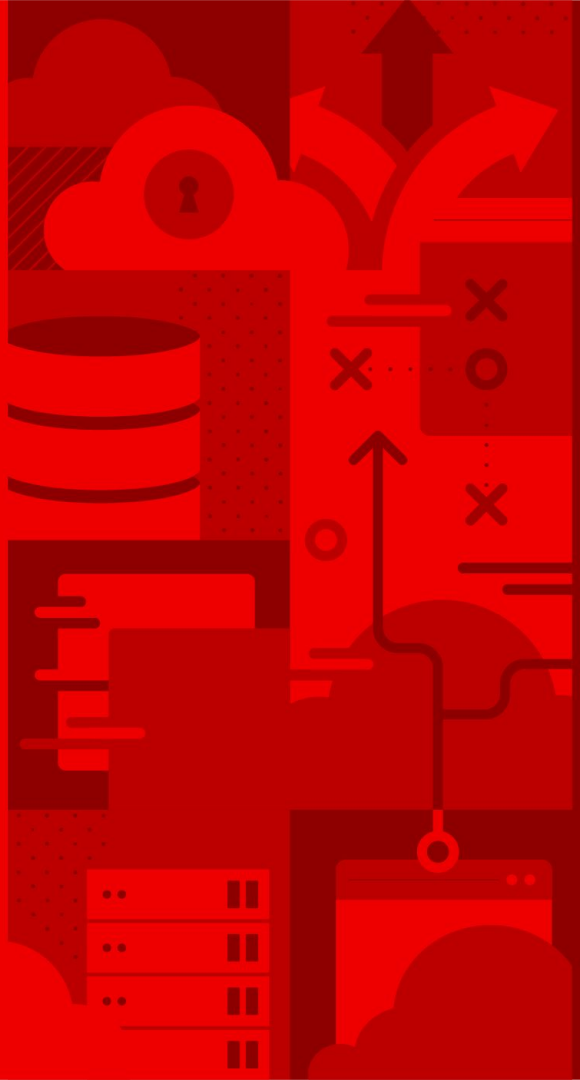
Red Hat
Ansible
Automation

Unifier la réponse de sécurité aux cyberattaques d'une nouvelle manière

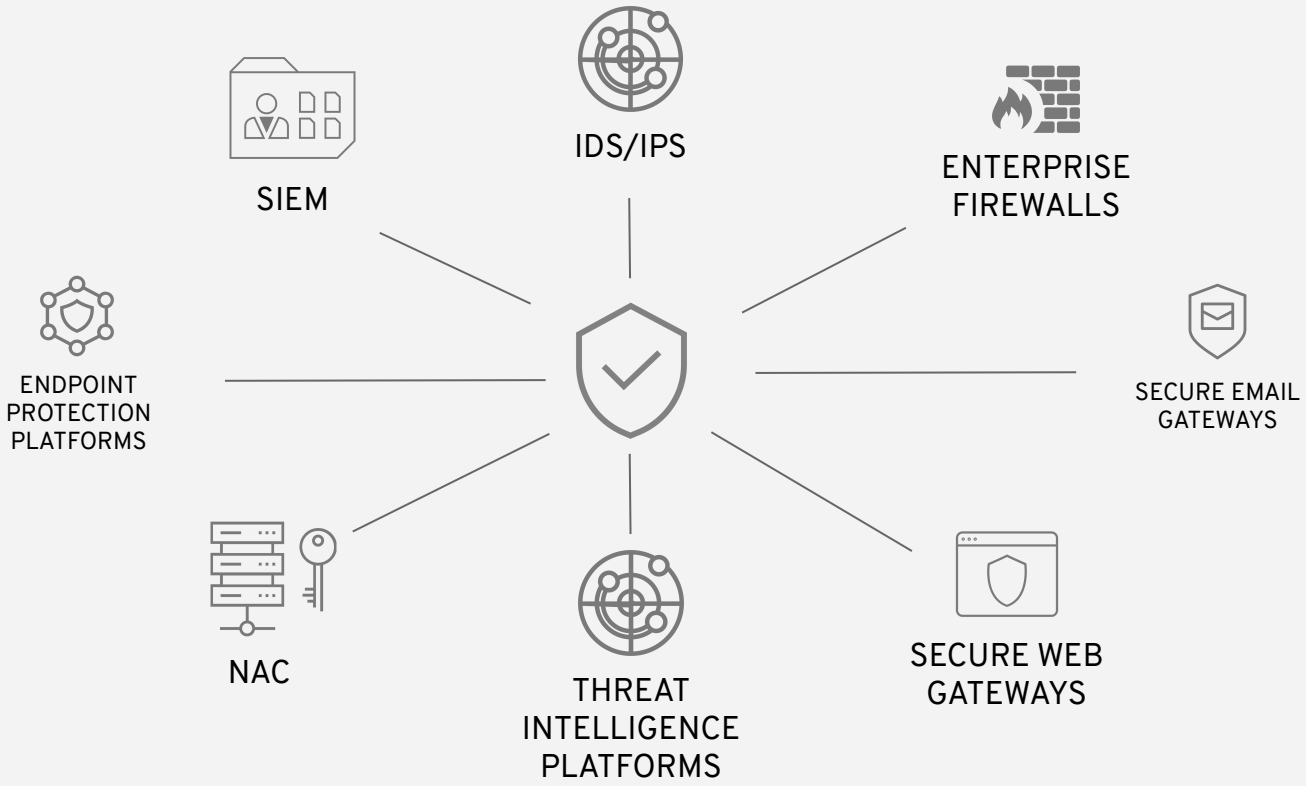
Michael Lessard
Principal Solutions Architect
mlessard@redhat.com
michaellessard

Red Hat

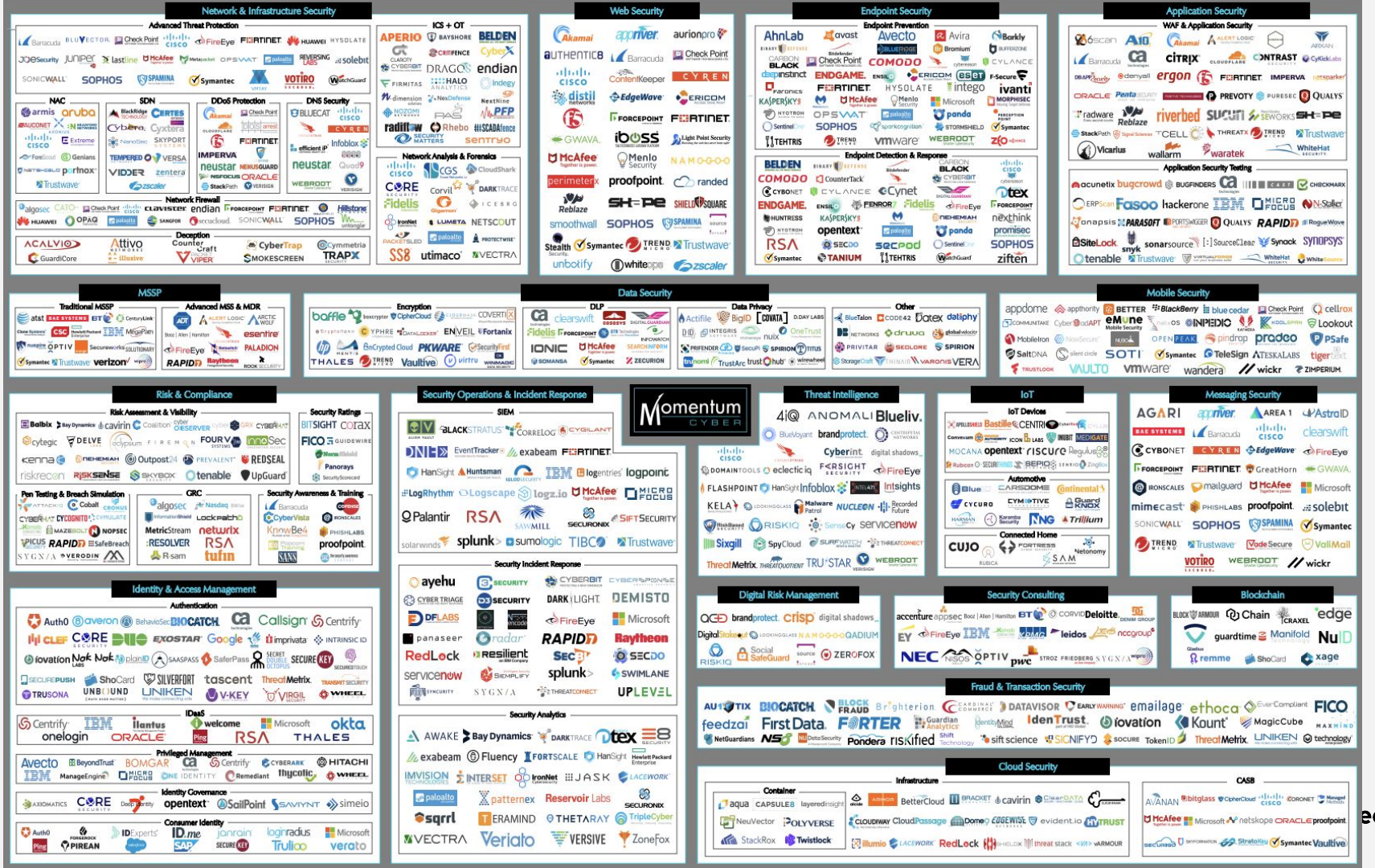


QUE SE PASSE-T-IL ?

