### **Security Automation**

with IBM Security QRadar and Ansible Automation Platform

### **Parag Pathak**

Team Lead, Product Marketing, IBM Security

#### **Jamie Beck**

Sr. Principal Product Mktg Mgr., Red Hat

### **Adam Miller**

Senior Principal Software Engineer, Red Hat



### 4 pillars of effective SIEM

Complete Visibility

Prioritized
Threat
Detection

Automated Investigations

Integrated Response

Endpoints

Network activity

Data activity

Users and identities

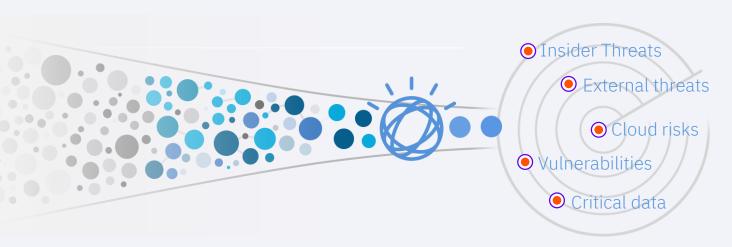
Threat intelligence

Configuration information

Vulnerabilities and threats

Application activity

Cloud platforms



IBM Security / © 2020 IBM Corporation

# How IBM Security QRadar addresses the 4 pillars

# Complete Visibility



- Normalization
- Categorization
- Enrichment
- Network, endpoint, cloud, user and application

Prioritized
Threat
Detection

- MITRF ATT&CK
- Models
- Behavior chaining
- Global threat intelligence

# Automated Investigations



- AT
- Data mining
- Supervised learning
- Unstructured data analysis
- Federated Search

# Integrated Response

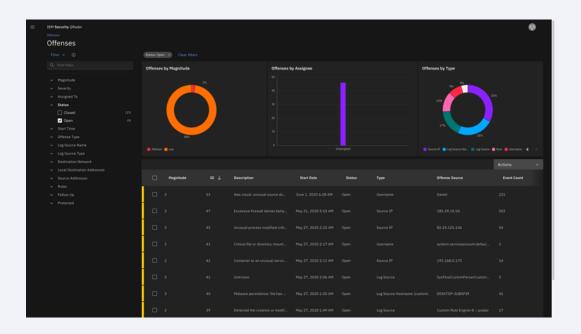


- Dynamic playbooks
- Automation
- Orchestration
- Privacy breach reporting

IBM Security / © 2020 IBM Corporation

# IBM Security QRadar

- **Unify SOC workflows** by effectively addressing threats with an integrated visibility, detection, investigation and response platform
- Augment security staff with AIassisted triage and automated response playbooks
- Mature security operations with visualized use case coverage, OOTB content, and expert threat intelligence powered by IBM's X-Force IRIS
- Address regulatory risk and report on compliance adherence with outof-the-box content for GDPR, ISO 27001, HIPAA, and more



IBM Security / © 2020 IBM Corporation

## Why Ansible?



### Simple

Human readable automation

No special coding skills needed

Hides away complexity

Usable by every team

Makes users productive faster



### Powerful

Configuration management
Deployment & Integration
Workflow orchestration
Multi domain automation

Able to orchestrate complex processes



### Agentless

Agentless architecture
Uses OpenSSH, WinRM, API
No agents to exploit or update
More efficient & secure

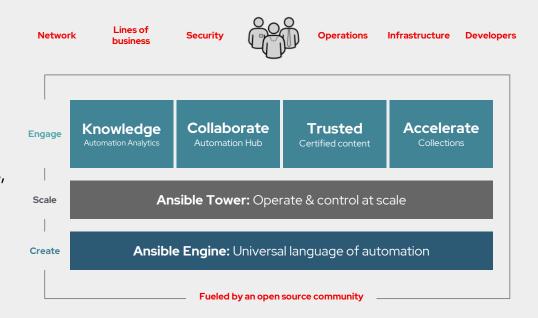
Easier to integrate in existing infrastructures



### What Is Ansible Automation Platform?

#### **Ansible Automation Platform**

is Red Hat's enterprise automation platform to automate the provisioning and configuration of modern enterprise IT environments, from compute resources, like VMs and containers, to networks, all the way to the application layer.





### Why Ansible security automation?









Portion of alerts coming in that the average security team examines every day

Said the time to resolve an incident has grown

Reported increased Severity of attacks Have their ideal securityskilled staffing level, making it the #2 barrier to Cyber resilience

Source:

1 The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute, 2018 (Sponsored by IBM)

2 https://venturebeat.com/2017/12/16/the-lesson-behind-2017s-biggest-enterprise-security-story/



## 6699



**'Lack of automation and orchestration'** ranked second and

'Too many tools that are not integrated' ranked third on the list of SOC challenges.

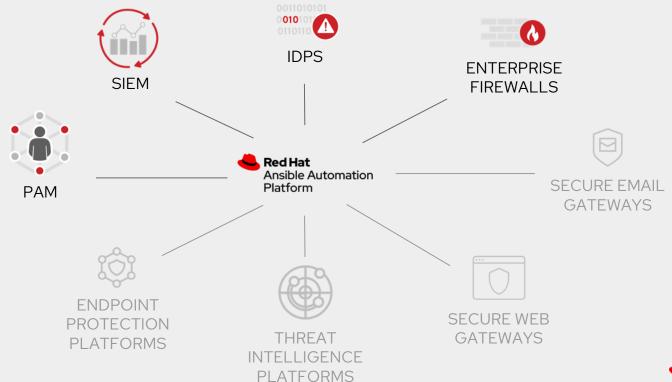
**SANS Institute** 

Source:

The Definition of SOC-cess? SANS 2018 Security Operations Center Survey



## What is Ansible security automation?





## What is Ansible security automation?

Ansible security automation is Ansible 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.

