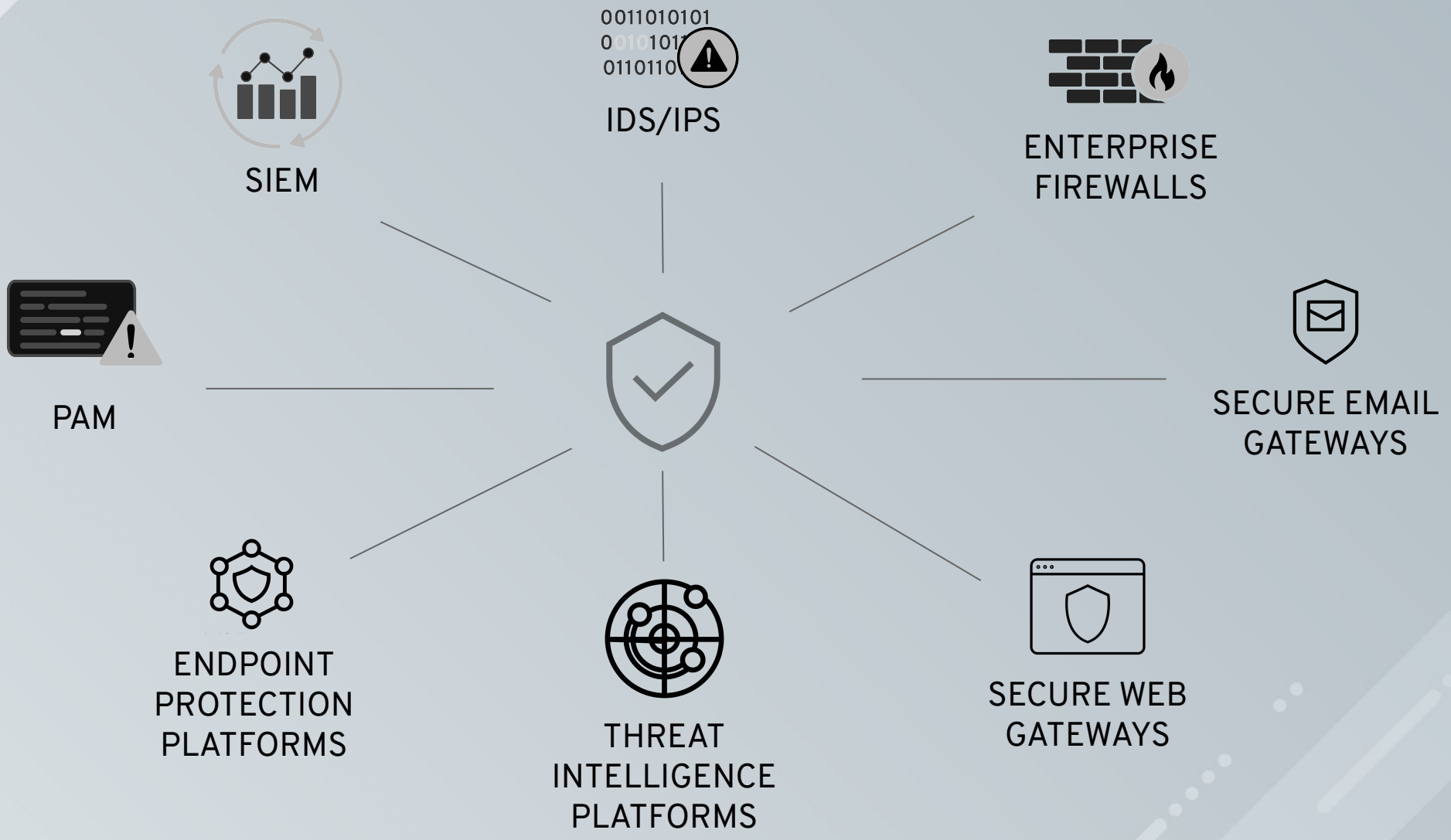
Red Hat | ANSIBLE

#ANSIBLEAUTOMATES MOSCOW 2019

ANSIBLE SECURITY AUTOMATION

Victor da Costa
Principal Technical Business Development, CCIE #39373
Twitter/@victorobotz, Github/@victorock


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

Network & Infrastructure Security

Advanced Threat Protection
Barracuda, BluVector, Check Point, Cisco, FireEye, Fortinet, Huawei, Hysolate, JoeSecurity, Juniper, lastline, McAfee, Metapacket, OPSWAT, paloalto, Reversing Labs, solebit, SonicWall, Sophos, Spamina, Symantec, Vintay, Votiro, WatchGuard

NAC
armis, aruba, Auconet, Axonius, Bradford Networks, Cisco, Extreme, ForeScout, Genians, Netshield, portnox, Trustwave

SDN
BlackRidge Technology, Certes Networks, Cybera, Cyxtera, NanoSec, Skyport Systems, Tempered, Versa Networks, Vidder, zentera, zscaler

DDoS Protection
Akamai, Check Point, Cloudflare, f5, Fortinet, Imperva, neustar, Nexusguard, NSFocus, Oracle, StackPath, Verisign

DNS Security
BlueCat, Cisco, Cyren, efficient IP, Infoblox, neustar, Quad9, Webroot, Verisign