Red Hat

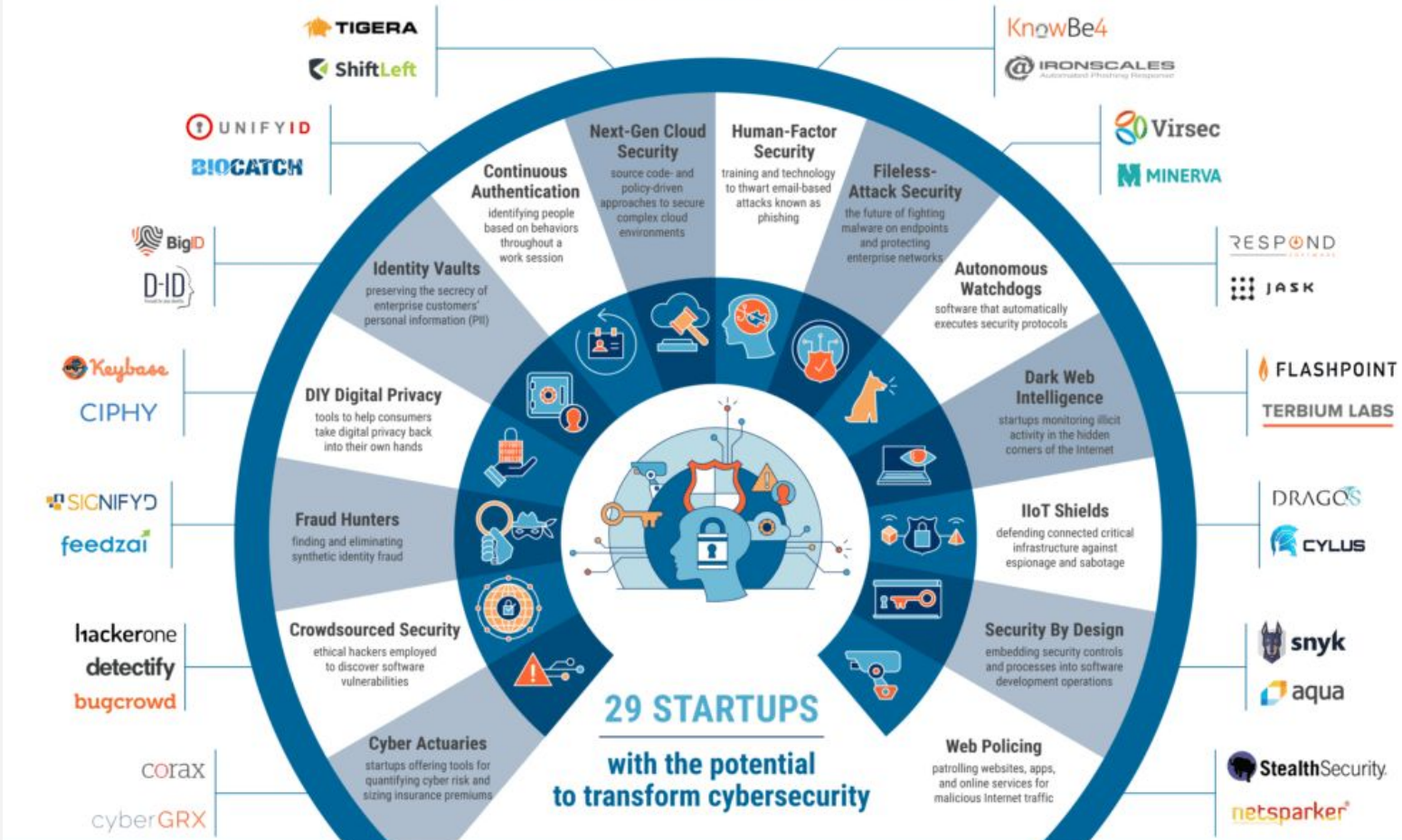

SIEM
IDS/IPS
ENTERPRISE FIREWALLS
ENDPOINT PROTECTION PLATFORMS
SECURE EMAIL GATEWAYS
NAC
THREAT INTELLIGENCE PLATFORMS
SECURE WEB GATEWAYS

Red Hat


Network & Infrastructure Security
Advanced Threat Protection
NAC
SDN
DDoS Protection
DNS Security
Network Firewall
Deception
ICS + OT
Network Analysis & Forensics
Web Security
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Application Security Testing
MSSP
Traditional MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Other
Mobile Security
Risk & Compliance
Risk Assessment & Visibility
Security Ratings
Pen Testing & Breach Simulation
GRC
Security Awareness & Training
Security Operations & Incident Response
SIEM
Security Incident Response
Security Analytics
Momentum CYBER
Threat Intelligence
IoT
IoT Devices
Automotive
Connected Home
Messaging Security
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Digital Risk Management
Security Consulting
Blockchain
Fraud & Transaction Security
Cloud Security
Container
Infrastructure
CASB

CBINSIGHTS

2018 CYBER DEFENDERS



Red Hat

VC | Corporate / Corp VC | Private Equity | Angel | Other | 2 years | 5 years

$3.58bn
Funding in last year

+71.99%
YoY Funding Growth

179
Deals in last year

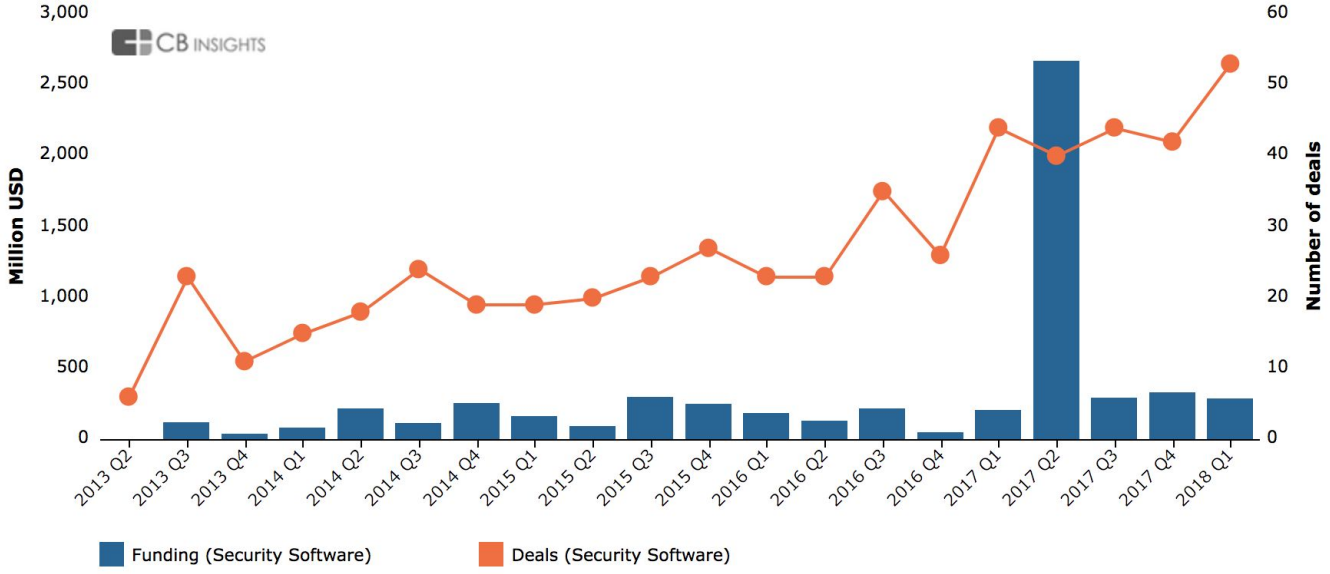
+26.62%
YoY Deal Growth

27
Avg Deals per Quarter

$298.9M
Avg Funding per Quarter

Q2'17
Biggest Quarter ($ Funding)

Q1'18
Biggest Quarter (# of deals)



Red Hat

Les dépenses mondiales en matériel, logiciels et services de sécurité dépasseront **103 milliards** de dollars en 2019, soit 9,4 % de plus qu'en 2018.

IDC

Source:
https://www.zdnet.com/article/global-security-spending-to-top-103-billion-in-2019-says-idc/

Les équipes de sécurité sont débordées. **L'équipe de sécurité moyenne examine généralement moins de 5 % des alertes qui lui parviennent chaque jour** (et dans de nombreux cas, beaucoup moins que cela).

