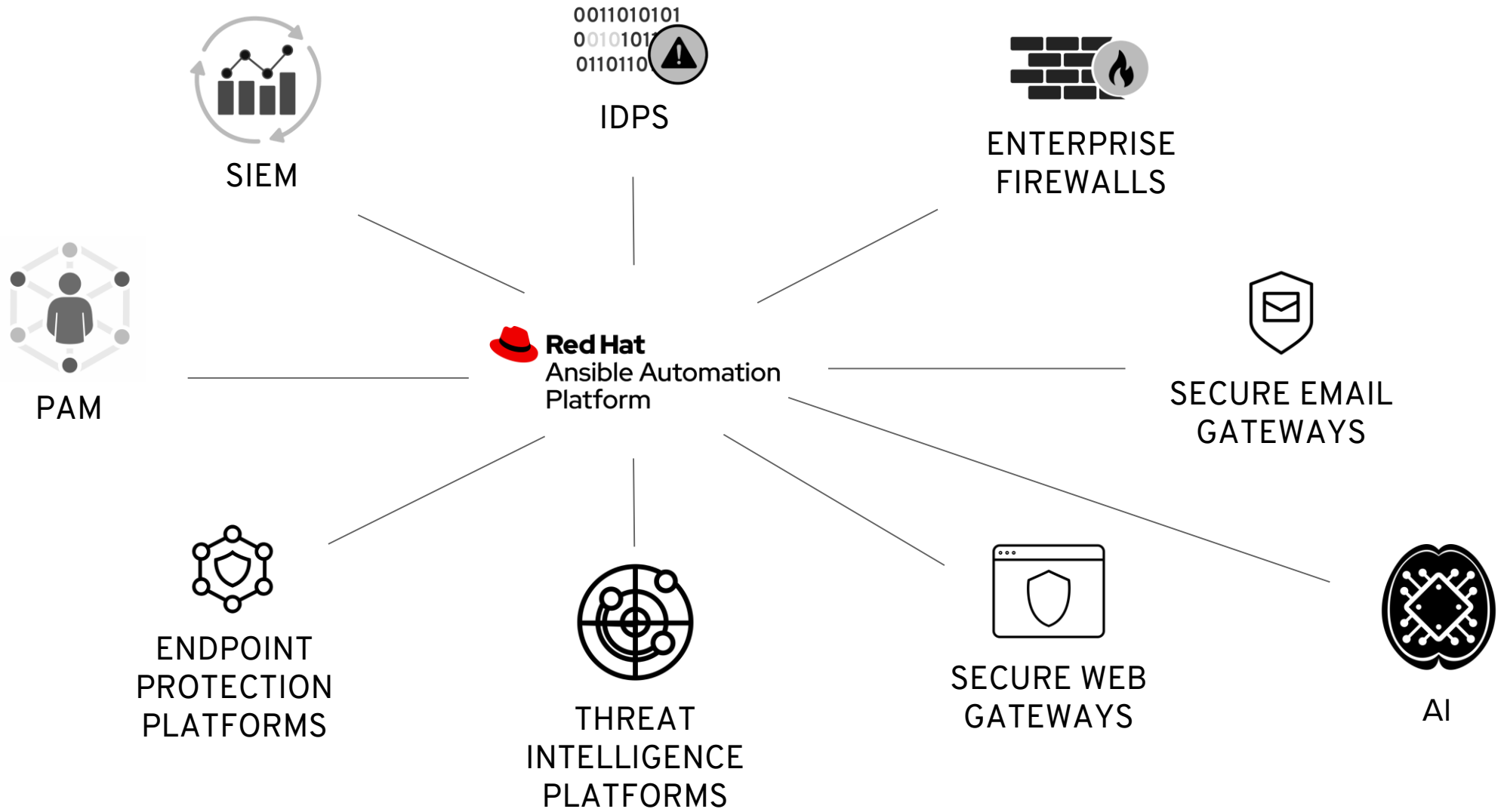
ENDPOINT PROTECTION PLATFORMS




THREAT INTELLIGENCE PLATFORMS



SECURE WEB GATEWAYS



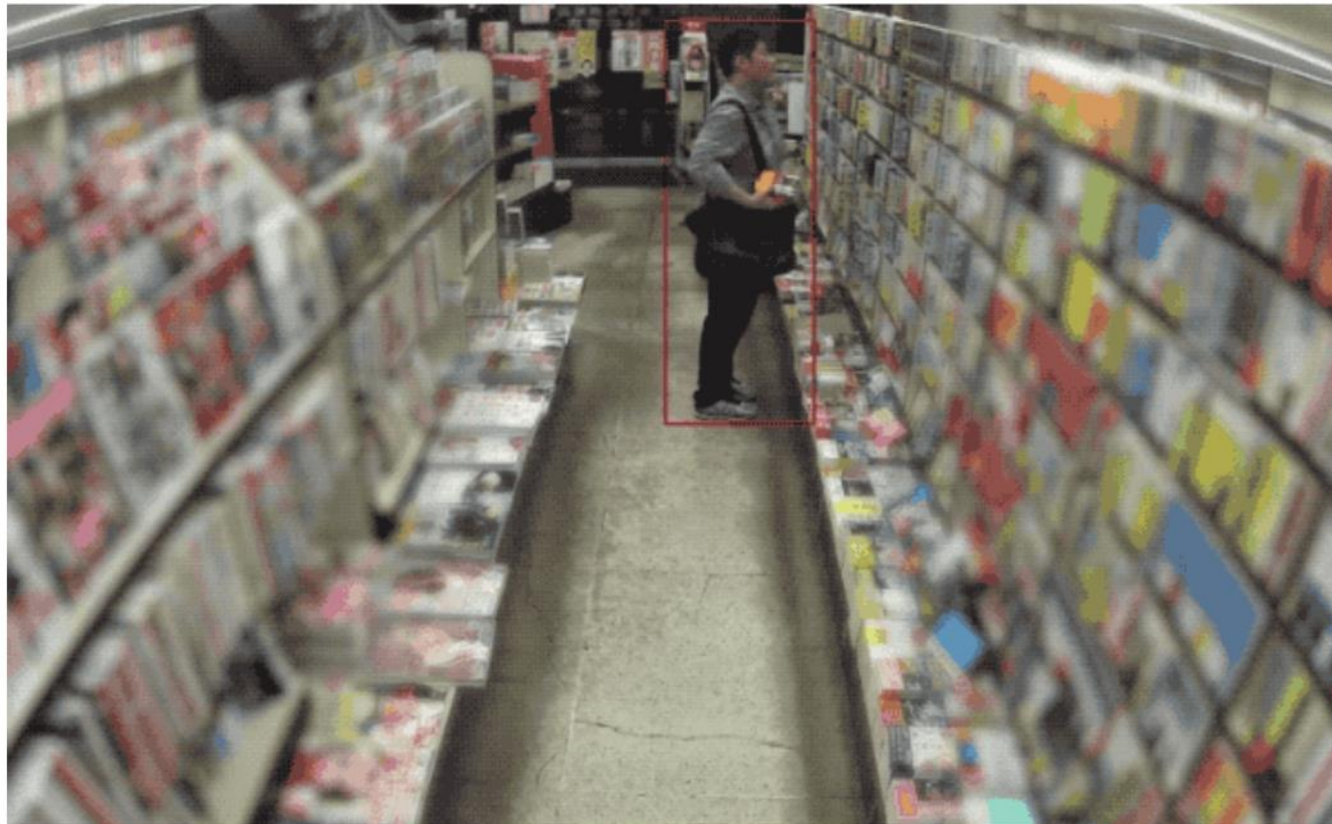
A wide-angle, high-angle photograph of a large industrial warehouse. The floor is a light-colored concrete with yellow safety lines. The warehouse is filled with rows of blue metal shelving units, each with multiple tiers. Many of these units are loaded with cardboard boxes. In the aisles between the shelving units, several orange automated guided vehicles (AGVs) are visible, some carrying a shelving unit. The lighting is bright and even, typical of a large industrial facility. The overall scene depicts a highly organized and automated logistics environment.