Network Firewall
algosec, CATO, Check Point, Cisco, Clavister, endian, Forcepoint, Fortinet, Hillstone, Huawei, OPAQ, paloalto, Sangfor, secucloud, SonicWall, Sophos, untangle

Deception
Acalvio, Attivo Networks, Counter Craft, CyberTrap, Cymmetria, GuardiCore, illusive, Viper, Smokescreen, TRAPX Security

ICS + OT
Aperio, Bayshore, Belden, Claroty, Cribercence, CyberX, Cyberbit, Dragos, endian, Firmitas, Halo Analytics, Indegy, dimension, NexDefense, Nozomi Networks, PAS, Nextnine, PFP, radiflow, Rhebo, SCADAfence, Security Matters, sentryo

Network Analysis & Forensics
Cisco, CGS, CloudShark, Core Security, Corvil, Dark Trace, Fidelis, Gigamon, Icebrg, IronNet, Lumeta, NetScout, Packetsled, paloalto, Protectwise, SS8, utimaco, Vectra

Web Security
Akamai, apriver, aurionpro, authentic8, Barracuda, Check Point, Cisco, ContentKeeper, Cyren, distil networks, EdgeWave, Ericom, f5, Forcepoint, Fortinet, GWAVA, iboss, Light Point Security, McAfee, Menlo Security, NAMOGOO, perimeterx, proofpoint, randed, Reblaze, SHIELD, SHAPE, smoothwall, Sophos, Spamina, Stealth, Symantec, Trend Micro, Trustwave, unbotify, whitecope, zscaler

Endpoint Security

Endpoint Prevention
AhnLab, avast, Avecto, Avira, Barkly, Bitdefender, Blueridge, Bromium, Bufferzone, Carbon Black, Check Point, Comodo, cyberreason, Cylance, deepinstinct, Endgame, Ensilo, Ericom, eset, F-Secure, Faronics, Fortinet, Hysolate, intego, ivanti, Kaspersky, McAfee, Menlo Security, Microsoft, Morphisec, Nyotron, OPSWAT, paloalto, panda, Perception Point, SentinelOne, Sophos, sparkcognition, Stormshield, Symantec, Tehtris, Trend Micro, vmware, Webroot, Zero Advance

Endpoint Detection & Response
Belden, Binary Defense, Bitdefender, Carbon Black, Cisco, Comodo, CounterTack, Cybereason, Cyberbit, Cyberx, Cylance, Cynet, Digital Guardian, Dtex, Endgame, Ensilo, Fenror, Fidelis, FireEye, Forcepoint, Huntress, Kaspersky, Minerva Labs, Nehemiah, nexthink, Nyotron, opentext, paloalto, panda, promisec, RSA, Secdo, secpod, Sentinel One, Sophos, Symantec, Tanium, Tehtris, WatchGuard, ziften

Application Security

WAF & Application Security
6scan, A10, Akamai, Alert Logic, Arxan, Barracuda, ca technologies, citrix, Cloudflare, Contrast Security, CyKick Labs, DB Appsecurity, denyall, ergon, f5, Fortinet, Imperva, netsparker, Oracle, Penta Security, Positive Technologies, Prevoty, Puresec, Qualys, radware, Reblaze, riverbed, sucuri, Seworks, SHAPE, StackPath, Signal Sciences, TCELL, Threatx, Trend Micro, Trustwave, Vicarius, wallarm, waratek, WhiteHat Security

Application Security Testing
acunetix, bugcrowd, BugFinders, ca technologies, Checkmarx, ERPScan, Fasoo, hackerone, IBM, Micro Focus, N-Stalker, onapsis, Parasoft, Portswigger, Qualys, Rapid7, RogueWave, SiteLock, snyk, sonarsource, SourceClear, Synack, Synopsys, tenable, Trustwave, Virtualforge, WhiteHat Security, WhiteSource

MSSP

Traditional MSSP
at&t, BAE Systems, BT, CenturyLink, Cleos Systems, CSC, Hewlett Packard Enterprise, IBM, MegaPath, nuspire, OPTIV, Secureworks, Solutionary, Symantec, Trustwave, verizon, wipro

Advanced MSS & MDR
ADT, Alert Logic, Arctic Wolf, Booz | Allen | Hamilton, esentire, FireEye, Netsurion, PALADION, Rapid7, Raytheon, ROOK Security

Data Security

Encryption
baffle, boxcryptor, CipherCloud, Cloudmark, Coverti, CryptoNovo, Cyphre, DataLocker, Enveil, Fortanix, hp, Mentis, BnCrypted Cloud, PKWARE, SecurityFirst, Thales, Trend Micro, Vaultive, virtru, WinMagic

DLP
ca technologies, clearswift, Cososys, Digital Guardian, Fidelis, Forcepoint, GTB Technologies, Infoguard, Ionic, McAfee, Searchinform, Somansa, Symantec, Zecurion

Data Privacy
Actifile, BigID, Covata, D.Day Labs, DID, Integris Software, minerva, nuix, OneTrust, Prifender, SecuPi, Spirion, Titus, nomi, TrustArc, trust hub, wirewhee

Other
BlueTalon, Code42, Datex, dataphy, Networks, druva, globalvelocity, Privitar, Seclore, Spirion, StorageCraft, Thinair, Varonis, VERA