Venturebeat

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

57 % des répondants ont dit que le

le délai de résolution d'un incident a augmenté

65 % ont déclaré que le

la gravité des attaques a augmenté

Ponemon Institute

Source:
The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute (Sponsored by IBM)

Red Hat

L'insuffisance de personnel qualifié dédié à la cybersécurité constituait le deuxième obstacle à la cyberrésistance, **29%** seulement ayant le niveau idéal de personnel.

Ponemon Institute

Source:
The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute (Sponsored by IBM)

63 % des répondants affirment que leurs dirigeants comprennent que **l'automatisation, le machine learning, l'intelligence artificielle et l'orchestration** renforcent la cyberrésilience.

Ponemon Institute

Source:
The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute (Sponsored by IBM)

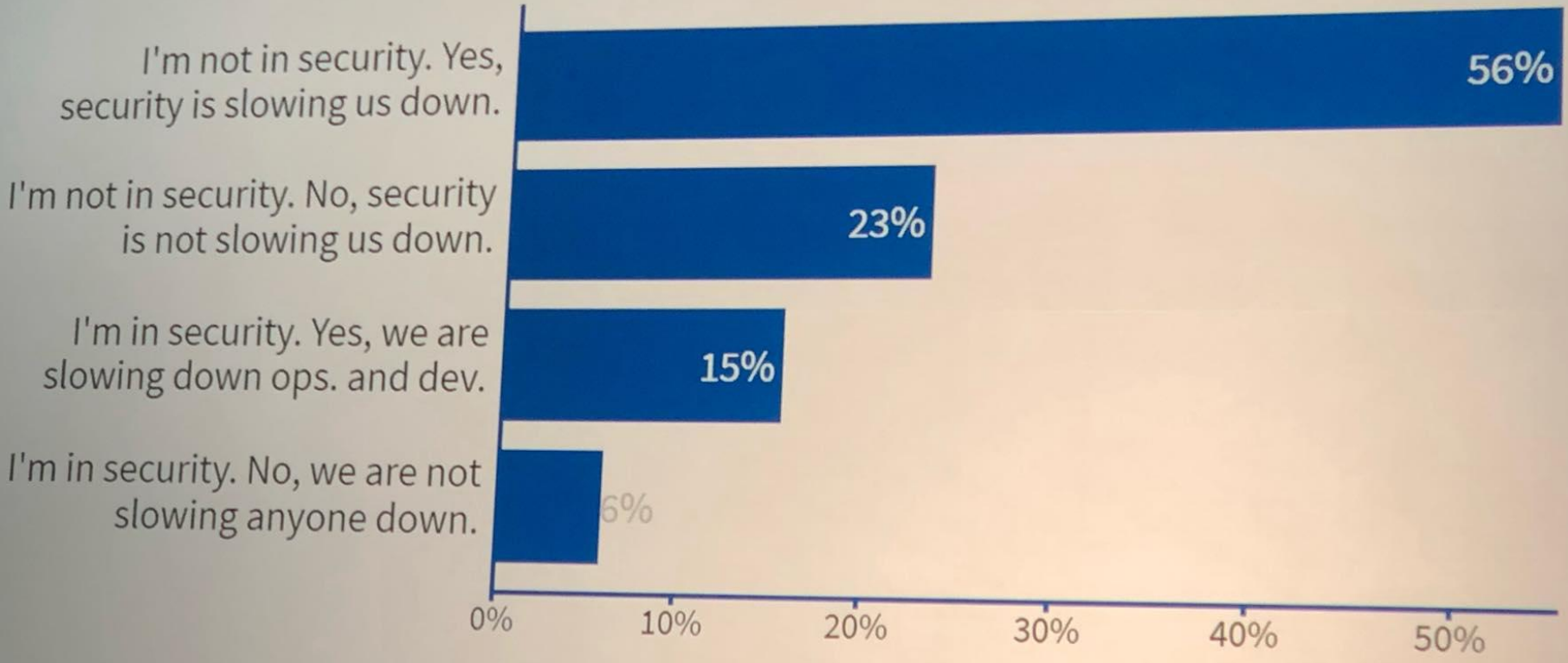
Red Hat

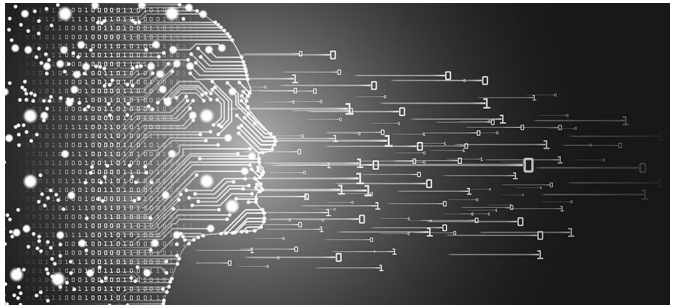
Il s'agit simplement de l'inefficacité inhérente du monde de la sécurité informatique.

2 nouveaux aspects émergents....

Visit gartner.com/gpolls3

Do you believe information security is slowing down agile operations and agile development?





L'utilisation de l'IA pour automatiser les tâches liées à l'exécution des cyberattaques permettra d'atténuer les compromis existants entre l'ampleur et l'efficacité des attaques. Cela peut accroître la menace associée aux cyberattaques qui demande normalement plus de main d'oeuvre (comme le spear phishing). Nous nous attendons également à de nouvelles attaques qui exploitent les vulnérabilités humaines (par exemple par l'utilisation de la synthèse vocale pour usurper l'identité), les vulnérabilités logicielles existantes (par exemple par piratage automatisé) ou les vulnérabilités des systèmes d'IA (à travers des exemples contratictoires et par l'empoisonnement des données).

Future of Humanity Institute | University of Oxford | Centre for the Study of Existential Risk | University of Cambridge | Center for a New American Security | Electronic Frontier Foundation | OpenAI

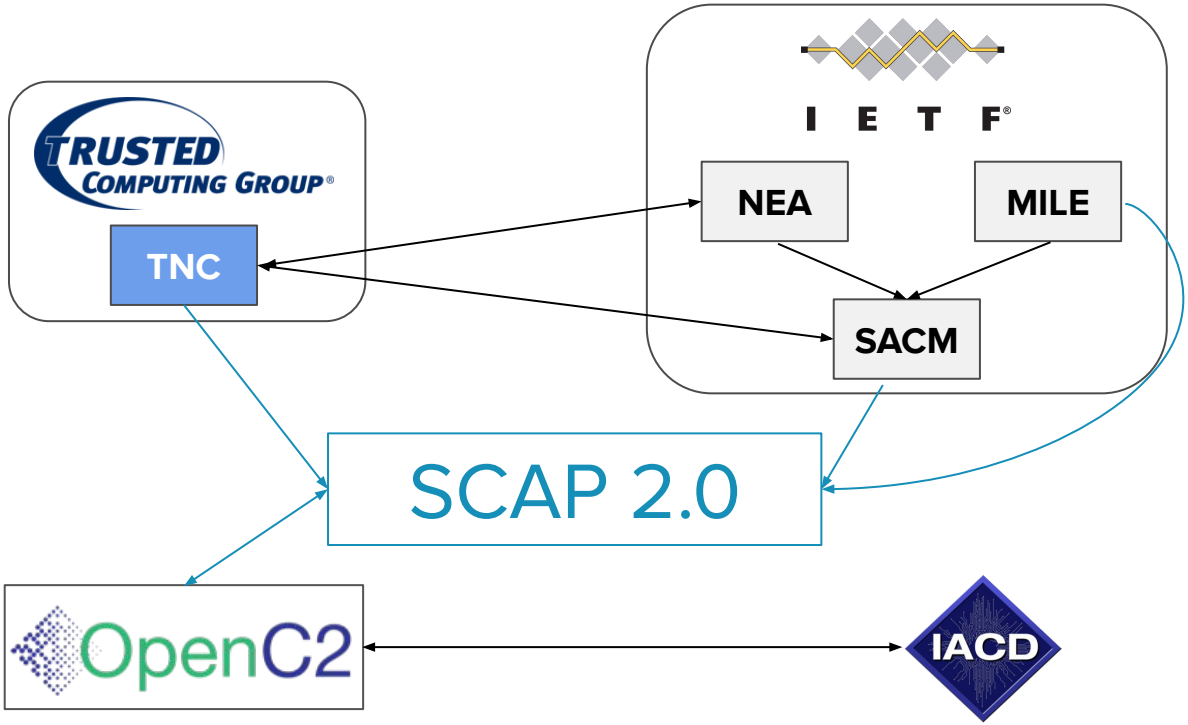
Source:
The Malicious Use of Artificial Intelligence - Future of Humanity Institute | University of Oxford | Centre for the Study of Existential Risk | University of Cambridge | Center for a New American Security | Electronic Frontier Foundation | OpenAI

https://www.blackhat.com/us-18/briefings/schedule/#deeplocker---concealing-targeted-attacks-with-ai-locksmithing-11549