**At Cloud Scale
You Have No Choice But
Automate**

This Japanese AI security camera shows the future of surveillance will be automated

By James Vincent | @jjvincent | Jun 26, 2018, 7:31am EDT

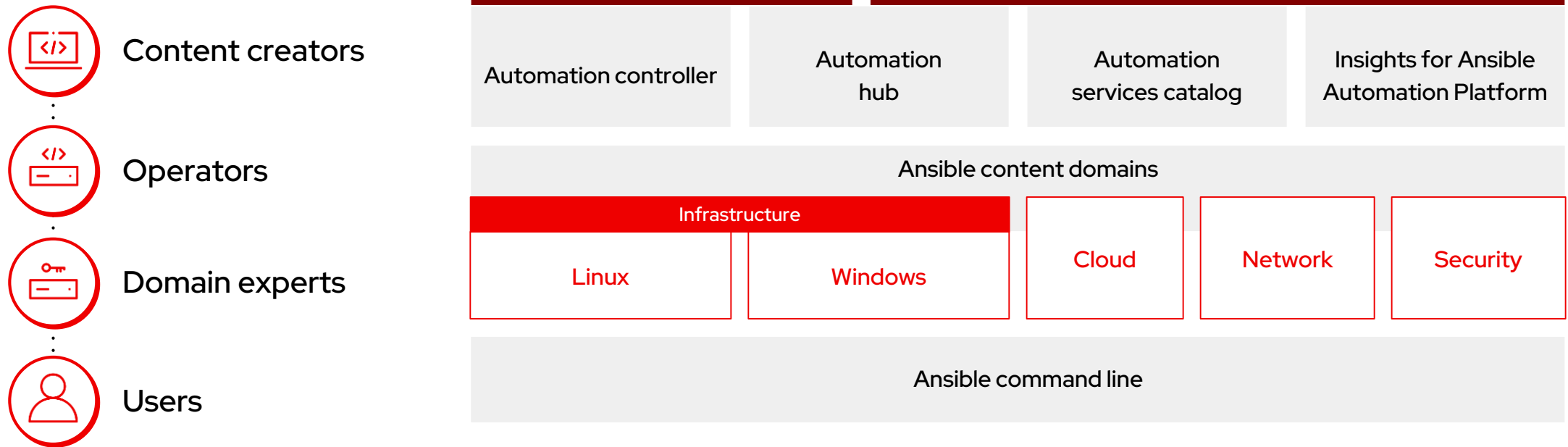
f   SHARE



Introducing Ansible Automation Platform