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.

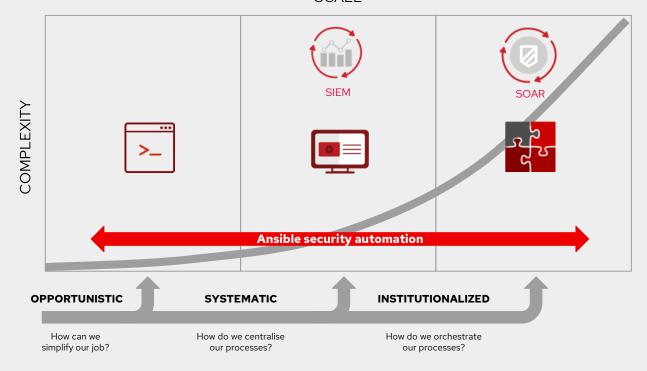


# IBM QRadar & Ansible, better together.

BM Security / © 2020 IBM Corporation

### How customers adopt security automation?

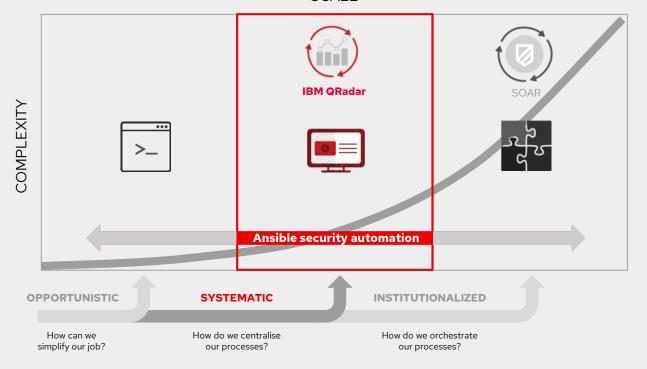
SCALE





### How customers adopt security automation?

SCALE





# Why Ansible Automation Platform + QRadar Better Together



Simplicity

Automate deployment, configuration and mundane tasks

Ansible security automation offers modules to automate the most common and yet onerous tasks, like adding new log sources.

This contributes to lower the running cost of a SIEM freeing up time for Security Operations Centers to focus on more critical activities.



# Why Ansible Automation Platform + QRadar Better Together



Consistency

Interoperate multiple platforms from multiple vendors

Ansible security automation enables management at scale and platform-agnostic operations.

Security Operations Centers can operate consistently across multiple instances IBM QRadar or other SIEMs from different vendors.



# Why Ansible Automation Platform + QRadar Better Together



Modernization

Integrate SIEM in DevSecOps workflows

Ansible security automation modules enable QRadar users to more easily integrate into modern automated workflows.

Response & remediation actions may be triggered in any part of the security organization and potentially outside of it. The Ansible Automation Platform provide a common integration substrate across all the different areas of IT organizations.



# Why Ansible Automation Platform + QRadar Better Together



Extensibility

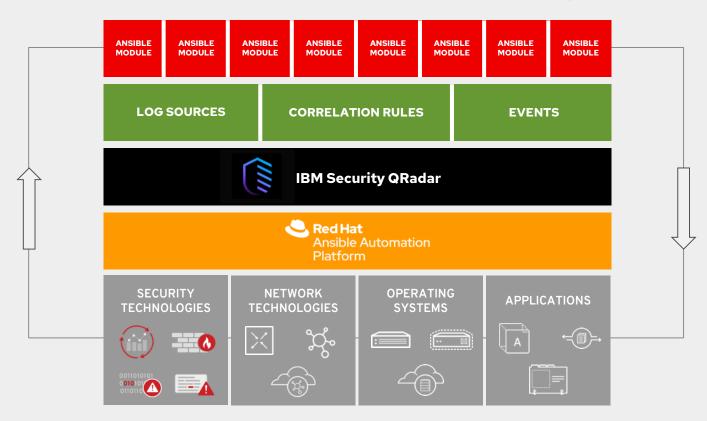
Automate investigation & remediation tasks from the SIEM

Ansible security automation allows security organizations to create pre-approved automation workflows that can be maintained centrally and shared across different teams.

The Ansible Automation Platform can be integrated with IBM QRadar to trigger these workflows directly from the UI, accelerating the response and reducing the operational burden.



### Ansible Automation Platform & QRadar





IBM QRadar and Ansible Automation Platform

# Demo

BM Security / © 2020 IBM Corporation

### Relevant Resources



#### **Get Started**

#### Security automation on ansible.com



https://www.ansible.com/usecases/security-automation



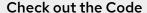
#### Join the Community

#### Security automation community wiki

https://github.com/ansible/community/wiki/Security-Automation

### Blog posts

https://www.ansible.com/blog/topic/ security-automation



Ansible Galaxy

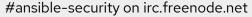
IBM Qradar collection

https://galaxy.ansible.com/ibm/qradar

**Automation Hub** 

IBM Qradar Supported collection

https://cloud.redhat.com/ansible/automation-hub/ibm/qradar





## Questions?



### Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

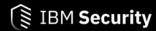
xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

© Copyright IBM Corporation 2020. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty, of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.





# IBM