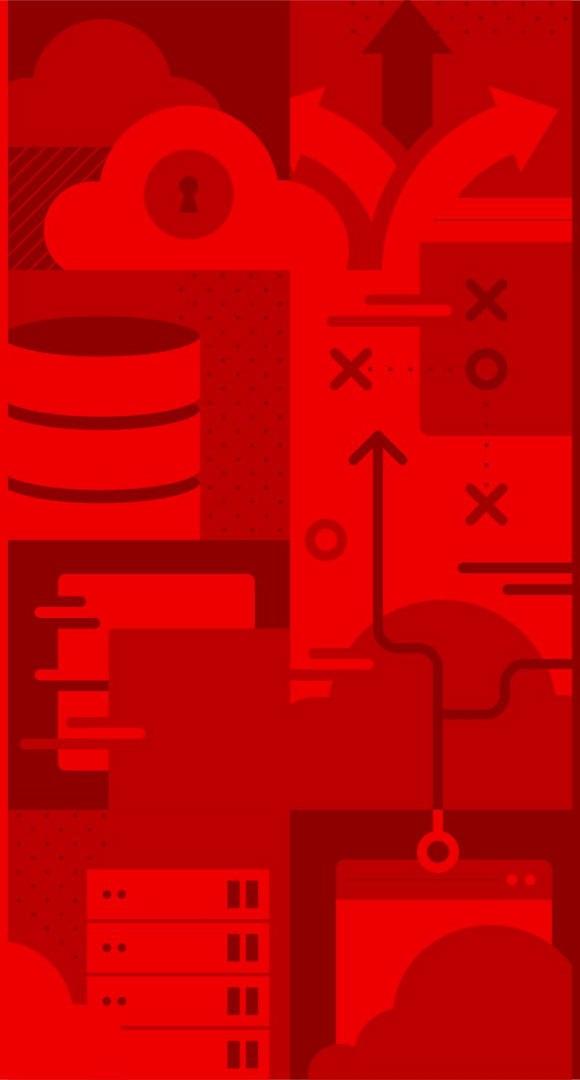
Il n’y a pas d’intégration

- Les normes proposées pour les intégrations (CYBOX, OPENIOC, YARA, STIX / TAXII) ne sont pas largement adoptées
- Les tâches automatisées impliquent rarement plus de deux systèmes
- Les promoteurs principaux des intégrations sont les fournisseurs de contenu de sécurité
- On ne fait pas confiance à la correction automatisée

Recherche actuelle et normes pour l'automatisation de la sécurité




L'automatisation peut devenir
La lingua franca
De la sécurité informatique



Security Orchestration And Automated Response (SOAR) est né

Red Hat

IBM Resilient

Red Hat

Hosted by:

Anton Chuvakin
VP Distinguished Analyst

Discussion Topics:

- What is SOAR
- Who should use SOAR
- How organizations are using SOAR
- The best practices in deployment and use of SOAR tools

Click "Attend" to add this webinar to your calendar.

VIEW ALL WEBINARS

Polling Question 1

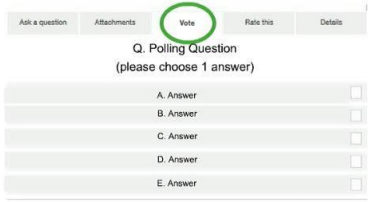
Question: given what you know now, do you see your organization deploying a SOAR tool in the next 12 months?

A. **Yes, a commercial tool**
B. **Yes, an open source tool**
C. **No, see no need or not ready**
D. **No for other reasons**
E. **Not sure**

How to participate in our polling

If you are in full screen mode – click Esc
The poll question is on the "Vote" tab.
Please click the box to make your selection.
Upon voting you will see the results.

Thank you!



Gartner

The first poll is open! Please provide you answer. Upon voting you will see the results.

Close

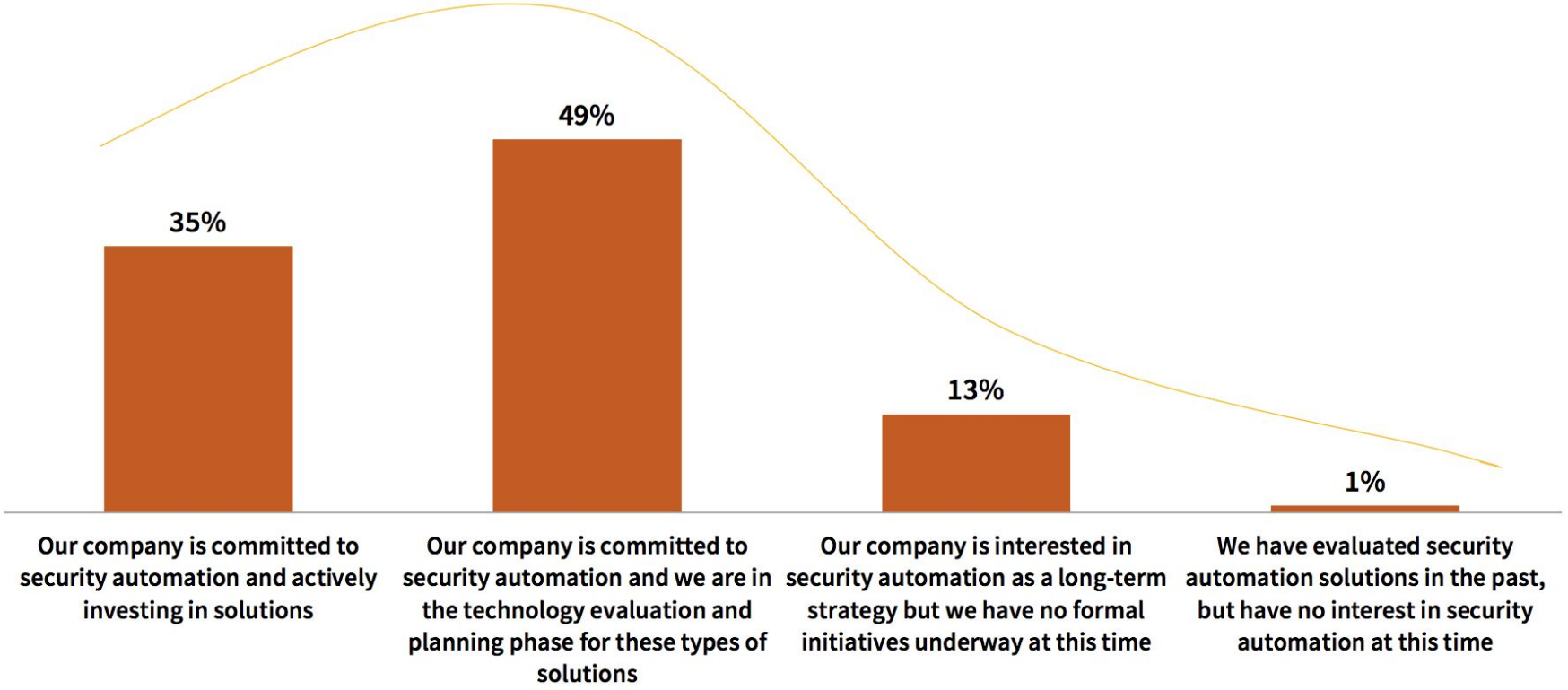
Ask a question | Attachments | **Vote** | Rate this | Details

Q (1 of 1) Given what you know now, do you see your organization deploying a SOAR tool in the next 12 months?

Yes, a commercial tool	32%
Yes, an open source tool	22%
No, see no need or not ready	20%
No for other reasons	1%
Not sure	24%

Prepare Your Security Operations for Orchestration and Automation Tools - Gartner - April 2018

Red Hat



Oracle and KPMG Cloud Threat Report, 2018 - Oracle

Red Hat

Les premiers outils SOAR supposaient que les utilisateurs **étaient à la fois un expert en sécurité et un développeur Python expérimenté**, mais heureusement, cette époque est révolue. Cependant, même aujourd'hui, Python est utilisé pour personnaliser l'automatisation de plusieurs des outils SOAR populaires, tels que Phantom, Demisto et Swimlane... Les fournisseurs insistent sur le fait qu'intégrer un outil SOAR à un outil SIEM ou EDR est un pointer-cliquer. Cela peut être valide, dans certains cas spécifiques, mais les clients signalent que dans la plupart des cas, **ces solutions ne fonctionnent tout simplement pas comme prévu** et qu'il est nécessaire de faire appel à un expert pour affiner et corriger le tout.

Anton Chuvakin
VP Distinguished Analyst

Augusto Barros
Research Director

Source:
Preparivng Your Security Operations for Orchestration and Automation Tools - Gartner

Ansible Security Automation

Red Hat

Pourquoi Ansible ?

Simple

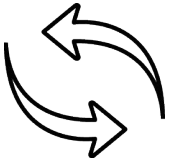
Automatisation facile

Pas besoin d'être programmeur

Les tâches sont exécutées en ordre

Utilisable par tous

Devenez productif rapidement



Puissant

Déploiement d'application

Gestion de configuration

Orchestration de workflow

Automatisation des réseaux

Orchestrez le cycle de vie complet

Sans Agent

Aucun agent à installé

Utilise OpenSSH & WinRM

Pas d'agent à exploiter ou maintenir

Démarrer immédiatement

Plus efficace, plus sécure

Red Hat

Que puis-je faire avec Ansible?