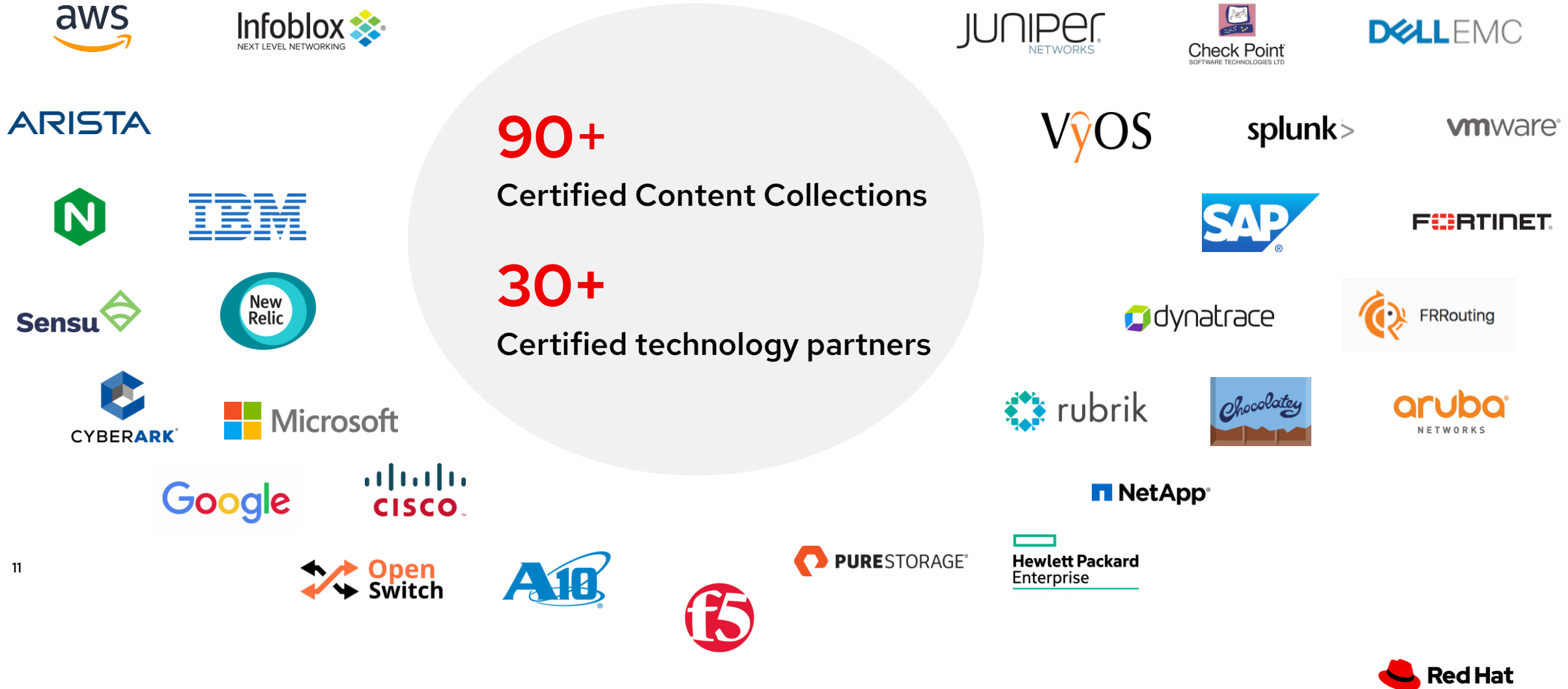
What makes a platform?

Red Hat Ansible Automation Platform



Fueled by an open source community

Red Hat Ansible Automation Platform has a robust ecosystem ...



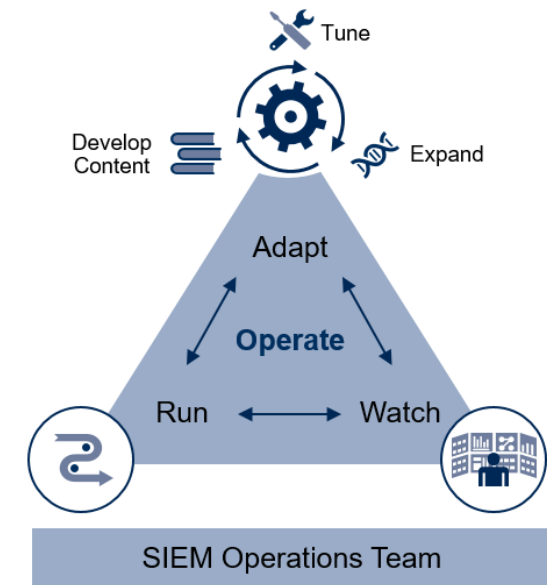
SIEM and SOAR: Why they matter

What is a SIEM?