Mobile Security
appdome, appthority, Better, BlackBerry, blue cedar, Check Point, cellrox, Communitake, CyberArk, eMune Mobile Security, Nubico, Inpedio, Kaymera, Kool Span, Lookout, MobileIron, NowSecure, Open Peak, pindrop, pradeo, PSafe, SaltDNA, silent circle, SOTI, Symantec, TeleSign, Teskalabs, tigertext, Trustlook, Vaulto, vmware, wandera, wickr, Zimperium

Risk & Compliance

Risk Assessment & Visibility
Balbix, Bay Dynamics, cavirin, Coalition, Cyber Observer, Cybergrx, CyberHat, cytegic, Delve, eclypsium, Firemon, Four V Systems, nnoSec, kenna, Nehemiah, Outpost24, Prevalent, RedSeal, riskrecon, RiskSense, Skybox Security, tenable, UpGuard

Security Ratings
BitSight, corax, FICO, Guidewire, Norse Shield, Panorays, SecurityScorecard

Pen Testing & Breach Simulation
Attackiq, Cobalt, Cronus, CyberHat, Cycognito, Cymulate, Xmodo Security, Mazebolt, Nopsec, Picus Security, Rapid7, SafeBreach, Sygnia, Verodin

GRC
algosec, Nasdaq, Information Shield, Lockpath, MetricStream, netwrix, Resolver, RSA, R-sam, tufin

Security Awareness & Training
Barracuda, Cofense, CyberVista, Ironscales, KnowBe4, Phishlabs, Popcorn Training, proofpoint, SANS

Security Operations & Incident Response

SIEM
Alien Vault, Blackstratus, Correlog, Cygilant, DNI, EventTracker, exabeam, Fortinet, HanSight, Huntsman, IBM, logentries, logpoint, LogRhythm, Logscape, logz.io, McAfee, Micro Focus, Palantir, RSA, Sawmill, Securonix, Sift Security, solarwinds, splunk, sumologic, TIBCO, Trustwave

Security Incident Response
ayehu, Security, Cyberbit, Cyberspace, Cyber Triage, Security, Dark Light, Demisto, DFLabs, FireEye, Microsoft, panaseer, radar, Rapid7, Raytheon, RedLock, resilient, Secdo, servicenow, Siemplify, splunk, Swimlane, Syncurity, Sygnia, Threatconnect, Uplevel

Security Analytics
Awake, Bay Dynamics, Darktrace, Dtex, E8 Security, exabeam, Fluency, Fortscale, HanSight, Hewlett Packard Enterprise, Imvision Technologies, Interset, IronNet, Jask, Lacework, paloalto, patternex, Reservoir Labs, Securonix, sqrrl, Teramind, Thetaray, TripleCyber, Vectra, Veriato, Versive, ZoneFox

Momentum Cyber

Threat Intelligence
4iQ, Anomali, Blueliv, BlueVoyant, brandprotect, Centripetal Networks, Cisco, Cyberint, digital shadows, Crowdstrike, Domaintools, eclectic iq, Foresight Security, FireEye, Flashpoint, HanSight, Infoblox, Intel 471, Intsights, KELA, Lookingglass, Malware Patrol, Nucleon, Recorded Future, RiskBased Security, Riskiq, SenseCy, servicenow, Sixgill, SpyCloud, Surfwatch, Threatconnect, ThreatMetrix, Threatquotient, TRU*STAR, Verisign, Webroot

IoT

IoT Devices
Apolloshield, Bastille, Centri, Cyberta, Cylus, Convesum, Authority, Icon Labs, Inbuit, Medigate, Mocana, opentext, riscure, Regulus, Rubicon, Securithings, Sepio, Senrio, ZingBox

Automotive
Blue, Carsdome, Continental, Cycuro, Cymotive, Guard Knox, Harman, Karamba Security, NNG, Trillium

Connected Home
Cujo, Fortress Cyber Security, Netonomy, Rubica, SAM

Messaging Security
AGARI, apriver, Area 1, AstraID, BAE Systems, Barracuda, Cisco, clearswift, Cybonet, Cyren, EdgeWave, FireEye, Forcepoint, Fortinet, GreatHorn, GWAVA, Ironscales, mailguard, McAfee, Microsoft, mimecast, Phishlabs, proofpoint, solebit, SonicWall, Sophos, Spamina, Symantec, Trend Micro, Trustwave, VadeSecure, ValiMail, Votiro, Webroot, wickr

Digital Risk Management
QED, brandprotect, crisp, digital shadows, DigitalStakeout, Lookingglass, NAMOGOO, QADIUM, Riskiq, Social SafeGuard, source, ZeroFox

Security Consulting
accenture, appsec, Booz | Allen | Hamilton, BT, Corvid, Deloitte, Denim Group, EY, FireEye, IBM, Kenda, leidos, Leidos, nccgroup, NEC, Nisos, Optiv, pwc, Stroz Friedberg, Sygnia, wipro

Blockchain
Block Armour, Chain, Craxel, edge, Gladius, guardtime, Manifold Technology, NuID, remme, ShoCard, xage

Identity & Access Management

Authentication
Auth0, averon, BehavioSec, BIOCATCH, ca technologies, Callsign, Centrify, CLEF, Core Security, DUO, Exostar, Google, imprivata, Intrinsic ID, iovation, Nok Nok Labs, planID, SAASPASS, SaferPass, Secret Double Octopus, Secure Key, Secured Touch, Securepush, ShoCard, Silverfort, tascent, ThreatMetrix, Transmit Security, Trusona, Unbound, Uniken, V-Key, Virgil Security, Wheel

IDaaS
Centrify, IBM, Ilantus, welcome, Microsoft, okta, onelogin, Oracle, Ping, RSA, Thales

Privileged Management
Avecto, BeyondTrust, BOMGAR, ca technologies, Centrify, CyberArk, Hitachi, IBM, ManageEngine, Micro Focus, One Identity, Remediant, thycotic, Wheel

Identity Governance
Axiomatics, Core Security, DeepIdentity, opentext, SailPoint, Saviynt, simeio

Consumer Identity
Auth0, Ping, Forgerock, Pirean, IDExperts, ID.me, janrain, loginradius, Microsoft, SAP, Secure Key, Trulioo, verato

Fraud & Transaction Security
AU10TIX, BIOCATCH, Block Fraud, Brighterion, Cardinal Commerce, Datavisor, Early Warning, emailage, ethoca, Ever Compliant, FICO, feedzai, First Data, FORTER, Guardian Analytics, IdentityMind Global, IdenTrust, iovation, Kount, MagicCube, Maxmind, NetGuardians, NS8, NU Data Security, Pondera, RISKified, Shift Technology, sift science, SIGNIFYD, Socure, TokenID, ThreatMetrix, UNIKEN, technology

Cloud Security

Infrastructure

Container
aqua, Capsule8, layeredinsight, NeuVector, Polyverse, StackRox, Twistlock

Aviatrix, Armor, BetterCloud, Bracket, cavirin, ClearDATA, Cloudway, CloudPassage, Dome9, Edgewise, evident.io, HyTrust, illumio, Lacework, RedLock, Shelox, threat stack, vARMOUR

CASB
Avanan, bitglass, CipherCloud, Cisco, Coronet, Managed Methods, McAfee, Microsoft, netskope, Oracle, proofpoint, Securiqo, Skyformation, StratoKey, Symantec, Vaultive

CBINSIGHTS 2018 CYBER DEFENDERS

Continuous Authentication
identifying people based on behaviors throughout a work session

Next-Gen Cloud Security
source code- and policy-driven approaches to secure complex cloud environments

Human-Factor Security
training and technology to thwart email-based attacks known as phishing

Fileless-Attack Security
the future of fighting malware on endpoints and protecting enterprise networks

Autonomous Watchdogs
software that automatically executes security protocols

Dark Web Intelligence
startups monitoring illicit activity in the hidden corners of the Internet

IIoT Shields
defending connected critical infrastructure against espionage and sabotage

Security By Design
embedding security controls and processes into software development operations

Web Policing
patrolling websites, apps, and online services for malicious Internet traffic

Cyber Actuaries
startups offering tools for quantifying cyber risk and sizing insurance premiums

Crowdsourced Security
ethical hackers employed to discover software vulnerabilities

Fraud Hunters
finding and eliminating synthetic identity fraud

DIY Digital Privacy
tools to help consumers take digital privacy back into their own hands

Identity Vaults
preserving the secrecy of enterprise customers' personal information (PII)

29 STARTUPS

with the potential to transform cybersecurity

TIGERA
ShiftLeft
KnowBe4
IRONSCALES
UNIFYID
BIOCATCH
Virsec
MINERVA
BigID
D-ID
RESPOND
JASK
Keybase
CIPHY
FLASHPOINT
TERBIUM LABS
SIGNIFYD
feedzai
DRAGOS
CYLUS
hackerone
detectify
bugcrowd
snyk
aqua
corax
cyberGRX
StealthSecurity
netsparker

“For one, security teams are overwhelmed. **The average security team typically examines less than 5% of the alerts flowing into them every day** (and in many cases, much less than that). "

Venturebeat

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

57% of respondents said the **time to resolve an incident has increased**

65% reported the **severity of attacks has increased**

Ponemon Institute

Source:

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

> Having **insufficient skilled personnel** dedicated to cybersecurity was the second biggest barrier to cyber resilience, with only 29% having the ideal staffing level.

Ponemon Institute

Source:

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

“”

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

Ponemon Institute

Source:

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

Automation Can Become The Lingua Franca Of IT Security

What Is It?

Ansible 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.

Ansible Security Automation is a supported set of Ansible modules, roles and playbooks designed to unify the security response to cyberattacks in a new way - by orchestrating the activity of multiple classes of security solutions that wouldn't normally integrate with each other.

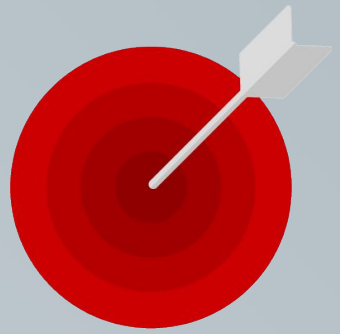
What Does It Do?

Triage Of Suspicious Activities

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

Who Is It For?

Security Teams In Large Organizations

Security Operations Centres (SOCs) dealing with increasingly fast and complex attacks

Managed Security Service Providers

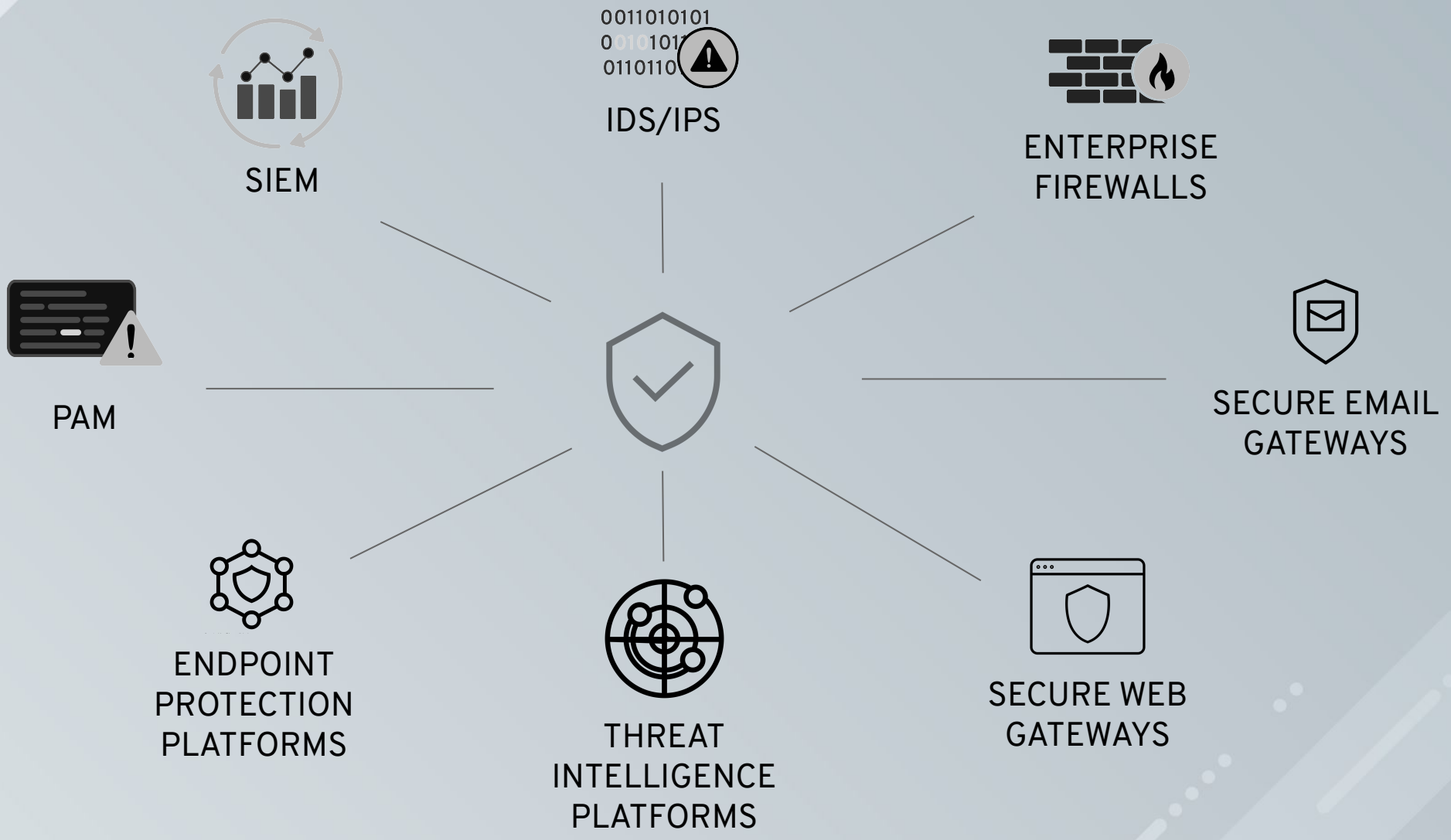
Dealing with thousands of security solutions across their whole customer base

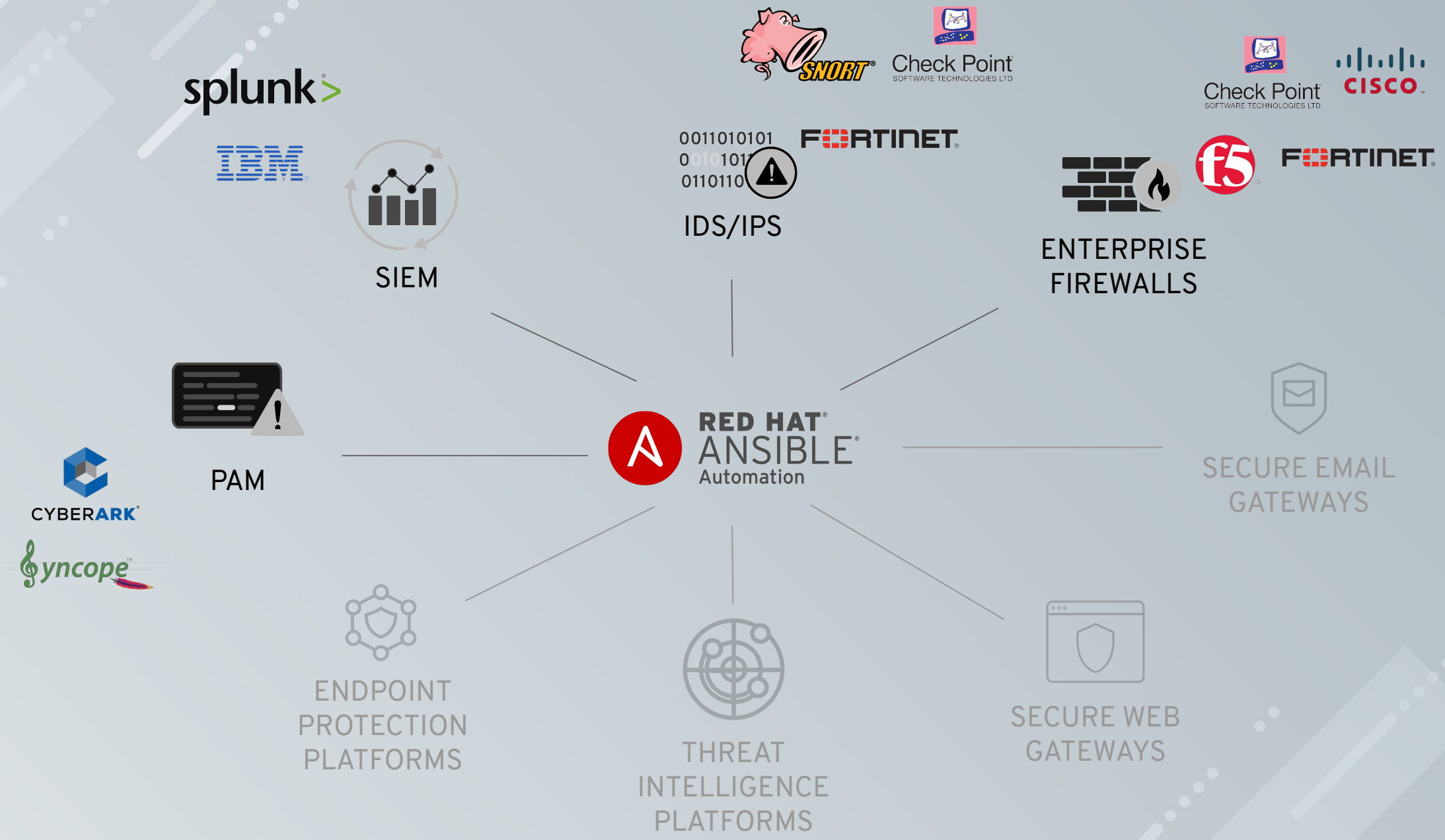
Security Isvs

Offering security orchestration and automation solutions currently using custom-made automation frameworks

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


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

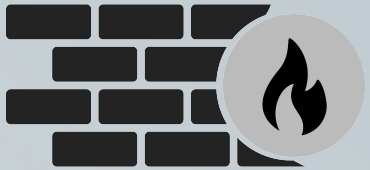

splunk>
IBM
SIEM
SNORT
Check Point
SOFTWARE TECHNOLOGIES LTD
0011010101
0110110
FORTINET
IDS/IPS
Check Point
SOFTWARE TECHNOLOGIES LTD
CISCO
f5
FORTINET
ENTERPRISE FIREWALLS
PAM
CYBERARK
Syncope
RED HAT
ANSIBLE
Automation
SECURE EMAIL GATEWAYS
ENDPOINT PROTECTION PLATFORMS
THREAT INTELLIGENCE PLATFORMS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

Who Are Our Partners?

Security Information & Events Management

splunk>

IBM



Enterprise Firewalls

Check Point SOFTWARE TECHNOLOGIES LTD

CISCO

f5

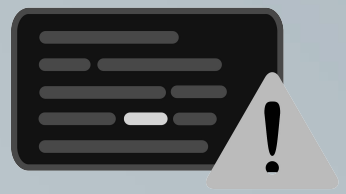
FORTINET

Intrusion Detection & Prevention Systems

SNORT

Check Point SOFTWARE TECHNOLOGIES LTD

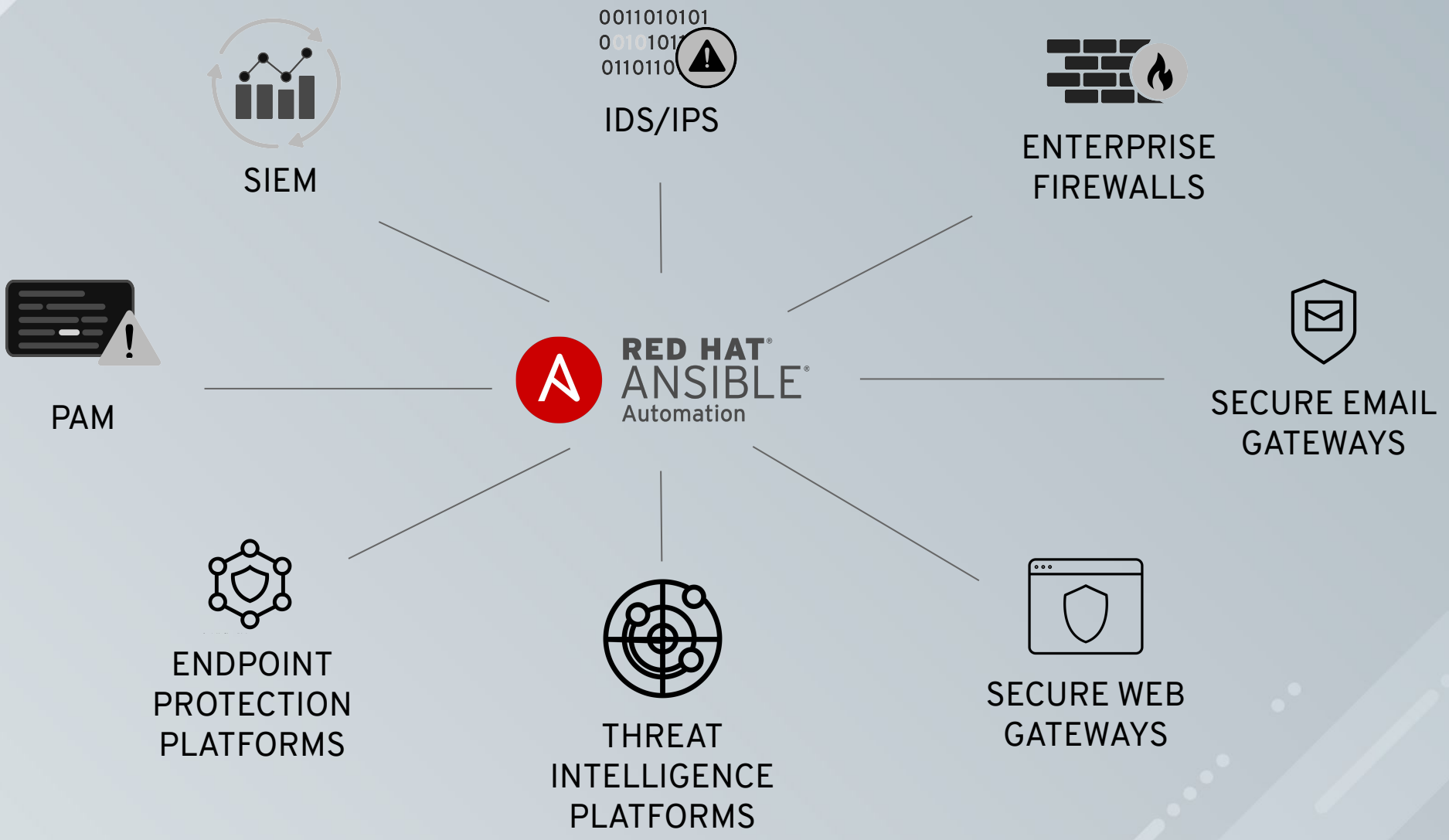
FORTINET

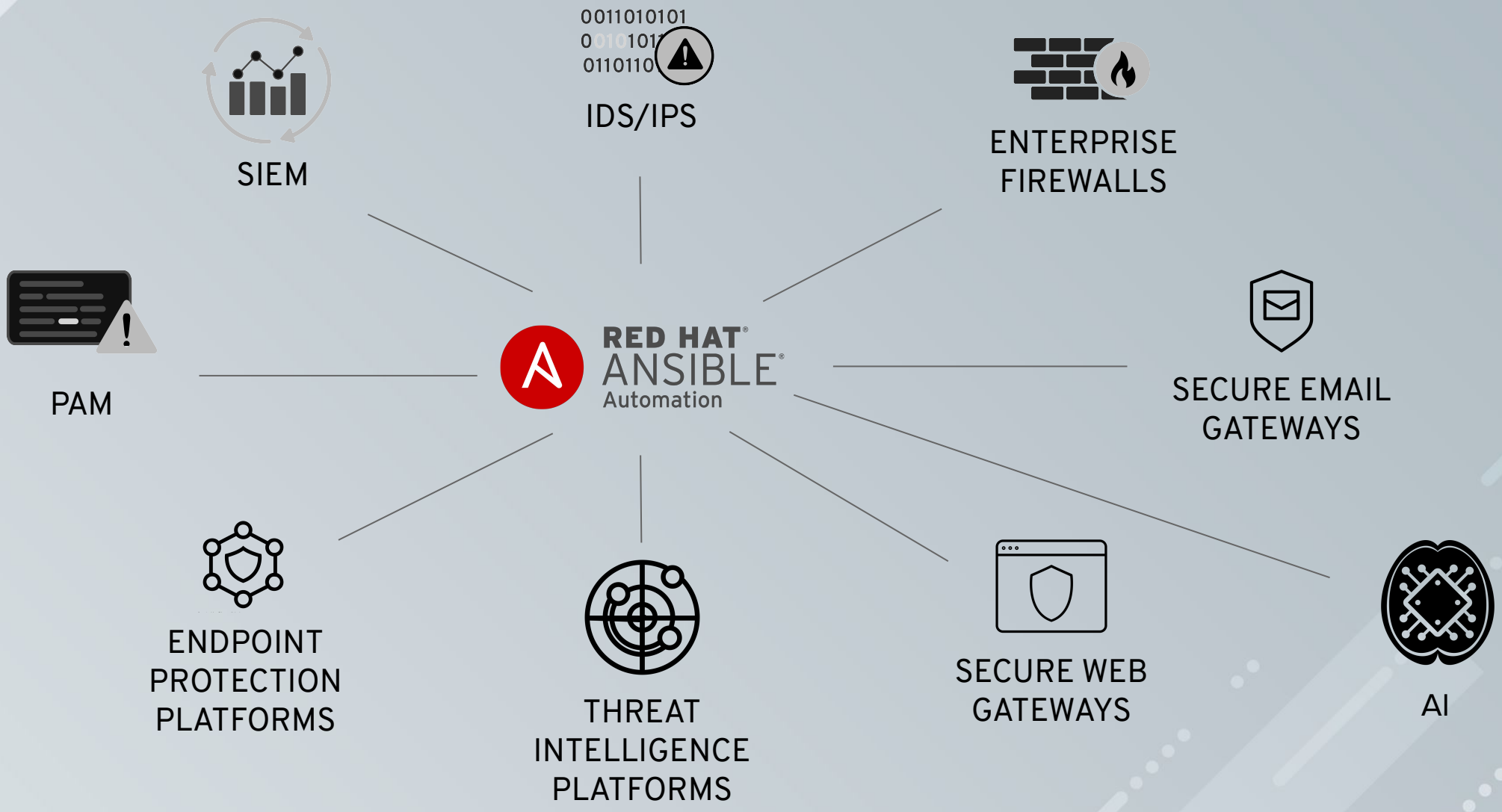


Privileged Access Management

CYBERARK

Syncope


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


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

Typical Use Cases

Most prominent scenarios for threat analysis

01

Triage Of Suspicious Activities:
Application behaviour

02

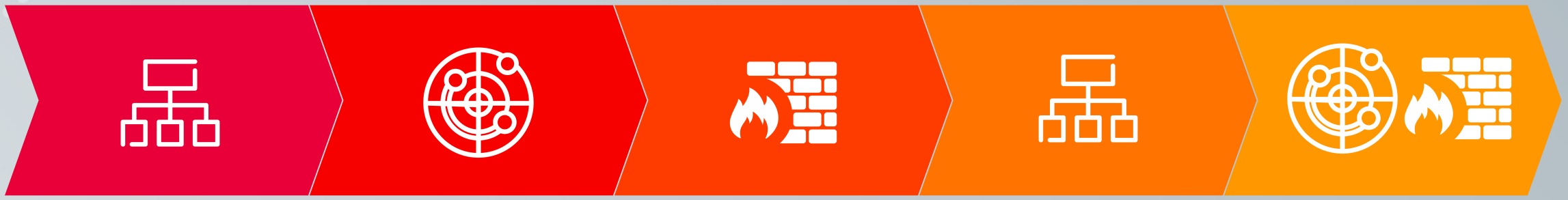
Threat Hunting:
Firewall rule violation

03

Incident Response:
SQL Injection Attack

Risk Assessment: 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 NGFW for more information.

SNORT®

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

Check Point® SOFTWARE TECHNOLOGIES LTD.

Raises the level of logging on low level networking perimeter.

splunk>

Consolidates information for the triage.

SNORT® Check Point® SOFTWARE TECHNOLOGIES LTD.

Restore original configurations.

Threat Hunting: Firewall Rule Violation

A Threat Intelligence Or Incident Responder Could Investigate An Incident And End Up With Hundreds Of Ips, File Hashes, And Domains.

CISCO

Registers a continuous rule violation. Sends alerts to IBM QRadar.

IBM

Creates an offense, requests additional information to Fortinet IPS.

FORTINET

Creates a new rule to investigate the origin of the violation.

IBM

Confirms the rule violation is caused by a misconfigured IP address.

CISCO

Whitelists the IP address.

Incident Response: Sql Injection Attack

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

Check Point IPS detects a SQL Injection attack & alerts IBM QRadar.

Validates the threat, creates an Offense & triggers remediation.

Fortinet NGFW creates a new rule to blacklist the IP source of the attack.

Confirms the end of the attack & updates IBM QRadar.

Double checks the end of the attack and closes the incident.

How Can You Trigger The Remediation?

	WHO	HOW	THROUGH	EXAMPLES
NOW	splunk> IBM	Systems with logic on board, such SOAR or SIEM, can trigger actions when a set of conditions are matched. Actions can simply be launching scripts or directly linux commands.	RED HAT ANSIBLE Engine RED HAT ANSIBLE Tower	Splunk can use *custom search command* or, *custom alert action scripts* to execute a perl/python script that calls Ansible Linux command. Through *Workflow actions* Splunk can call Ansible Tower APIs.
NOW	CISCO SNORT FORTINET Check Point SOFTWARE TECHNOLOGIES LTD.	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. 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.	RED HAT ANSIBLE Engine	Snort can output as syslog and use syslog-ng's *program()* destination combined with a filter. Check Point can schedule a *cronjob* in the management station.
FUTURE	RED HAT ANSIBLE Tower	Ansible Tower can provide a central point of coordination for all the technologies involved in a remediation process. 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.	CISCO SNORT FORTINET Check Point SOFTWARE TECHNOLOGIES LTD.	

#ANSIBLEAUTOMATES

redhat | ANSIBLE