Automatisez le déploiement et la gestion de l'ensemble de votre parc informatique.

Faire ça ...

Orchestration	Gestion de configuration	Déploiement d'applications	Provisioning	Livraison en continue	Sécurité et conformité

Sur ...

Pare-feux	Balanceurs de Charge	Applications	Containeurs	Nuage informatique
Serveurs	Infrastructure	Stockage	Composantes réseau	**Et plus ...**

Red Hat

AUTOMATISATION LINUX

150+

Linux Modules

AUTOMATISER TOUT LINUX

Red Hat Enterprise Linux, BSD, Debian, Ubuntu et beaucoup plus!

Le seul pré-requis :
Python 2 (2.6 +)
ou Python 3 (3.5 +)

ansible.com/get-started

Red Hat

AUTOMATISATON DES RÉSEAUX

65+
Plateformes réseau

1000+
Modules réseau

15*
Galaxy Network Roles

ansible.com/for/networks
galaxy.ansible.com/ansible-network

* *Rôles développés et maintenus par les ingénieurs Ansible Network*

Red Hat

AUTOMATISATON WINDOWS

100+
Modules
Windows

1,300+
Ressources
Powershell DSC

ansible.com/windows

Red Hat

AUTOMATISATION NUAGE INFORMATIQUE

800+
Modules
Cloud

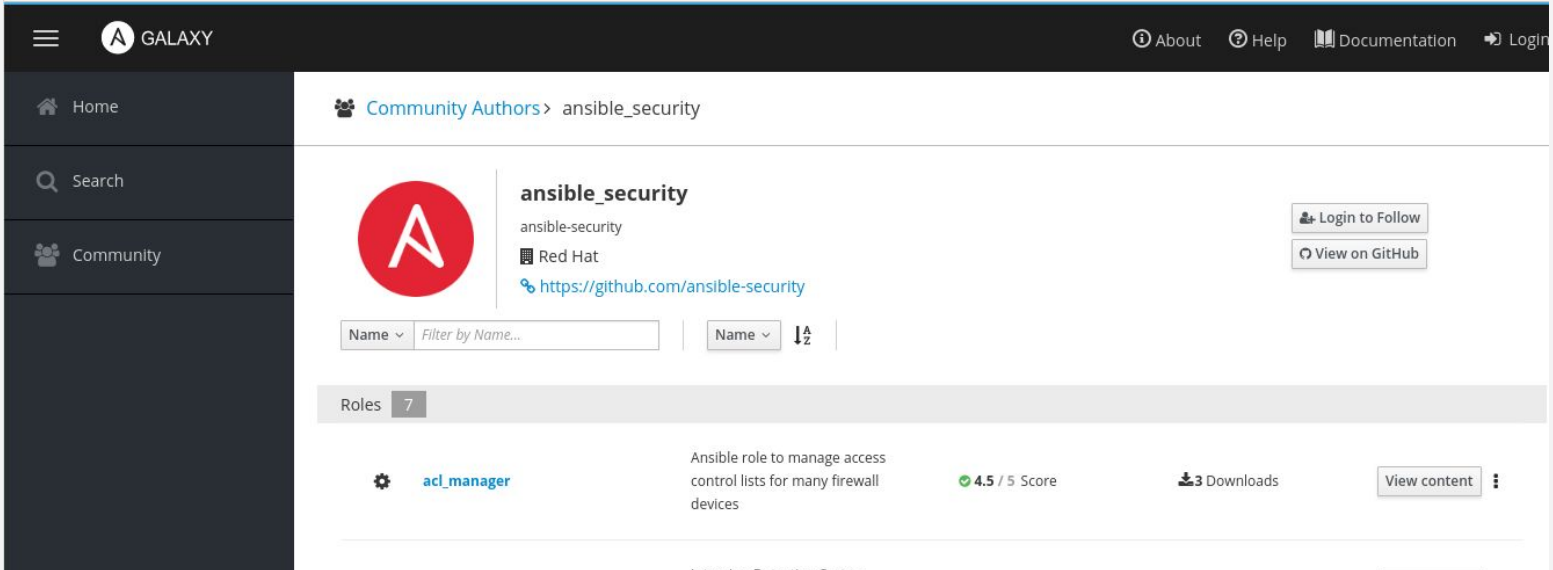
30+
Plateformes
Cloud

ansible.com/cloud

Red Hat

What is it?

Ansible Security Automation est un ensemble supporté de modules, de rôles et de playbook Ansible conçus pour unifier la réponse de sécurité aux cyberattaques d'une nouvelle manière - en orchestrant l'activité de plusieurs solutions de sécurité qui ne s'intégreraient pas normalement via un langage commun et ouvert - Ansible.



Red Hat

QUELS TYPES DE DISPOSITIFS?
QUI SONT NOS PARTENAIRES?

Security Information & Events Management (SIEM)

splunk>

IBM

Enterprise Firewalls

Check Point SOFTWARE TECHNOLOGIES LTD

CISCO

f5

FORTINET

Intrusion Detection & Prevention Systems

SNORT

Check Point SOFTWARE TECHNOLOGIES LTD

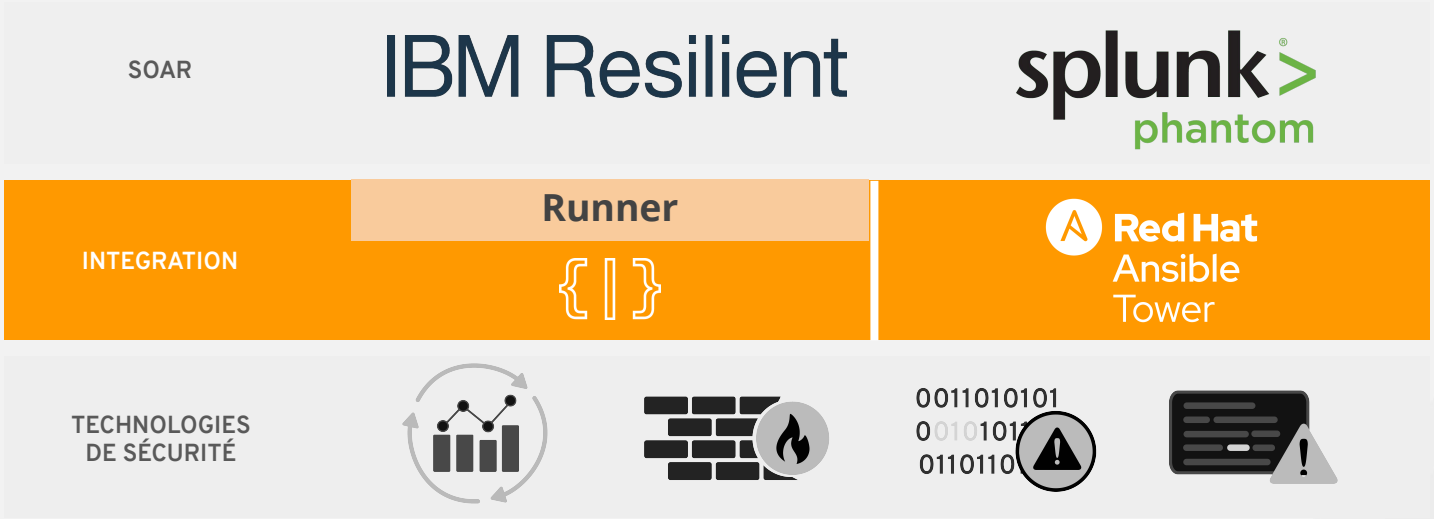
FORTINET

Privileged Access Management

CYBERARK

Syncope

INTEGRATION ANSIBLE AVEC SOAR

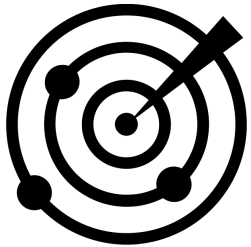


Qu'est-ce qu'il fait ?

Avec Ansible Security Automation, les organisations informatiques peuvent traiter plusieurs cas d'utilisation courants.

Tri des activités suspectes

Activation de l'accès aux configurations de journaux telles que destination, verbosité, etc.