“”

Gartner defines the security and information event management (SIEM) market by the customer's need to analyze event data in real time for **early detection of targeted attacks and data breaches, and to collect, store, investigate and report on log data for incident response, forensics and regulatory compliance.** SIEM technology aggregates event data produced by security devices, network infrastructure, systems and applications.

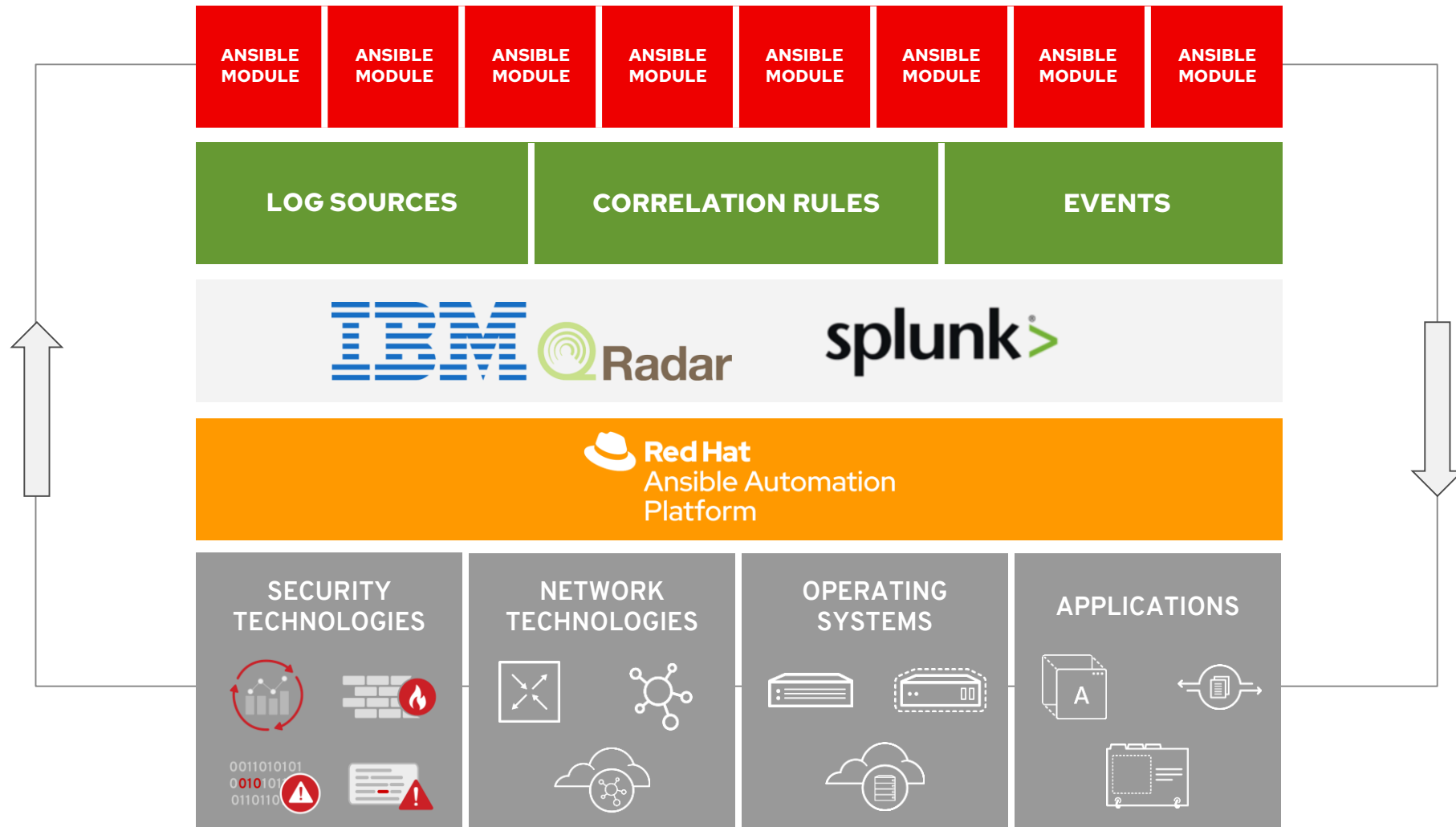
Guidance Framework to Operate and Evolve a SIEM



ID: 366355

© 2018 Gartner, Inc.

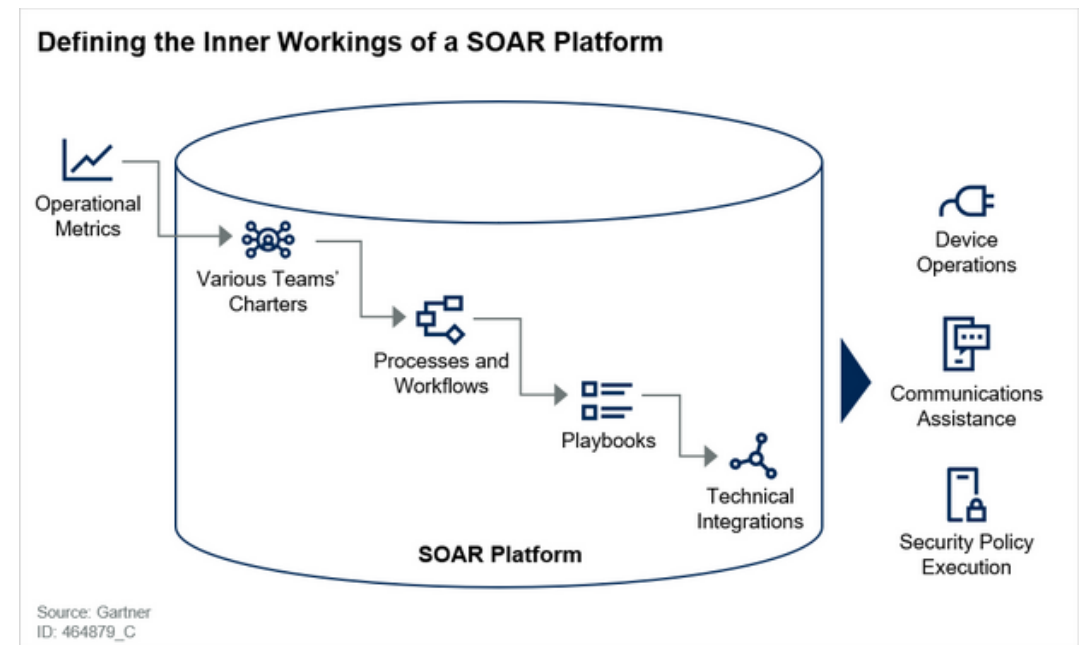
Ansible Automation Platform & SIEM



What is SOAR?

“”

Gartner defines security orchestration, automation and response (SOAR) as technologies that enable organizations to collect security data and alerts from different sources. **SOAR allows incident analysis and triage to be performed leveraging a combination of human and machine power.** This helps define, prioritize and drive standardized incident response activities according to a standard workflow.



How Ansible security automation relates to SOAR?

Ansible security automation **doesn't** compete in the SOAR space.