Chasse à la menace

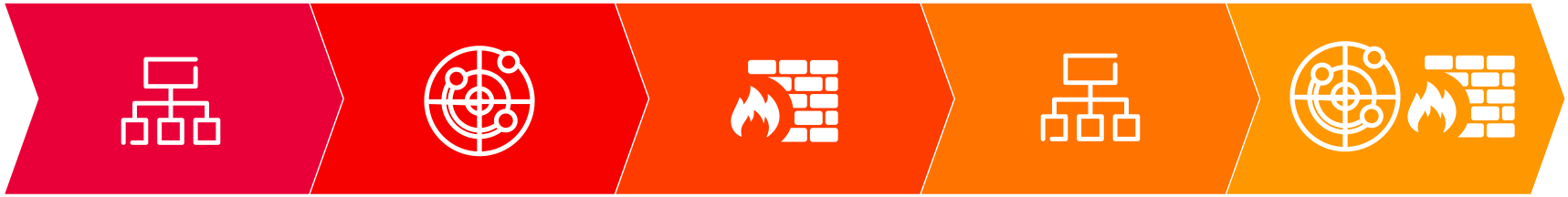
Automatisation des alertes, recherches de corrélation et manipulation des signatures

Réponse à un incident

Création de nouvelles stratégies de sécurité pour mettre en “whitelist”, “blacklist” ou mettre en quarantaine

Évaluation des risques : Comportement d'une application

L'évaluation des comportements anormaux comporte plusieurs étapes, comme la validation d'une adresse IP contre de multiples sources, la recherche de signes d'infiltration dans l'environnement, etc. et ensuite traiter et présenter l'information à l'analyste de la sécurité.



splunk>

Détecte une anomalie dans le comportement d'une application. Demande à Snort & Check Point pour plus d'informations.

SNORT®

Implémente une nouvelle règle pour collecter plus d'informations dans le périmètre affecté.

Check Point SOFTWARE TECHNOLOGIES LTD.

Augmente le niveau de journalisation sur le périmètre réseau..

splunk>

Regroupe l'information pour le triage.

SNORT® Check Point SOFTWARE TECHNOLOGIES LTD.

Restaurer les configurations d'origine.

Red Hat

Chasse aux menaces : Violation des règles du pare-feu

Une personne chargée d'enquêter sur une menace ou d'intervenir en cas d'incident pourrait enquêter sur un incident et se retrouver avec des centaines d'ips, de hachages de fichiers et de domaines.

CISCO

Enregistre une violation continue des règles. Envoie des alertes à IBM QRadar.

IBM

Crée une infraction, demande des informations supplémentaires à Fortinet IPS.

FORTINET

Crée une nouvelle règle pour rechercher l'origine de la violation.

IBM

Confirme que la violation de la règle est causée par une adresse IP mal configurée.

CISCO

Mettre l'adresse ip sur une "whitelist"

Intervention en cas d'incident : attaque par injection SQL

La mitigation de ce type d'attaque nécessite jusqu'à 10 étapes manuelles entre l'identification et la correction.

Check Point IPS détecte une attaque par injection SQL et alerte IBM QRadar.

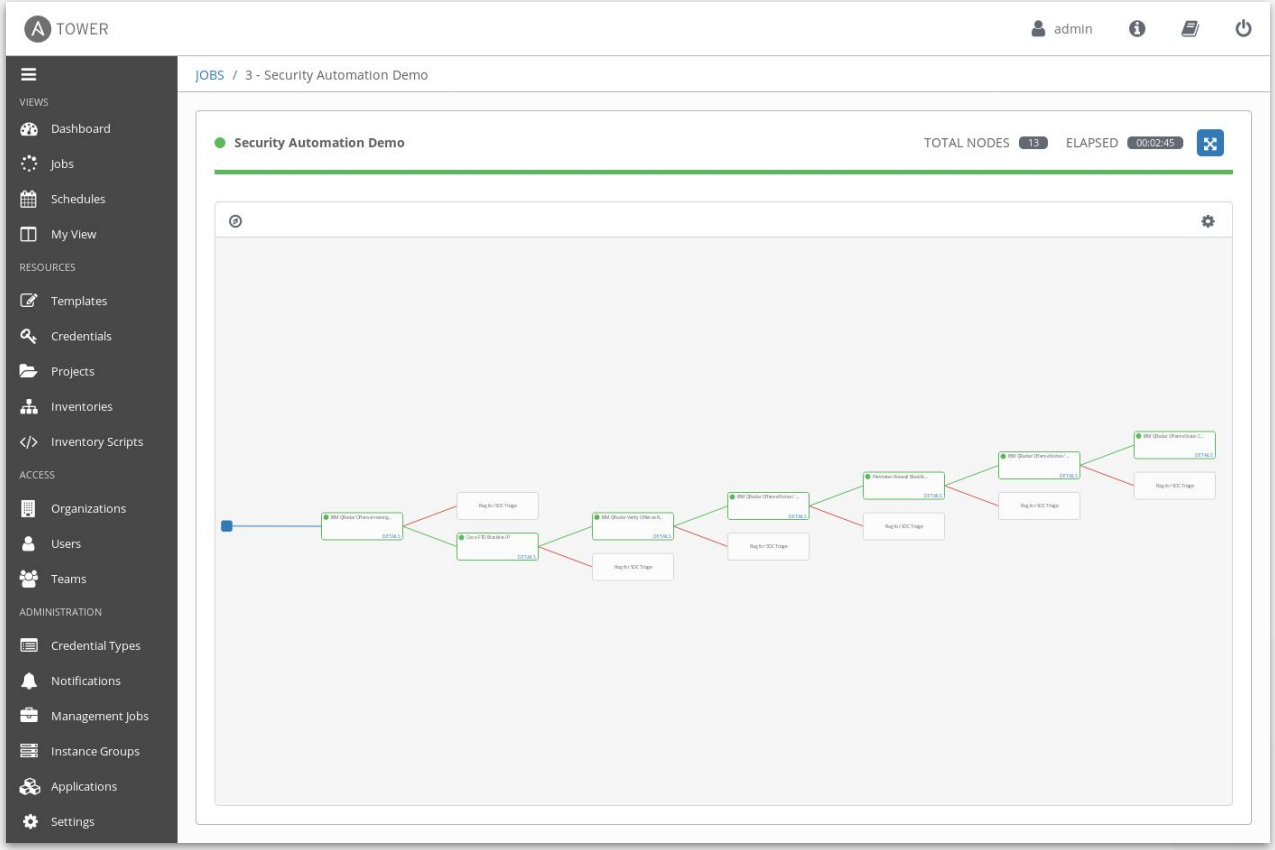
Valide la menace, crée une correction.

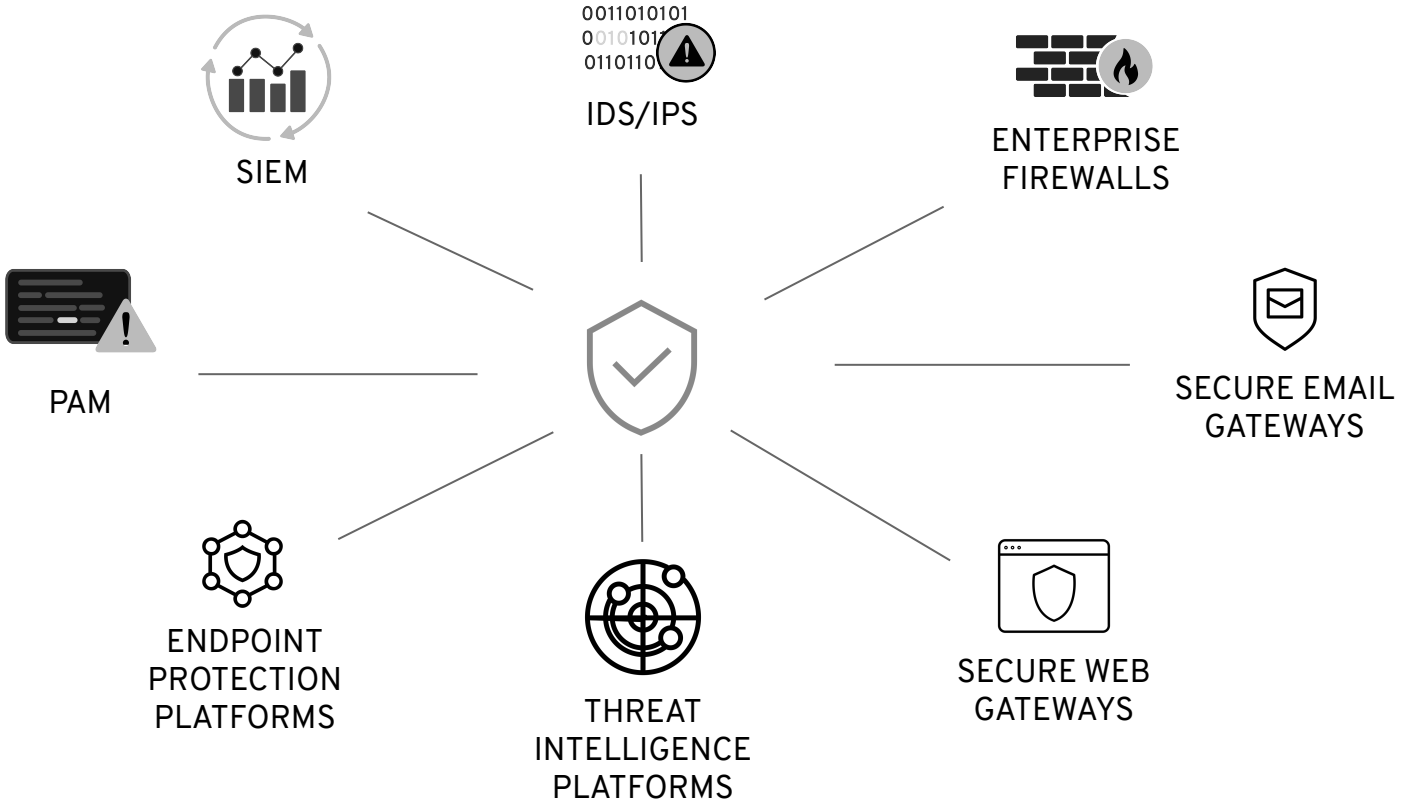
Fortinet NGFW crée une nouvelle règle pour mettre en "blacklist" la source IP de l'attaque.