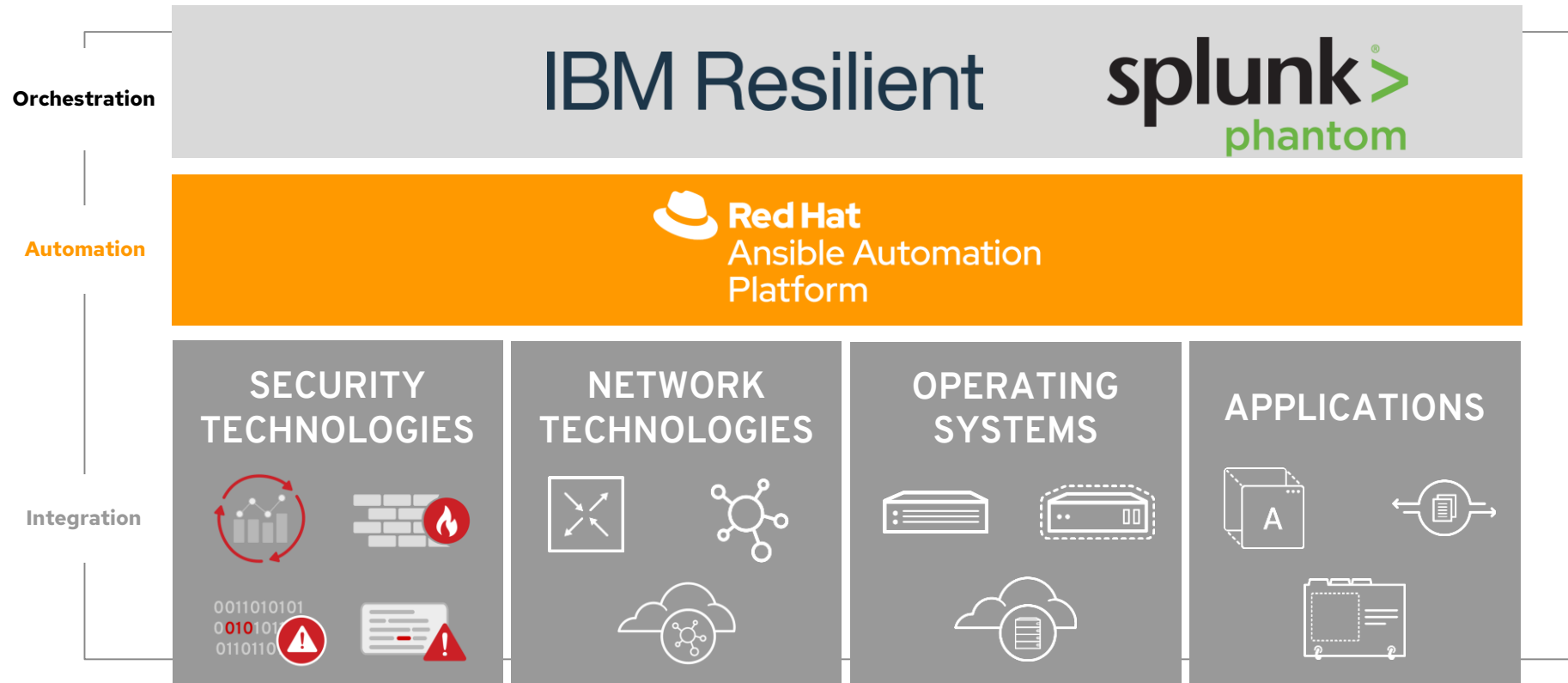
Ansible Automation Platform **complements** and **extends** the custom automation engines included in most SOAR.

The Four Major Engines of a SOAR Platform



Source: Gartner
ID: 464879_C

Ansible Automation Platform Integration With SOAR



Introducing Ansible Security Automation

What Is Ansible security automation?



Ansible security automation is our expansion deeper into the security use case. The goal is to provide a more efficient, streamlined way for security teams to automate their various processes for the identification, search, and response to security events. This is more complex and higher-value than the application of a security baseline (PCI, STIG, CIS) to a server.

Ansible security automation is a supported set of Ansible modules, roles and playbooks designed to unify the security response to cyberattacks.

Is It A Security Solution?

No. Ansible can help Security teams “stitch together” the numerous security solutions and tools already in their IT environment for a more effective cyber defense.



By automating security capabilities, organizations can better unify responses to cyberattacks through the coordination of multiple, disparate security solutions, helping these technologies to act as one in the face of an IT security event.

Red Hat will not become a security vendor, we want to be a security enabler.

What Does It Do?