Confirme la fin de l'attaque et met à jour IBM QRadar.

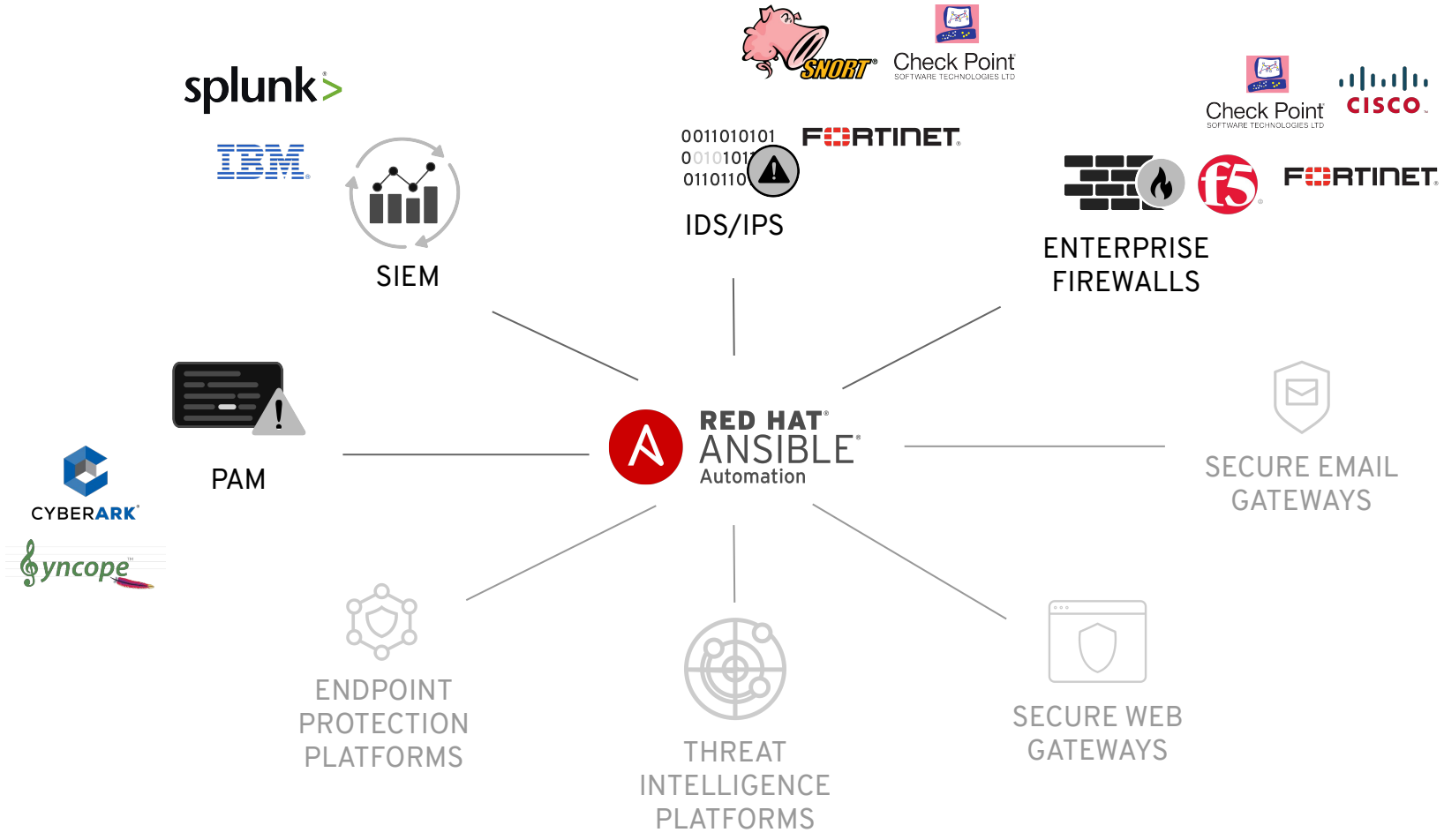
Double vérification de la fin de l'attaque et clôture l'incident.

FLUX DE TRAVAIL ANSIBLE TOWER

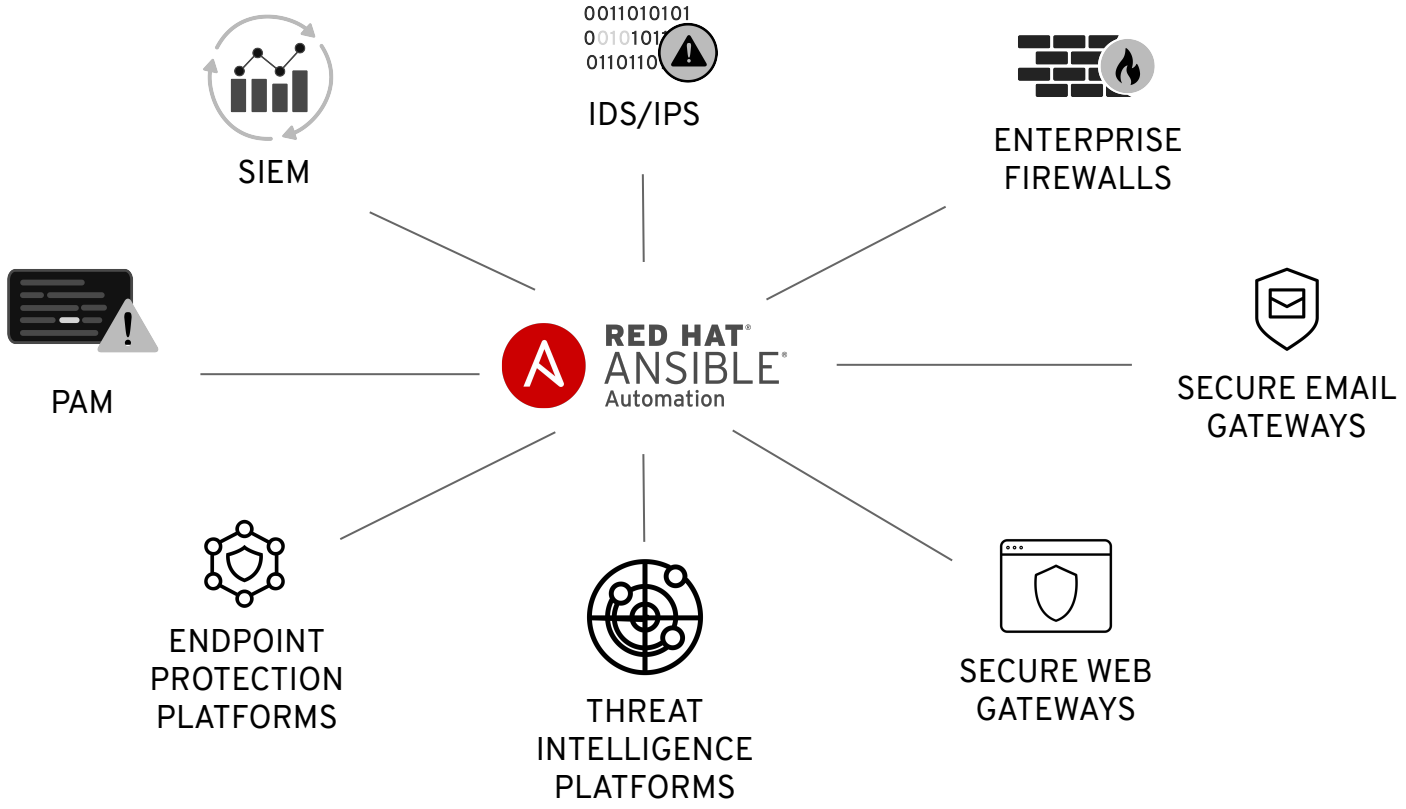



SIEM
0011010101
0010101
0110110
IDS/IPS
ENTERPRISE FIREWALLS
PAM
SECURE EMAIL GATEWAYS
ENDPOINT PROTECTION PLATFORMS
THREAT INTELLIGENCE PLATFORMS
SECURE WEB GATEWAYS