Through Ansible Security Automation, IT organizations can address multiple popular use cases.



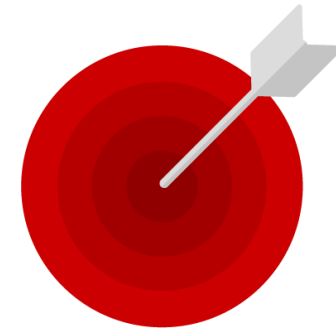
Investigation Enrichment

Enabling programmatic access to log configurations such as destination, verbosity, etc.



Threat Hunting















Automating alerts, correlation searches and signature manipulation



Incident Response

Creating new security policies to whitelist, blacklist or quarantine a machine

How Can You Trigger The Remediation?

WHO	HOW	THROUGH	EXAMPLES
 	<p>Systems with logic on board, such SOAR or SIEM, can trigger actions when a set of conditions are matched.</p> <p>Actions can simply be launching scripts or directly linux commands.</p>	 	<p>Splunk can use <i>custom search command</i> or, <i>custom alert action scripts</i> to execute a perl/python script that calls Ansible Linux command.</p> <p>Through <i>Workflow actions</i> Splunk can call Ansible Tower APIs.</p>
   	<p>Systems with no logic on board, such base firewalls or IDS, has to rely on their underlying OSES, usually Linux-based, to trigger any external action.</p> <p>For those systems a DIY approach is likely to be necessary, using a combination of scripting, OSES' facilities and third party programs to check the conditions and consequently trigger actions.</p>		<p>Snort can output as syslog and use syslog-ng's <i>program()</i> destination combined with a filter.</p> <p>Check Point can schedule a <i>cronjob</i> in the management station.</p>
	<p>Ansible Tower can provide a central point of coordination for all the technologies involved in a remediation process.</p> <p>Ansible Playbooks can be used as security workflows to coordinate actions between different areas of the IT stack and Job Templates can be shared through APIs across different teams.</p>	   	



Investigation Enrichment: Application Behaviour

The Assessment Of Abnormal Behaviours Involves Multiple Steps Like Validating An Ip Address Against Multiple Sources, Searching The Environment For Signs Of Infiltration, Etc. And Then Process And Present The Information To The Security Analyst.



splunk>

Detects an anomaly from the behaviour of an application. Asks Snort & Check Point for more information.



Implements a new rule to collect more information in the affected perimeter.



Raises the level of logging on low level networking perimeter.

splunk>

Consolidates information for the triage.



Restore original configurations.

Incident Response: Sql Injection Attack

Dos Mitigation Requires Up To 10 Manual Steps Between Identification And Remediation.



A *Error Based SQL Injection* event is logged, syslog-ng launches an ansible playbook which exports the log and ships it to Splunk.

splunk >

Ansible module creates a new *notable event*, Splunk ES correlates other sources and confirms it's a SQL Injection attack. Using *adaptive response actions* launches a playbook toward Check Point passing the attacker's IP.



Ansible module creates a new firewall rule to blacklist the IP source of the attack.



After *n* seconds that *Error Based SQL Injection* event disappeared, syslog-ng launches an ansible playbook to update Splunk.

splunk >

Ansible module marks notable event as *Resolved*.

How Do We Get There?

- Reconsider automation as a strategic defense, not just another tactical tool
- Discover what automation tools are the most used in your org, and why
- Assess selected tools' capability to mitigate risks of automation
- Include automation software as target for pen-testing
- Pilot automated host and network security for non-critical applications
- Evaluate feasibility of centralized automation and lock down of platforms against rogue scripting
- Let your automation vendor know what security tools you are using, and how you'd like them to interact with each other
- Pressure security vendors to start integrating with automation tools

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.



[linkedin.com/company/red-hat](https://www.linkedin.com/company/red-hat)



[youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)



[facebook.com/redhatinc](https://www.facebook.com/redhatinc)



twitter.com/RedHat