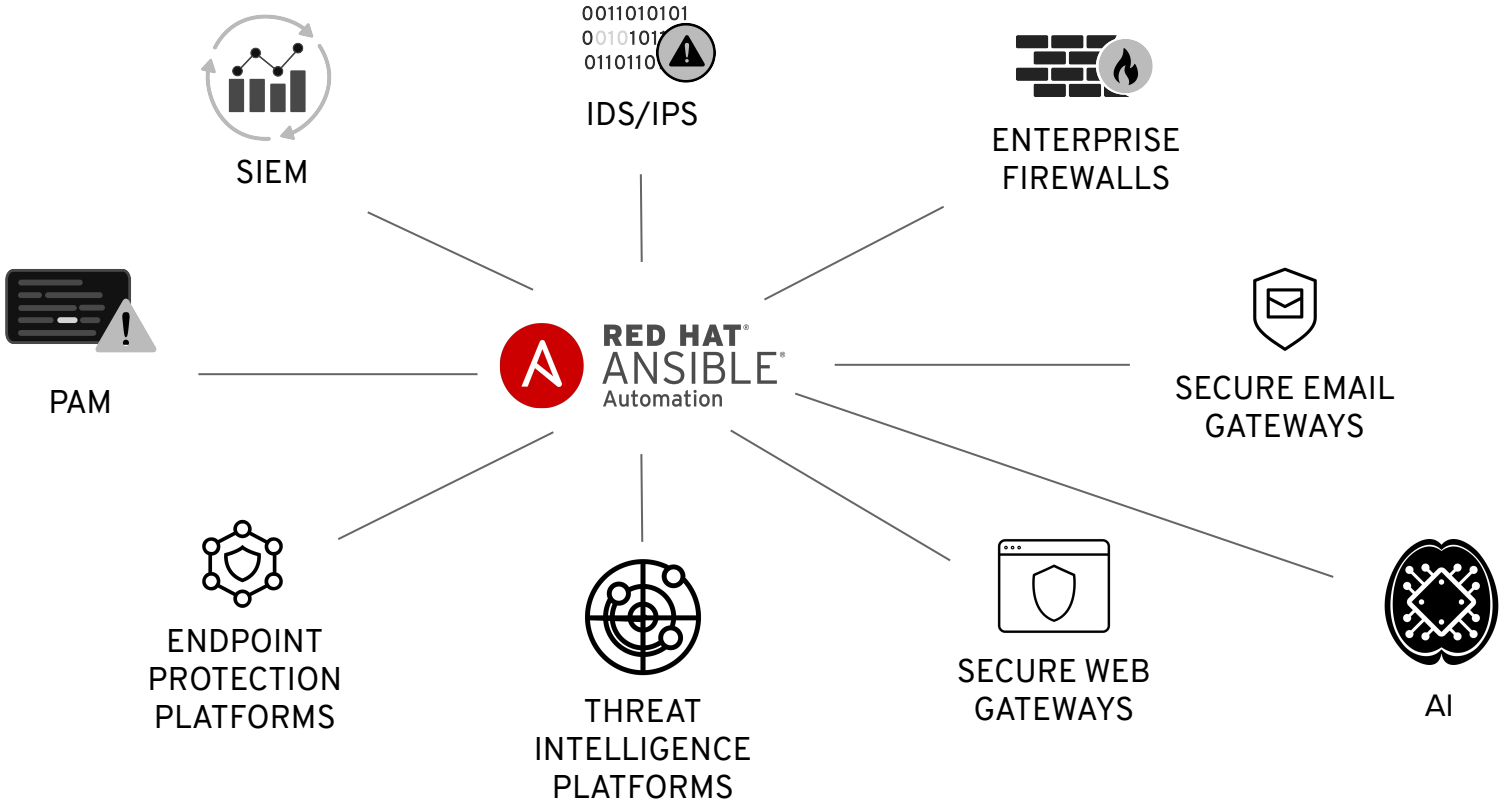
Red Hat


splunk>
IBM
SIEM
SNORT
Check Point
SOFTWARE TECHNOLOGIES LTD
0011010101
0010101
0110110
FORTINET
IDS/IPS
Check Point
SOFTWARE TECHNOLOGIES LTD
CISCO
f5
FORTINET
ENTERPRISE
FIREWALLS
PAM
CYBERARK
syncope
RED HAT
ANSIBLE
Automation
SECURE EMAIL
GATEWAYS
ENDPOINT
PROTECTION
PLATFORMS
THREAT
INTELLIGENCE
PLATFORMS
SECURE WEB
GATEWAYS

Red Hat


SIEM
0011010101
0010101
0110110
IDS/IPS
ENTERPRISE FIREWALLS
PAM
RED HAT
ANSIBLE
Automation
SECURE EMAIL GATEWAYS
ENDPOINT PROTECTION PLATFORMS
THREAT INTELLIGENCE PLATFORMS
SECURE WEB GATEWAYS

Red Hat


SIEM
0011010101
0010101
0110110
IDS/IPS
ENTERPRISE FIREWALLS
PAM
RED HAT
ANSIBLE
Automation
SECURE EMAIL GATEWAYS
ENDPOINT PROTECTION PLATFORMS
THREAT INTELLIGENCE PLATFORMS
SECURE WEB GATEWAYS
AI

Red Hat

DÉMONSTRATION

CHASSE AUX MENACES

Comment pouvez-vous y arriver?

- **Reconsidérer l'automatisation comme une défense stratégique et non comme un outil tactique de plus.**
- Découvrez quels sont les outils d'automatisation les plus utilisés dans votre organisation, et pourquoi.
- Évaluer la capacité des outils choisis à atténuer les risques liés à l'automatisation
- Inclure un logiciel d'automatisation comme cible pour vos pen-testing
- Expérimenter la sécurité automatisée pour les applications non critiques
- Informez votre fournisseur d'automatisation des outils de sécurité que vous utilisez et de la façon dont vous aimeriez qu'ils interagissent les uns avec les autres.
- Faire pression sur les fournisseurs de sécurité pour qu'ils commencent à s'intégrer aux outils d'automatisation

PROCHAINES ÉTAPES

DÉMARRER

ansible.com/get-started

ansible.com/tower-trial

ANSIBLE SECURITY AUTOMATION

https://galaxy.ansible.com/ansible_security

https://github.com/ansible-security/

https://www.ansible.com/use-cases/security-automation

JOINDRE LA COMMUNAUTÉ

ansible.com/community

PARTAGER VOTRE HISTOIRE

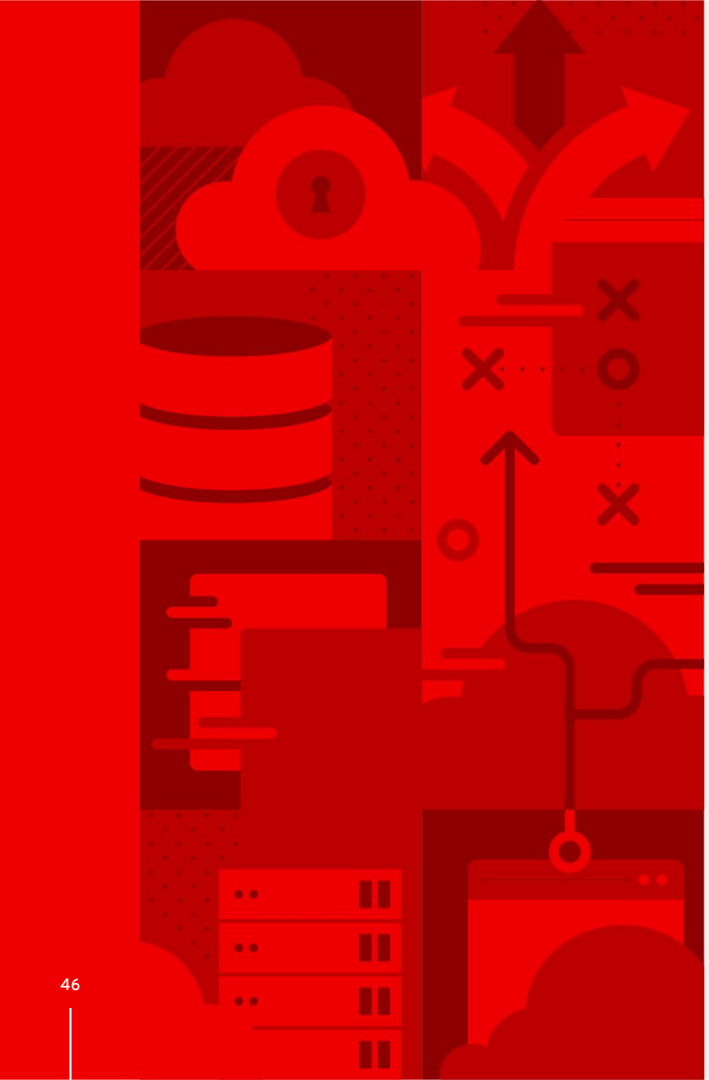
Nous suivre Twitter @Ansible

Nous suivre sur Facebook

WORKSHOPS & FORMATIONS

Red Hat Training

Red Hat



MERCI !

Red Hat est le premier fournisseur mondial de solutions logicielles open source pour entreprises. Des services de support, de formation et de conseil primés font de Red Hat un conseiller de confiance.

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat