VITA Virginia Information Technologies Agency

Welcome and Opening Remarks

Mike Watson

July 8, 2020

July ISOAG AGENDA

- Mike Watson, Opening & Welcome Remarks
- Jayne Freidland, NIC
- Nick Lenaeus & Sean Cannata, RedHat
- Rick Tiene, MissionSecure
- Stephone Dixon, SAIC
- Ed Miller, VITA

Incident Response and Secure Payment Processing

Jayne Friedland Holland

Chief Security Officer, NIC Inc.

VITA | July 8, 2020

AGENDA

01 Incident Response Planning

02 Secure Payment Processing

03 PCI DSS 4.0

05 Text Here

Incident Response Planning

16 billion records

compromised in 2019

INCIDENT RESPONSE PLANNING

*It's not a question of **if**, but **when**.*

- Today's reality and NIC's mantra – **ALWAYS BE PREPARED**
- No one is immune from attack
- Government is one of the top 3 targets for attackers
- Social, legal and legislative issues have made state government an even bigger target
- NIC maintains a comprehensive, multi-department incident response plan for every state we serve – plan is reviewed, updated and tested regularly

TIMING IS EVERYTHING – Have an Incident Response Plan

- **Define events** or incidents that activate the plan
- **Establish team** members
- **Designate roles** and responsibilities
- **Establish timelines** for notification and communication
- **Test annually** and modify where appropriate
- **Train employees** on the process

TIMING IS EVERYTHING – Preserve the Scene

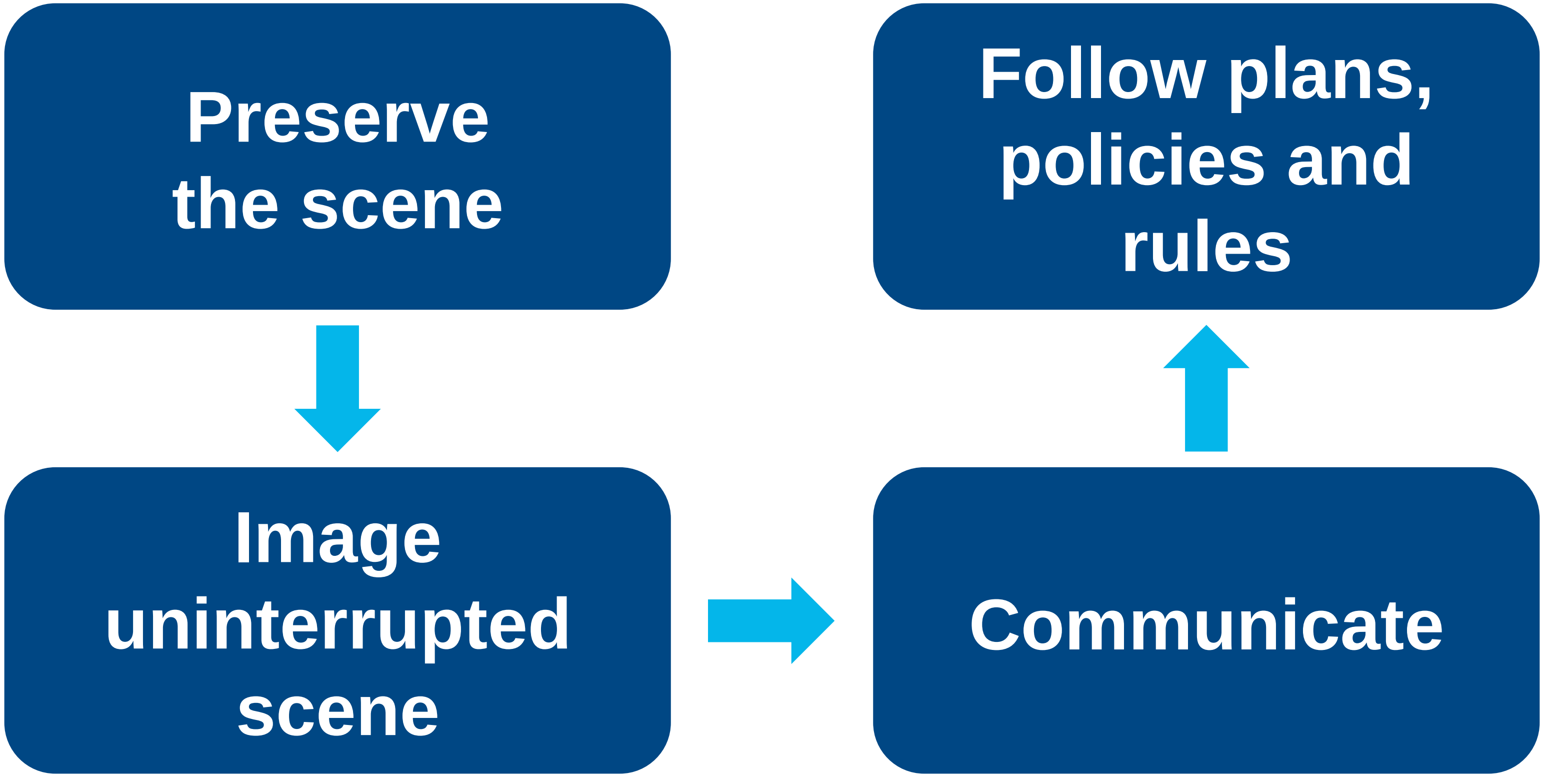

Preserve the scene

Image uninterrupted scene

Communicate

Follow plans, policies and rules

TIMING IS EVERYTHING – Assess the Scene

- When was unusual activity first observed?
- Was data exfiltrated? If so, what data?
- What else happened?
- How did they gain access?
- Was malware involved?
- Do you have the data to answer the questions?
- Do you have the forensic expertise, or will outside support be necessary?
- Do you know if the incident has been contained?

TIMING IS EVERYTHING – Understand Breach Notification Requirements

STATE
Data Breach
Notification Laws

FEDERAL
Laws
i.e., HIPAA

INDUSTRY
Standards
i.e., PCI DSS

TIMING IS EVERYTHING – Third-Party Agreements

- Forensic support
- Call center support
- Identity theft services support
- Public relations support
- Printing support

TIMING IS EVERYTHING – Communication Templates

- Key messages with Q&A
- Press release
- Webpage
- Notification letter
- Call center script

Secure Payment Processing

PAYMENT FRAUD AND COVID-19

COVID-19 has increased the demand for online transactions.

More transactions create more risk.

475% increase in malicious reports related to Coronavirus in March *

**Source: PCI Security Standards Council, LLC*

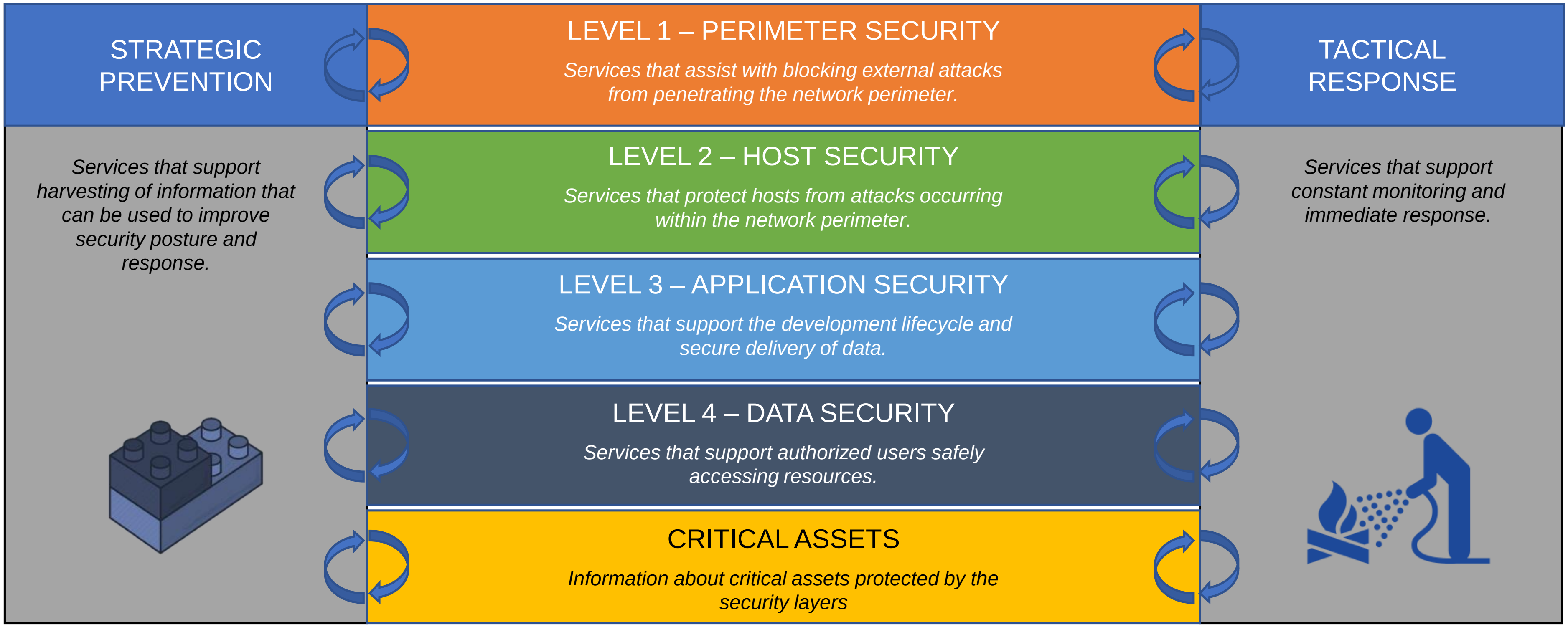
HIGHLIGHTS OF NIC'S SECURITY PROGRAM

- Controls based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, NIC Corporate Security Requirements and PCI DSS
- Comprehensive policies, standards, and procedures
- Personnel & Security Training
- Physical Security – at Data Centers and NIC's offices
- Network Security
- Systems Security
- Application Security
- Data Security
- Logical security
- Encryption
- Audits, Testing and Governance
- Detailed Incident Response Policy and Procedures

HIGHLIGHTS OF NIC'S SECURITY PROGRAM

- Certified by the Payment Card Industry Data Security Standards (PCI-DSS) as a Level 1 Service Provider by a Qualified Security Assessor
- Listed as a PCI-DSS Compliant provider on Visa and MasterCard's Global Registry of Service Providers
- SOC2, Type 2 certified solution
- Fully compliant with federal, state, local, and industry standards
- Meets all Sarbanes-Oxley compliance requirements
- Participating Organization on the Payment Card Industry Security Standards Council

HIGHLIGHTS OF NIC’S SECURITY PROGRAM



STRATEGIC PREVENTION

Services that support harvesting of information that can be used to improve security posture and response.

LEVEL 1 – PERIMETER SECURITY

Services that assist with blocking external attacks from penetrating the network perimeter.

LEVEL 2 – HOST SECURITY

Services that protect hosts from attacks occurring within the network perimeter.

LEVEL 3 – APPLICATION SECURITY

Services that support the development lifecycle and secure delivery of data.

LEVEL 4 – DATA SECURITY

Services that support authorized users safely accessing resources.

CRITICAL ASSETS

Information about critical assets protected by the security layers

TACTICAL RESPONSE

Services that support constant monitoring and immediate response.

TIPS FOR KEEPING PAYMENT DATA SECURE

- Avoid storing payment data
- Use password best practices
- Ensure software is not vulnerable, and it’s patched and up-to-date
- Encrypt sensitive information
- Use secure remote access
- Check firewalls
- Choose trusted partners

*Source: PCI Security Standards Council, LLC

TIPS FOR KEEPING PAYMENT DATA SECURE (continued)

- Disable or uninstall necessary apps and software
- Implement access controls
- Disconnect remote access sessions after period of inactivity
- Make sure incident response plans have been updated
- Understand employees can be our weakest link and train on social engineering attacks

**Source: PCI Security Standards Council, LLC*

PCI DSS v4.0

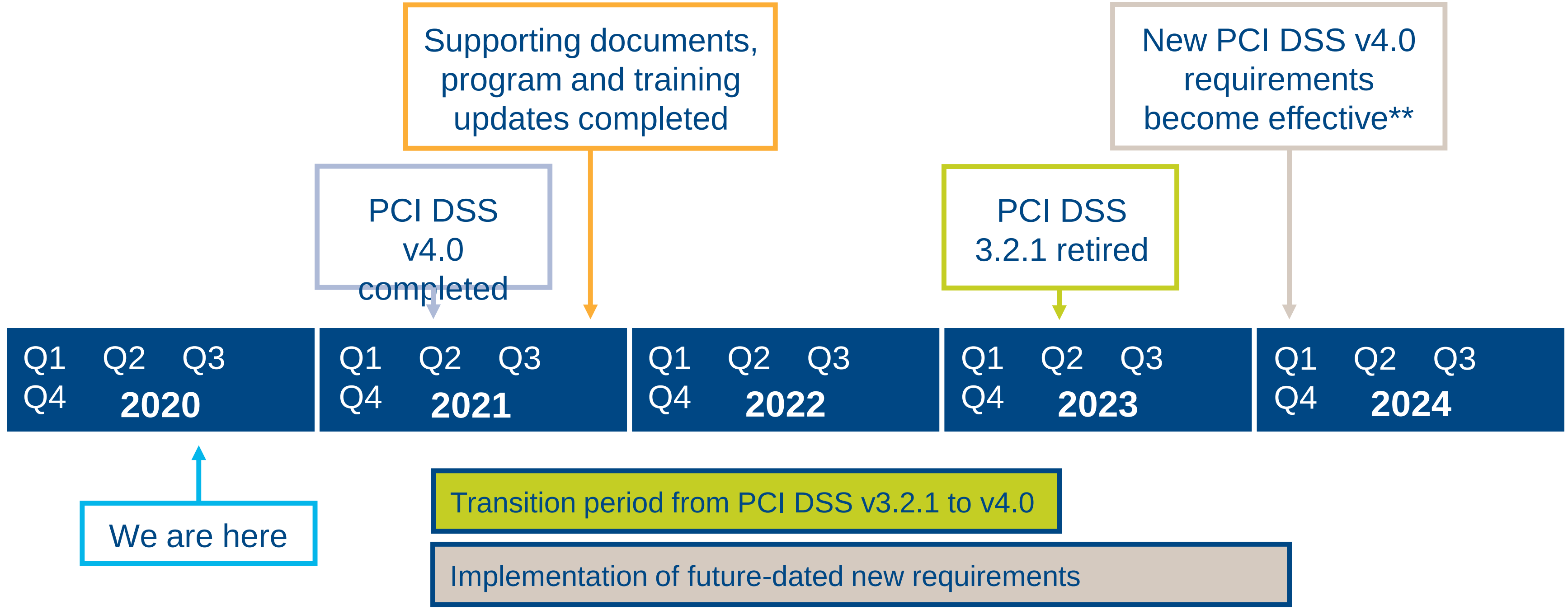
PCI DSS v4.0 – High-Level Goals

- Ensure the standard continues to meet the security needs of the payments industry
- Add flexibility and support of additional methodologies to achieve security
- Promote security as a continuous process
- Enhance validation methods and procedures

PCI DSS v4.0 – Upcoming Changes

- Two ways to validate
  1. Defined (standard way done today)
  2. Customized (replaces compensating controls)
- Will still have 12 main requirements, but wording of them will change in some cases
- Update guidance to be clear and provide more direction
- Improve standards to keep up with changes in security best practices such as requiring TLS on internal networks

PCI DSS v4.0 – Transition Timeline*



Supporting documents, program and training updates completed

New PCI DSS v4.0 requirements become effective**

PCI DSS v4.0 completed

PCI DSS 3.2.1 retired

Q1 Q2 Q3 Q4 2020

Q1 Q2 Q3 Q4 2021

Q1 Q2 Q3 Q4 2022

Q1 Q2 Q3 Q4 2023

Q1 Q2 Q3 Q4 2024

We are here

Transition period from PCI DSS v3.2.1 to v4.0

Implementation of future-dated new requirements

***All dates based on current projections and subject to change.**

** Refers to new PCI DSS requirements that are future-dated. Effective date to be determined upon confirmation of all new requirements.

THANK YOU

Jayne Friedland Holland

Chief Security Officer | NIC Inc.
jayne@egov.com

Increasing Compliance and Security through Automation

Jul 2020

Red Hat Team

Collin Suggs, Account Executive
csuggs@redhat.com
919.308.3911

Maksim Nikiforov, Senior Solutions Architect
maksim@redhat.com
951.444.0108

Nick Lenaeus
Emerging Technology and Business Advisor
nick.Lenaeus@redhat.com
919.949.6546

Sean Cannata
Specialist Solutions Architect
scannata@redhat.com
630.809.5102

“”

Worldwide spending on **security-related hardware, software, and services** will be **$106.6 billion in 2019**, an increase of 10.7% over 2018. This amount will reach **$151.2 billion** in **2023** with a compound annual growth rate (CAGR) of 9.4% over the 2019-2023 forecast period.

—

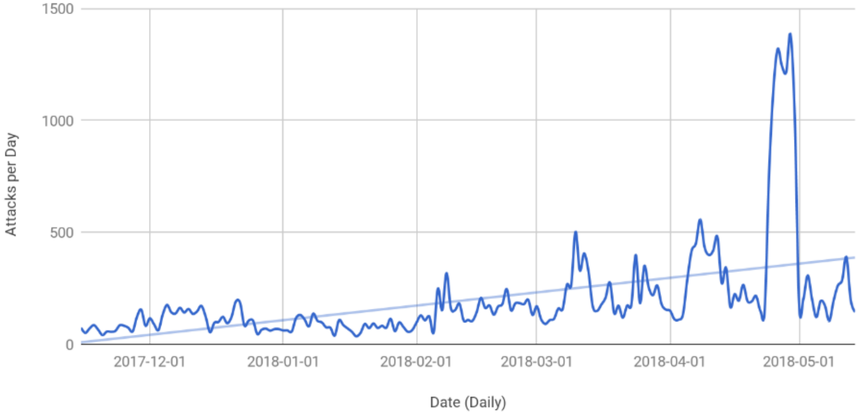
IDC

Source:
New IDC Spending Guide Sees Solid Growth Ahead for Security Products and Services

DEVELOPERS AREN'T SECURITY EXPERTS

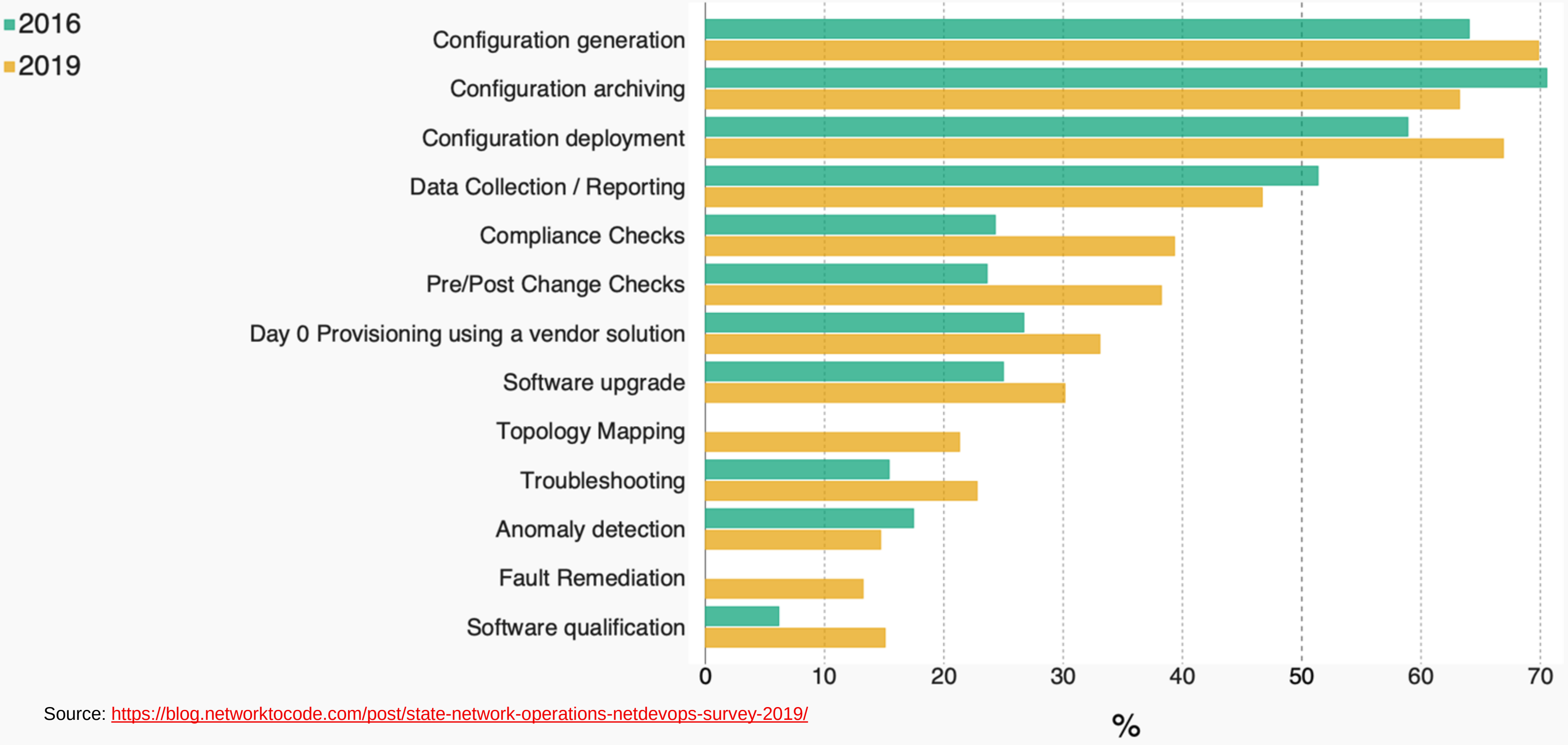
L7 ATTACKS ON THE RISE

*"**The softest target in most organizations is the app layer and attackers know this**. In the last 6 months we have seen a large **upward trend of Layer 7 based DDoS attacks**… On average seeing around 160 attacks a day, with some days spiking up to over 1000 attacks."*



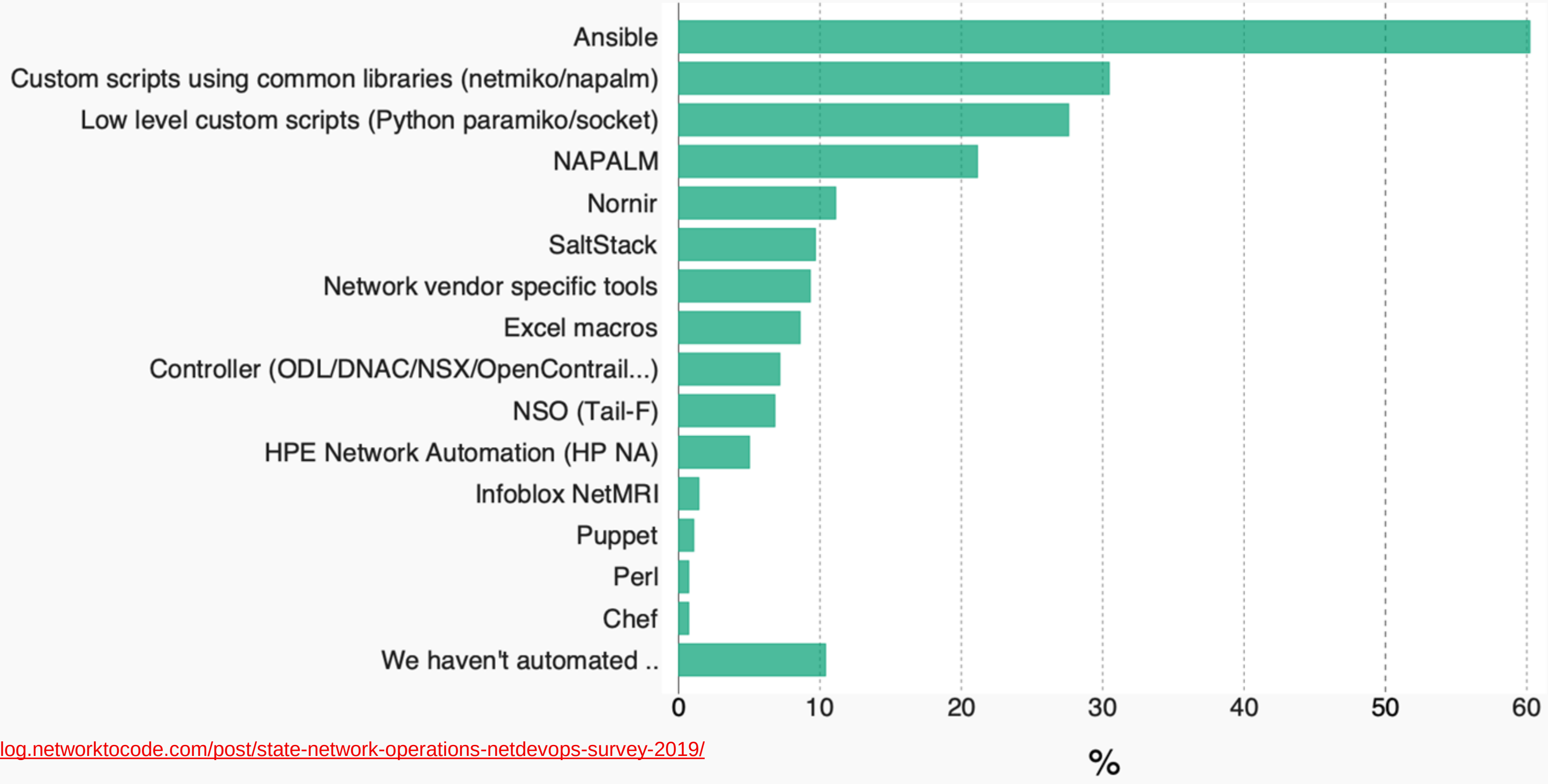
blog.cloudflare.com/rate-limiting-delivering-more-rules-and-greater-control/

NetDevOps Survey
What operations in your network are currently automated?



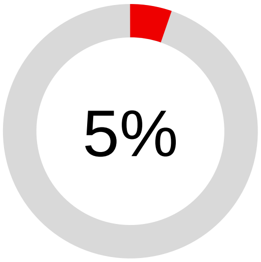
Source: https://blog.networktocode.com/post/state-network-operations-netdevops-survey-2019/

NetDevOps Survey (2019)
Configuration – If you are automating the generation and/or the deployment of your configurations what solution(s) are you using?
Stats: 2.13 avg, max 7

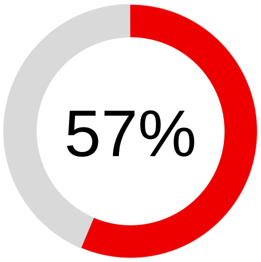


Source: https://blog.networktocode.com/post/state-network-operations-netdevops-survey-2019/

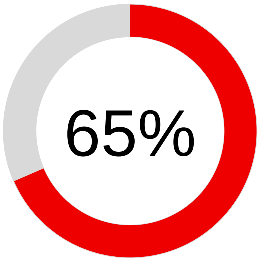
Why Ansible security automation?



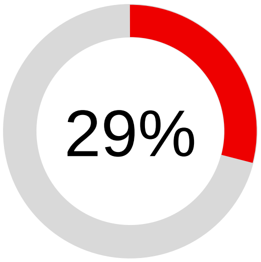
Portion of alerts coming in that the average security team examines every day



Said the time to resolve an incident has grown



Reported increased Severity of attacks



Have their ideal security-skilled 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)

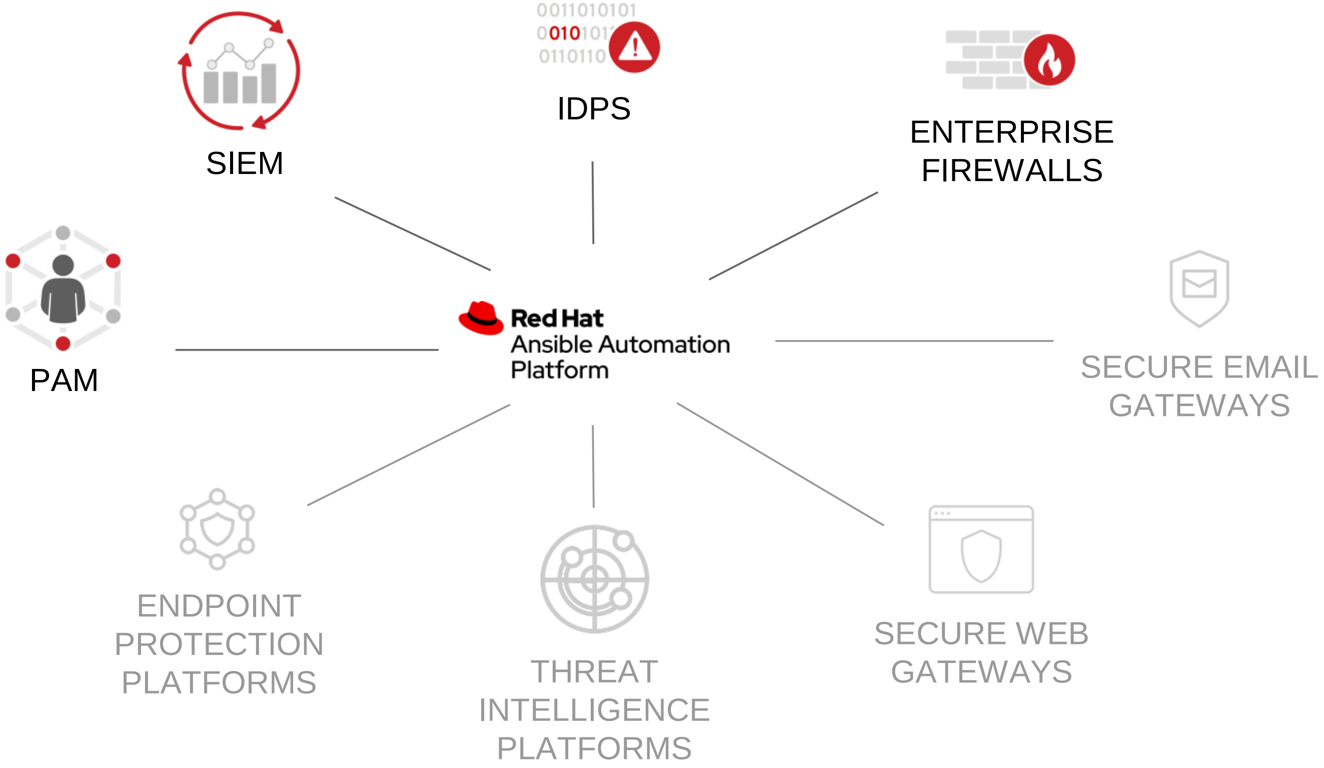
2 https://venturebeat.com/2017/12/16/the-lesson-behind-2017s-biggest-enterprise-security-story/

‘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?



Red Hat Ansible Automation Platform

SIEM

IDPS

ENTERPRISE FIREWALLS

PAM

SECURE EMAIL GATEWAYS

ENDPOINT PROTECTION PLATFORMS

THREAT INTELLIGENCE PLATFORMS

SECURE WEB GATEWAYS

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.

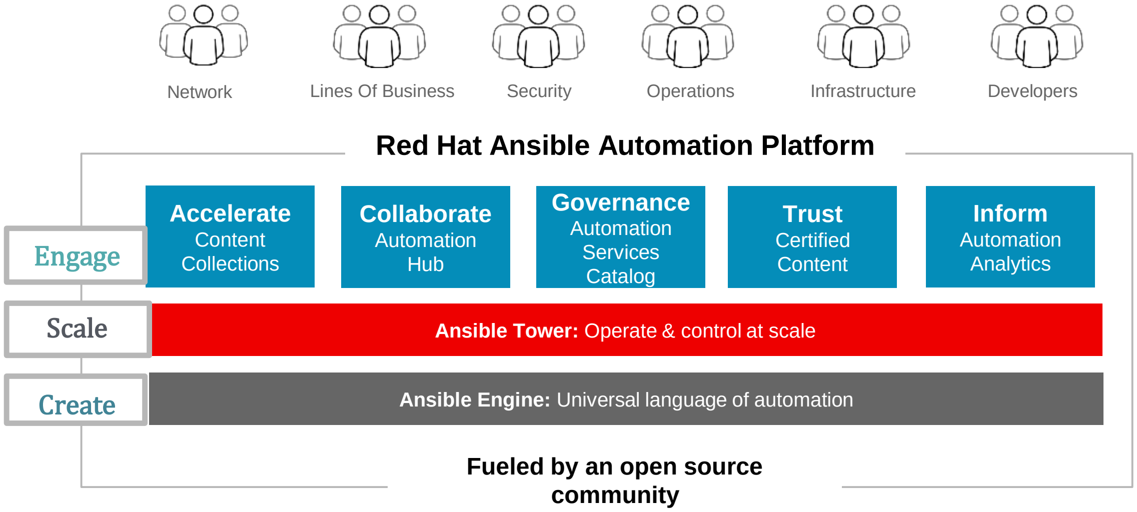
By automating security capabilities, organizations can better unify responses to cyberattacks through the coordination of multiple, disparate security solutions, helping these technologies to act as one in the face of an IT security event.

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

What 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.



Network

Lines Of Business

Security

Operations

Infrastructure

Developers

Red Hat Ansible Automation Platform

Engage

Accelerate Content Collections

Collaborate Automation Hub

Governance Automation Services Catalog

Trust Certified Content

Inform Automation Analytics

Scale

Ansible Tower: Operate & control at scale

Create

Ansible Engine: Universal language of automation

Fueled by an open source community

Growth by the numbers:

2M

downloads per month

4K

modules

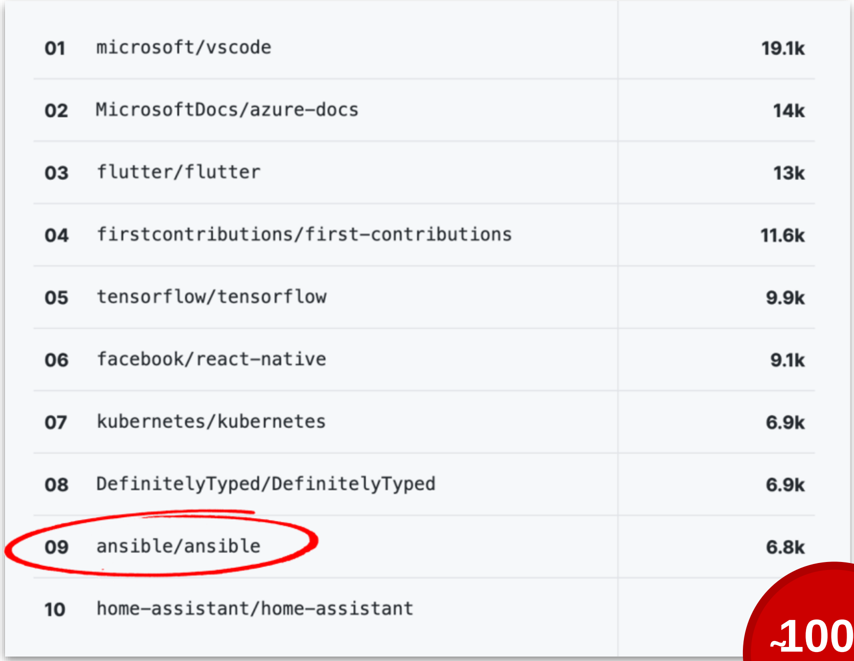
9TH

of 96M projects on
GitHub by contributors

>4M

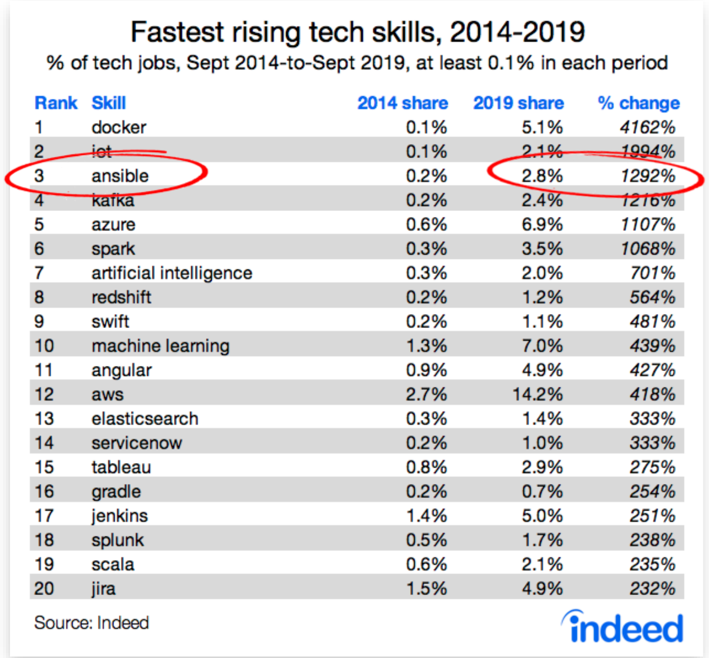
systems managed
by Red Hat®

Ansible Project Momentum - **Contribution**



01	microsoft/vscode	19.1k
02	MicrosoftDocs/azure-docs	14k
03	flutter/flutter	13k
04	firstcontributions/first-contributions	11.6k
05	tensorflow/tensorflow	9.9k
06	facebook/react-native	9.1k
07	kubernetes/kubernetes	6.9k
08	DefinitelyTyped/DefinitelyTyped	6.9k
09	ansible/ansible	6.8k
10	home-assistant/home-assistant	

~100M PROJECTS



Fastest rising tech skills, 2014-2019

% of tech jobs, Sept 2014-to-Sept 2019, at least 0.1% in each period

Rank	Skill	2014 share	2019 share	% change
1	docker	0.1%	5.1%	*4162%*
2	iot	0.1%	2.1%	*1994%*
3	ansible	0.2%	2.8%	*1292%*
4	kafka	0.2%	2.4%	*1216%*
5	azure	0.6%	6.9%	*1107%*
6	spark	0.3%	3.5%	*1068%*
7	artificial intelligence	0.3%	2.0%	*701%*
8	redshift	0.2%	1.2%	*564%*
9	swift	0.2%	1.1%	*481%*
10	machine learning	1.3%	7.0%	*439%*
11	angular	0.9%	4.9%	*427%*
12	aws	2.7%	14.2%	*418%*
13	elasticsearch	0.3%	1.4%	*333%*
14	servicenow	0.2%	1.0%	*333%*
15	tableau	0.8%	2.9%	*275%*
16	gradle	0.2%	0.7%	*254%*
17	jenkins	1.4%	5.0%	*251%*
18	splunk	0.5%	1.7%	*238%*
19	scala	0.6%	2.1%	*235%*
20	jira	1.5%	4.9%	*232%*

Source: Indeed

indeed

Source:
https://octoverse.github.com/#top-and-trending-projects,
https://www.hiringlab.org/2019/11/26/fastest-rising-tech-skills/

Ansible automates technologies you use

Time to automate is measured in minutes

Cloud

- AWS
- Azure
- Digital Ocean
- Google
- OpenStack
- Rackspace
- **+more**

Operating Systems

- RHEL
- Linux
- Windows
- **+more**

Virt & Container

- Docker
- VMware
- RHV
- OpenStack
- OpenShift
- **+more**

Storage

- Netapp
- Red Hat Storage
- Infinidat
- **+more**

Windows

- ACLs
- Files
- Packages
- IIS
- Regedits
- Shares
- Services
- Configs
- Users
- Domains
- **+more**

Network

- A10
- Arista
- Aruba
- Cumulus
- Bigswitch
- Cisco
- Dell
- Extreme
- F5
- Lenovo
- MikroTik
- Juniper
- OpenSwitch
- **+more**

Security

- Checkpoint
- Cisco
- CyberArk
- F5
- Fortinet
- Juniper
- IBM
- Palo Alto
- Snort
- **+more**

Monitoring

- Dynatrace
- Datadog
- LogicMonitor
- New Relic
- Sensu
- **+more**

Devops

- Jira
- GitHub
- Vagrant
- Jenkins
- Slack
- **+more**

Red Hat Ansible Automation Platform

by the numbers:

94% Reduction in recovery time following a security incident

84% Savings by deploying workloads to generic systems appliances using Ansible Tower

67% Reduction in man hours required for customer deliveries

Financial summary:

146%

ROI on Ansible Automation Platform

<3 MONTHS

Payback

SOURCE: *"The Total Economic Impact™ Of Red Hat Ansible Tower, a June 2018 commissioned study conducted by Forrester Consulting on behalf of Red Hat."*
redhat.com/en/engage/total-economic-impact-ansible-tower-20180710

Red Hat

Ansible Security Ecosystem

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

Ok, But In The End What’s In The Solution?

RED HAT SUPPORTED

SNORT

splunk>

CISCO

IBM

ANSIBLE CERTIFIED CONTENT

Check Point
SOFTWARE TECHNOLOGIES LTD

CISCO

FORTINET

f5

CYBERARK

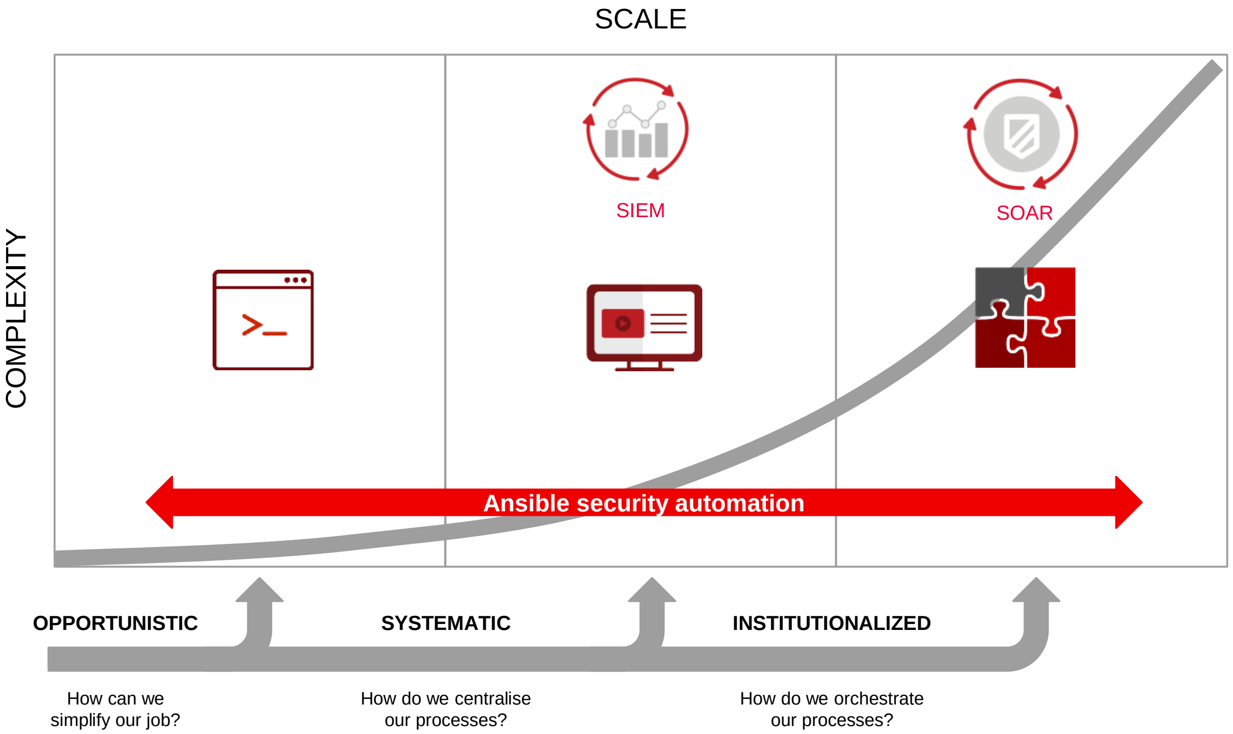
Syncope

SUPPORTED CONTENT

+

COMMUNITY

Security Automation Adoption


SCALE
COMPLEXITY
SIEM
SOAR
Ansible security automation
OPPORTUNISTIC
SYSTEMATIC
INSTITUTIONALIZED
How can we simplify our job?
How do we centralise our processes?
How do we orchestrate our processes?

https://www.ansible.com/blog/the-journey-to-security-automation

Stage 1: Opportunistic

At this stage, most organizations focus only on security operations.
Investigation and remediation processes tend to be spread across different, siloed teams, sometimes located in different physical sites.

Use Cases

- Reducing time to task
- Standardising security tasks

Target Audience

- Security Operations

In this scenario, Ansible Automation offers its ***human-readable YAML language*** *as a tool to easily describe security tasks, compare them and identify the best workflow to be used as a base for standardization. The outcome of this standardization process is a series of roles and playbooks that can be consumed immediately through Red Hat Ansible Engine and become the base for a library of response workflows which security teams will grow over time as more actions and processes are added.*

When security automation projects are successful, the resulting automated workflows can be split and assigned to different teams in the security organization, which maintain control and responsibility on their part of the process.

Additional Red Hat Management Offerings of benefit:

- Red Hat Satellite
- Red Hat Insights

The values automation brings to Security

Increase Speed

Reduce the number of manual steps and GUI-clicking, enable the orchestration of security tools and accelerate their interaction with each other

Reduce Human Errors

Minimize risks with automated workflows, avoid human operator errors in time-sensitive, stressful situations

Enforce Consistency

Enable auditable and verifiable security processes by using a single tool and common language covering multiple security tools

Security use cases typical in Stage 1

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 block, unblock IPs/URLs or quarantine a machine

Stage 2: Systematic

At this stage, many of these security teams see the benefit of implementing and operating a cohesive portfolio of security operations tools and services which, potentially, also interoperates with their larger IT practice.

Use Cases

- Centralizing response processes
- Standardising security operations

Target Audience

- Security Analysts
- Security Operations

Introduced at this stage, Red Hat Ansible Tower can ***integrate multiple security teams, helping them work more collaboratively*** *through enterprise features like centralised access to the entire library of response workflows and RBAC.*

More importantly, Ansible Tower offers the ability to ***connect multiple playbooks, from different teams, in structured and conditional workflows*** *that reflect the higher-level security processes.*

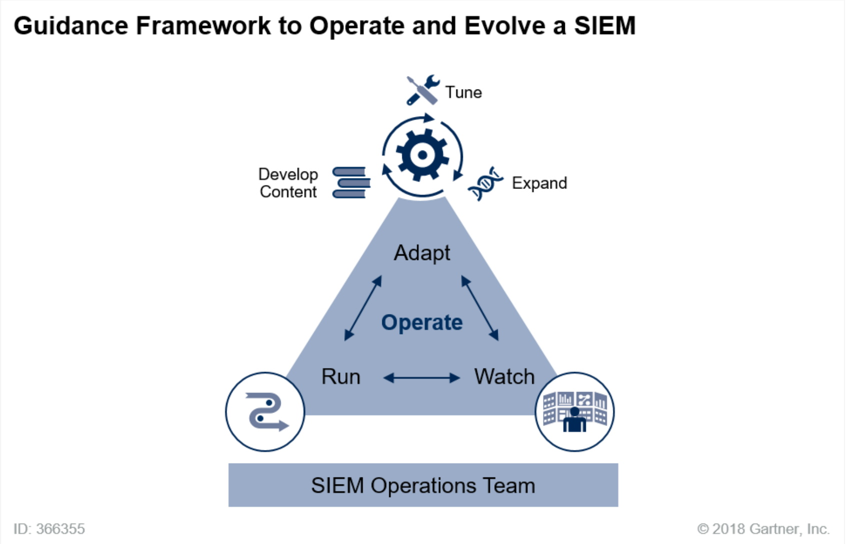
Among enterprises, a popular first step towards these goals is introducing a Security Information and Event Management (SIEM) solution to centralise investigation activities, and to make decisions easy to share across all the teams involved in a specific attack response. Thanks to its REST APIs ***Ansible Tower can more easily integrate with a SIEM, making automated actions available straight from the same tool where these actions are decided.***

Additional Red Hat Management Offerings of benefit:

- Red Hat Satellite
- Red Hat Insights

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 in Stage 2

Simplicity

Automate deployment, configuration and mundane tasks

Consistency

Interoperate multiple platforms from multiple vendors

Modernization

Integrate SIEM in DevSecOps workflows

Extensibility

Automate investigation & remediation tasks from the SIEM

Stage 3: Institutionalised

At this stage, security organizations have created a security operations program, such as the incident response program and its playbooks.

Use Cases

- Automating security processes
- Integrating the security and IT portfolios

Target Audience

- Security Analysts
- CISOs

This is the stage where security teams approach Security Orchestration, Automation and Remediation (SOAR) tools to design and orchestrate the higher-level security workflows identified in previous steps.

*Like for SIEMs, **Ansible Automation can be integrated with SOAR tools to extend their native capabilities**.*

In combination with Ansible Automation, a SOAR can leverage thousands of modules to create automated investigation and remediation plans.

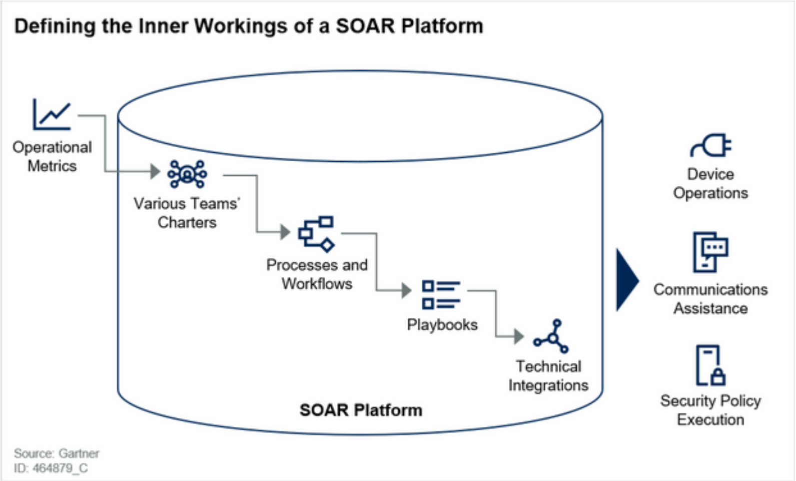
*These modules are contributed by the Ansible community, **Red Hat partners, and Red Hat itself**, and allow customers to automate the actions and configurations of enterprise security solutions as well as operating systems, applications, and network appliances.*

Ansible's automation workflows, written in a human-readable language, make the customization and maintenance of automated investigation and remediation plans simple even for professionals without a developer background.

What is SOAR?

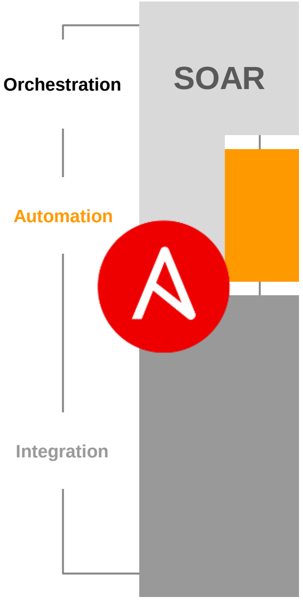
“”

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.



Source:
Preparing Your Security Operations for Orchestration and Automation Tools

How Ansible security automation relates to SOAR?

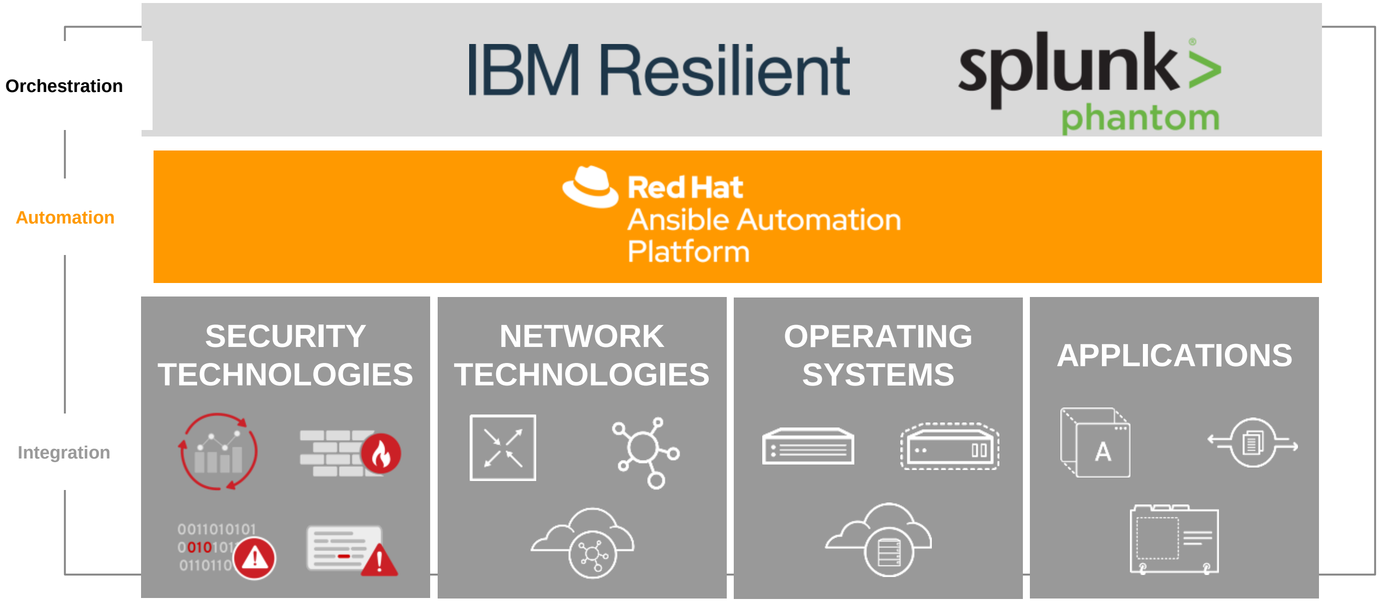


SOAR orchestrates the high-level threat response process. Their Security ‘Playbooks’ focus on Who is doing What, Why and When.

The Ansible Automation Platform automates tasks: the How.

The Ansible Automation Platform content initiatives, like Ansible security automation, provide technology integration: the Where.

Ansible Automation Platform Integration With SOAR



Orchestration

IBM Resilient

splunk> phantom

Automation

Red Hat Ansible Automation Platform

Integration

SECURITY TECHNOLOGIES

NETWORK TECHNOLOGIES

OPERATING SYSTEMS

APPLICATIONS

Use Cases

Security Use Cases

Networking

- IPSec Tunnels
- ACL block/allow IP
- Enable/disable packet capturing
- Switch ports enable/disable
- Verify CVE resolution
- Gather compliance report evidence

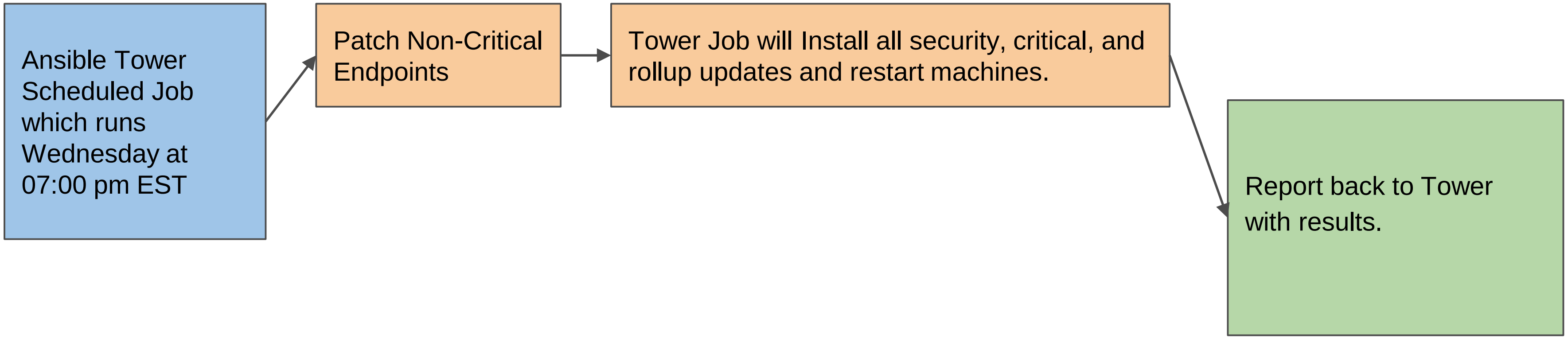
Operations

- Enable/Disable user account
- Check service SSL Certificate for expiry
- Detect system vulnerabilities and remediate
- Policy Enforcement and Auditing to maintain compliance (PCI/SOX/HIPAA)

Systems / Virtualization and Cloud

- Verify CVE resolution
- Gather compliance report evidence

Patch Non-Critical Windows & Install Software via Tower



Ansible Tower Scheduled Job which runs Wednesday at 07:00 pm EST

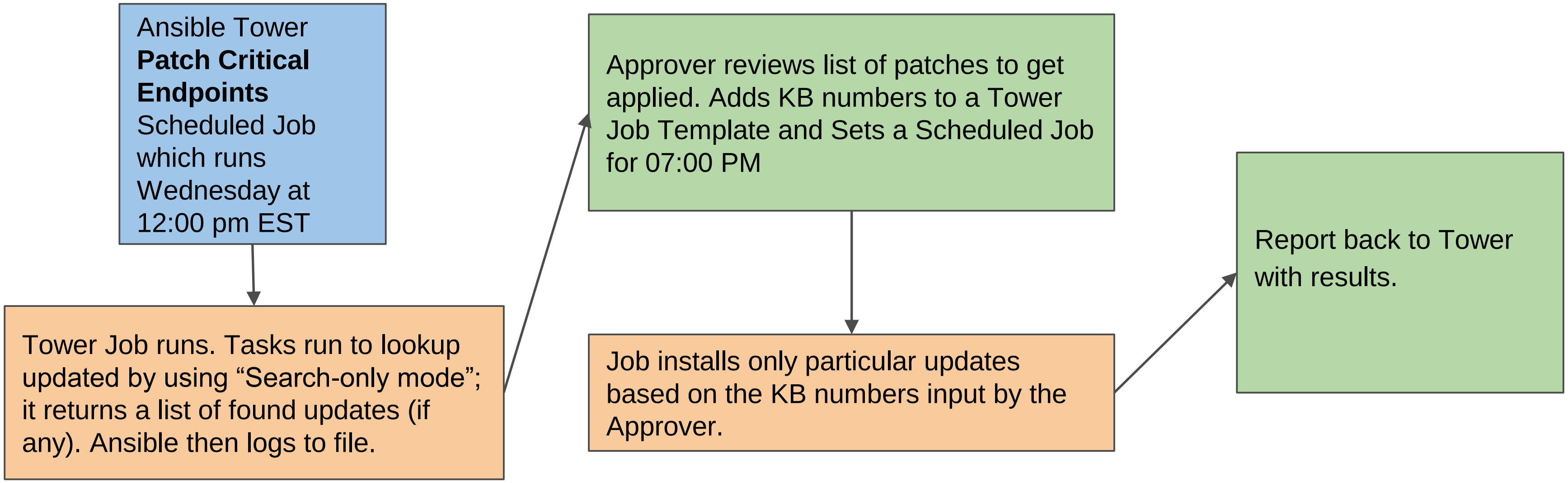
Patch Non-Critical Endpoints

Tower Job will Install all security, critical, and rollup updates and restart machines.

Report back to Tower with results.

Stage 1 - Opportunistic

Patch Critical Windows & Install Software via Tower



Ansible Tower **Patch Critical Endpoints** Scheduled Job which runs Wednesday at 12:00 pm EST

Tower Job runs. Tasks run to lookup updated by using “Search-only mode”; it returns a list of found updates (if any). Ansible then logs to file.

Approver reviews list of patches to get applied. Adds KB numbers to a Tower Job Template and Sets a Scheduled Job for 07:00 PM

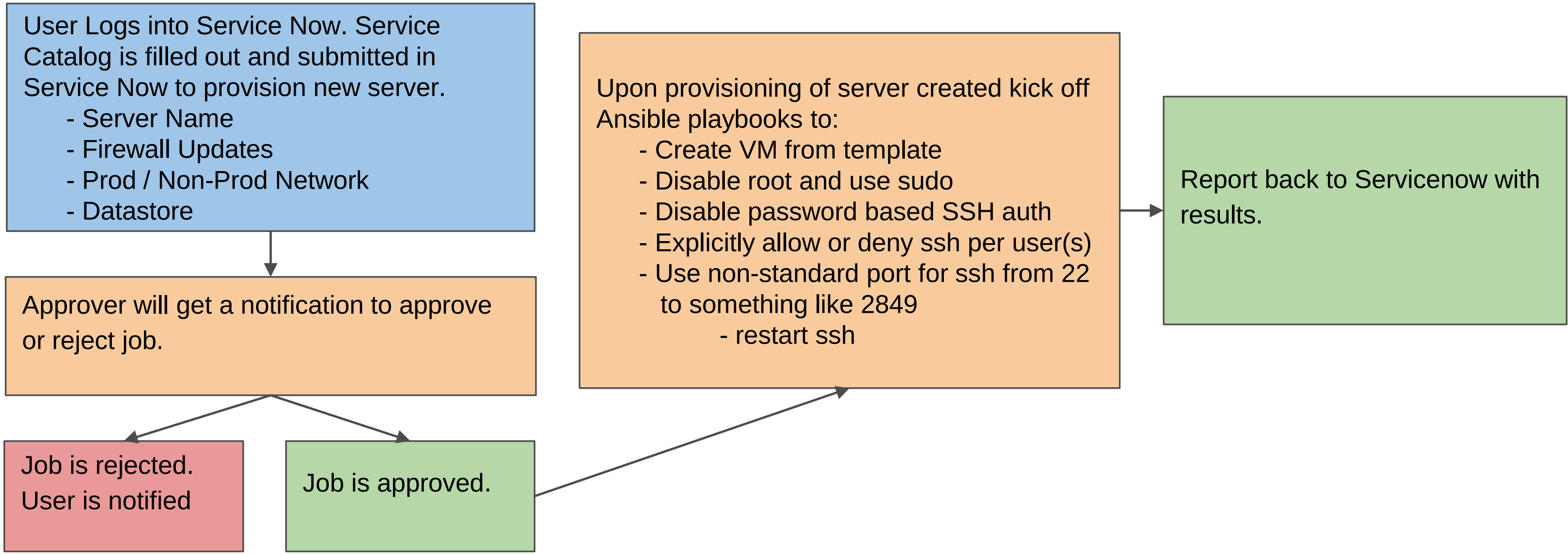
Job installs only particular updates based on the KB numbers input by the Approver.

Report back to Tower with results.

Stage 1 – Opportunistic, adding in governance

Use Cases

VM Template Deployment & Auth Security via Servicenow



User Logs into Service Now. Service Catalog is filled out and submitted in Service Now to provision new server.

- Server Name
- Firewall Updates
- Prod / Non-Prod Network
- Datastore

Approver will get a notification to approve or reject job.

Job is rejected. User is notified

Job is approved.

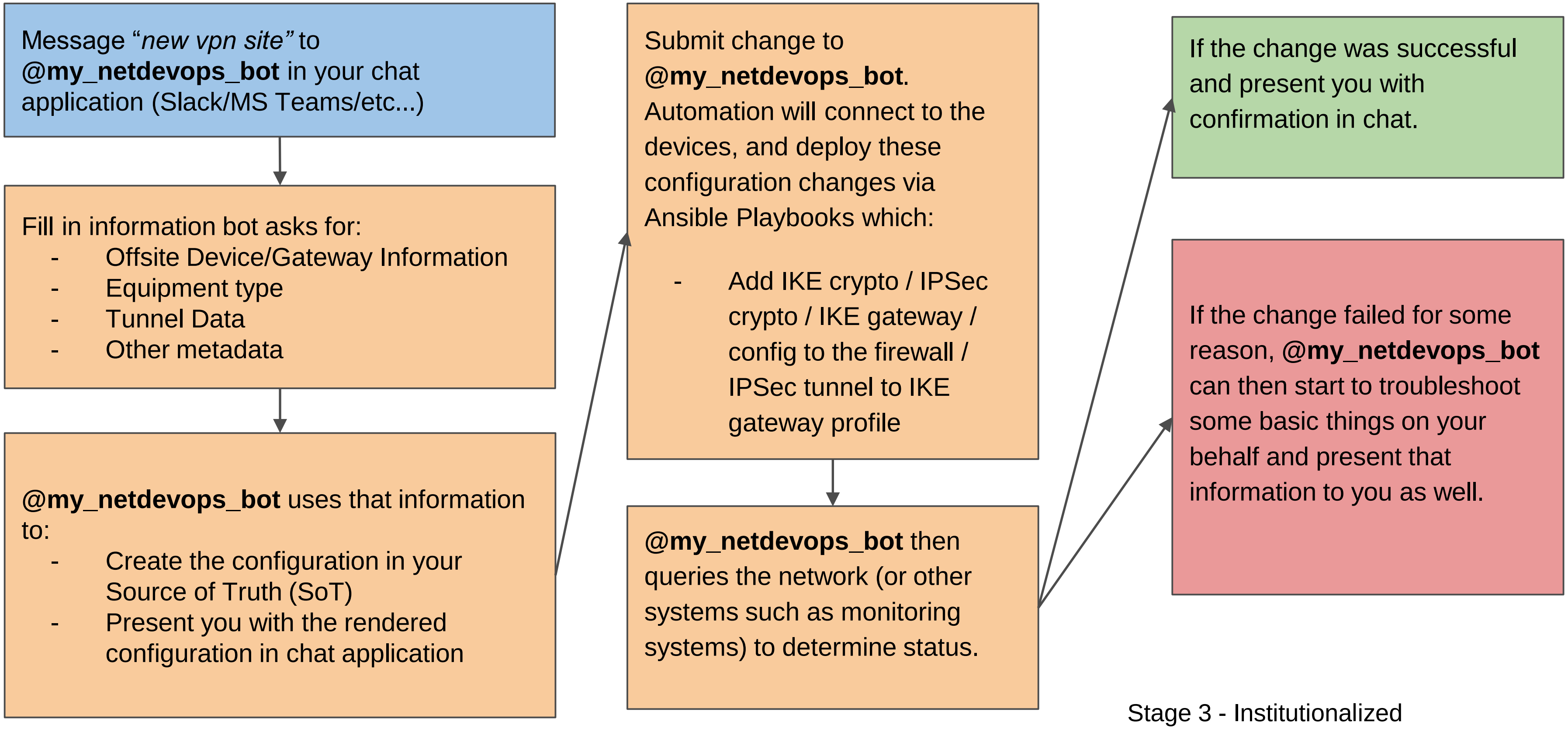
Upon provisioning of server created kick off Ansible playbooks to:

- Create VM from template
- Disable root and use sudo
- Disable password based SSH auth
- Explicitly allow or deny ssh per user(s)
- Use non-standard port for ssh from 22 to something like 2849
  - restart ssh

Report back to Servicenow with results.

Stage 2 – Systematic – end to end governance

Create A New Site to Site VPN via ChatOps



Message “*new vpn site*” to **@my_netdevops_bot** in your chat application (Slack/MS Teams/etc...)

Fill in information bot asks for:

- Offsite Device/Gateway Information
- Equipment type
- Tunnel Data
- Other metadata

@my_netdevops_bot uses that information to:

- Create the configuration in your Source of Truth (SoT)
- Present you with the rendered configuration in chat application

Submit change to **@my_netdevops_bot**. Automation will connect to the devices, and deploy these configuration changes via Ansible Playbooks which:

- Add IKE crypto / IPSec crypto / IKE gateway / config to the firewall / IPSec tunnel to IKE gateway profile

@my_netdevops_bot then queries the network (or other systems such as monitoring systems) to determine status.

If the change was successful and present you with confirmation in chat.

If the change failed for some reason, **@my_netdevops_bot** can then start to troubleshoot some basic things on your behalf and present that information to you as well.

Stage 3 - Institutionalized

AUTOMATION FOR EVERYONE: **SECURITY OPERATIONS**

```
---
- name: Create access rule in Checkpoint
  hosts: checkpoint
  connection: httpapi

  tasks:
    - name: create access rule
      checkpoint_access_rule:
          layer: Network
          name: "Drop attacker"
          position: top
          source: attacker
          destination: Any
          action: Drop
```

AUTOMATION FOR EVERYONE: **SECURITY OPERATIONS**

```
---
- name: Change QRadar rule state
  hosts: qradar

  tasks:
    - name: get info about qradar rule
      qradar_rule_info:
        name: "Potential DDoS Against Single Host (TCP)"
      register: rule_info

    - name: disable rule by id
      qradar_rule:
        state: disabled
        id: "{{ rule_info.rules[0]['id'] }}"
```

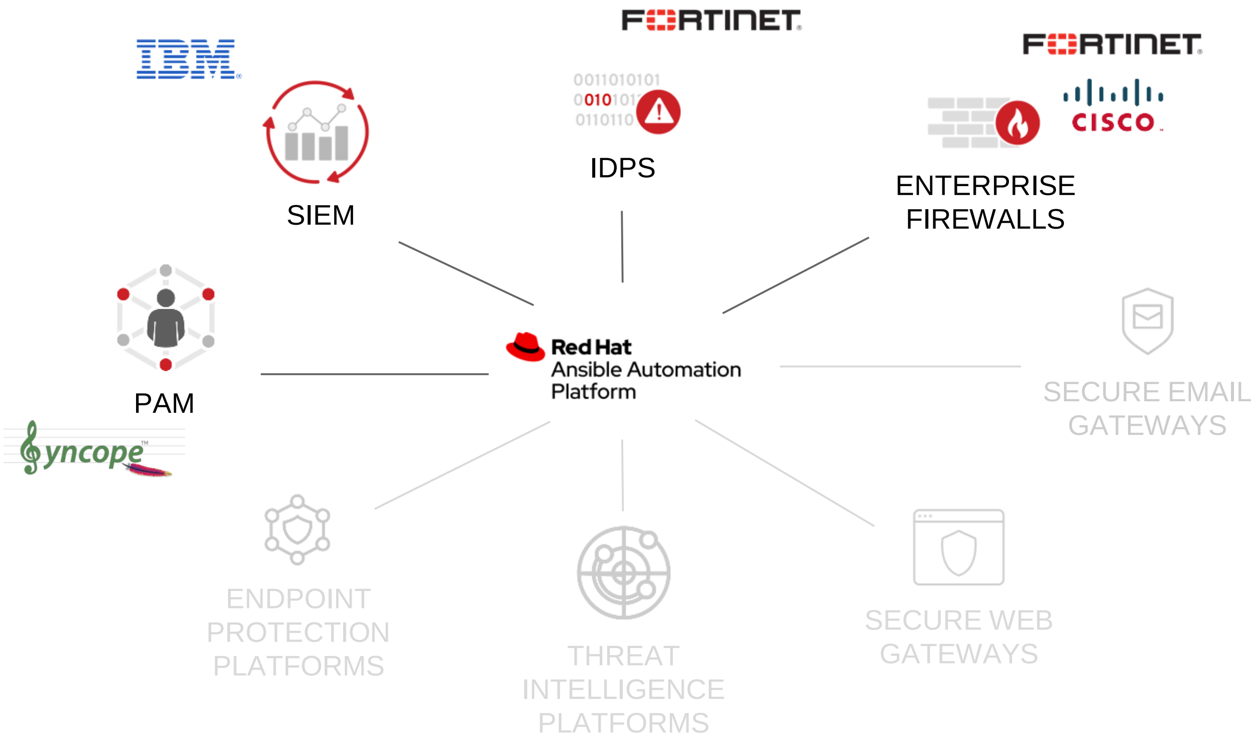
AUTOMATION FOR EVERYONE: **SECURITY OPERATIONS**

```yaml
---
- name: Add Snort rule
  hosts: snort

  tasks:
    - name: Add snort password attack rule
      include_role:
        name: "ansible_security.ids_rule"
      vars:
        rule: "alert tcp any 443 -> 192.168.12.0/24 any"
        state: present
        rules_file: /etc/snort/rules/grab_everything_http.rules
```

Customers Spotlight

Customer Spotlight

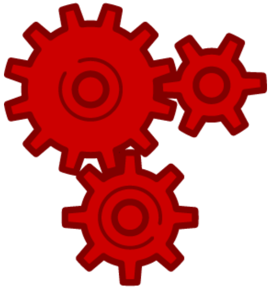


Public Sector serving it’s employees

Size: More than 190,000 users across 470+ locations, 15 datacenters.

Key Takeaways

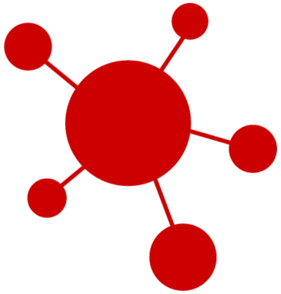
Ansible Automation Platform – Integrating well with Existing Automation Efforts



IT Operations

Add new security profiles to existing deployment use cases.

Extends compliance to contain security technologies.



Network Operations

Expand firewalls support.

Extend networking use cases with network security.

Team Cooperation

Make security consumable to others.

Integrate security procedures with operation and development workflows.

Next Steps

Get Started

Security automation on ansible.com

Ansible Security Automation in Mojo

Join the Community

Security automation community wiki

Blog posts

#ansible-security on irc.freenode.net

Join us at AnsibleFest

Join us at AnsibleFest 2020

Submit your talk to AnsibleFest 2020

Check out the Code

Ansible security on Ansible Galaxy

Check Point collections

Cisco ASA collection

Cyberark collections

F5 Networks collections

Fortinet collections

IBM Qradar collection

Splunk Enterprise Security collection

Tirasa Syncope collection

CONFIDENTIAL Designator

Thanks

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Mission Secure

Cybersecurity for Operational Technology & Control Systems

Threats, Strategy and Protections for Government Systems

The rise of Industry 4.0

The Industrial Internet of Things (IIoT) is ever-evolving. But with unprecedented connectedness comes new and unpredictable vulnerability.

To meet these risks head-on, we need a cybersecurity solution that delivers real visibility across the digital and physical components of the most important assets.

89%

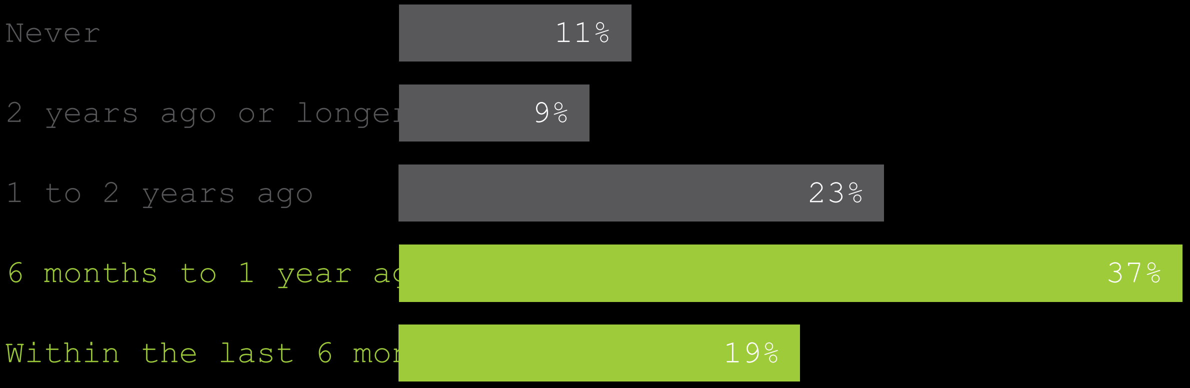
of industrial companies have experienced a cybersecurity breach in their control systems.

Source: Forrester Consulting on behalf of Fortinet, January 2018

Chances are, you've been attacked

In the last year alone, 56% of organizations have experienced a security breach in their industrial control systems. The result? Physical damage, lost productivity, safety risks and even ransom. And that number is only going up.

When have you experienced a security breach?



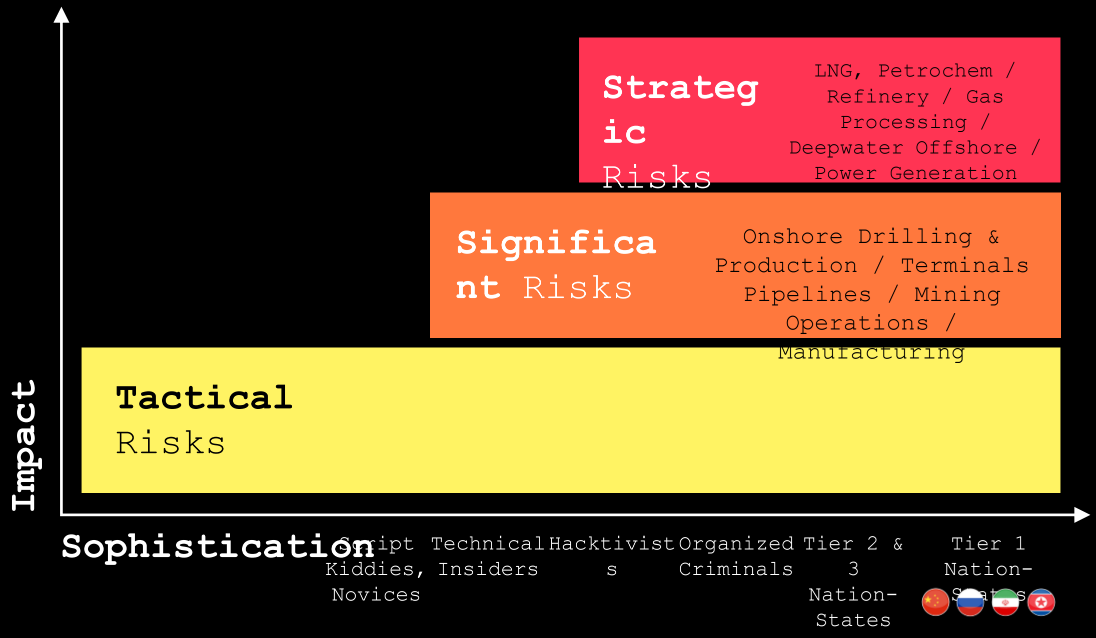
56% experienced a breach within the past year.

Base: 429 global decision makers responsible for security of critical infrastructure. Source: Forrester Consulting on behalf of

Business risks for operation technology systems

The complexities of assets like Traffic, Water or Power systems or even just public buildings make them especially vulnerable to high-impact attacks.

- Catastrophic explosions
- Danger to health and safety
- Extended shutdowns
- Multiple well kills
- Stolen well data
- Compressor damage
- Environmental impacts
- Loss of economic reputation
- Financial loss



Strategic Risks

LNG, Petrochem / Refinery / Gas Processing / Deepwater Offshore / Power Generation

Significant Risks

Onshore Drilling & Production / Terminals Pipelines / Mining Operations / Manufacturing

Tactical Risks

The Serious Impact of OT Cyber Threats

Attackers aim to control HMI and Level 1 devices to take over the process.

Incidences

Malware

Stuxnet
BlackEnergy 1, 2, 3
Havex
Industroyer
Triton
Shamoon 1&2
WannaCry, NotPetya

Events

Aurora
German Steel Plant
Ukraine 2015 & 2016
Dragonfly 1, 2

Attack Sequence

Identify one entry point (e.g., spear phishing)

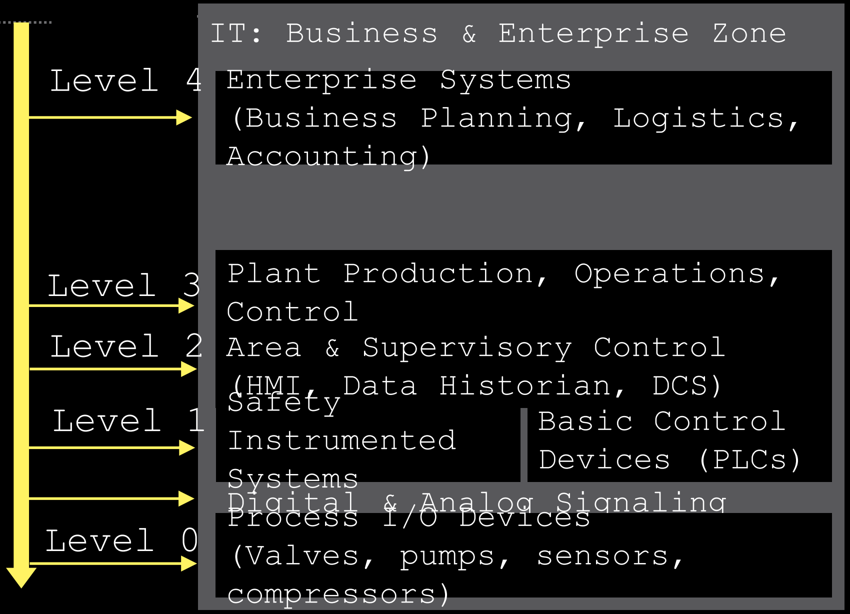
Enter OT

Mask the actual state of the attack (physical system)

Take control of CS and safety response systems

Create impact

Purdue Control System Model



IT: Business & Enterprise Zone

Level 4 Enterprise Systems (Business Planning, Logistics, Accounting)

Level 3 Plant Production, Operations, Control

Level 2 Area & Supervisory Control (HMI, Data Historian, DCS)

Level 1 Safety Instrumented Systems | Basic Control Devices (PLCs)

Digital & Analog Signaling

Level 0 Process I/O Devices (Valves, pumps, sensors, compressors)

Impacts can be felt at all levels

Level 2 – HMIs, Operators & ATMS

- Loss of view
- False view
- Loss of control

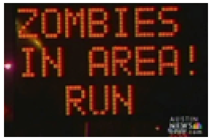
Operator at the Human Machine Interface (HMI) or ATMS

Level 1 – Controller, PLC & ATC

- Instruct devices, change processes or cause damage
- Send "normal" signals across network to HMI
- Steal sensitive data or report false data

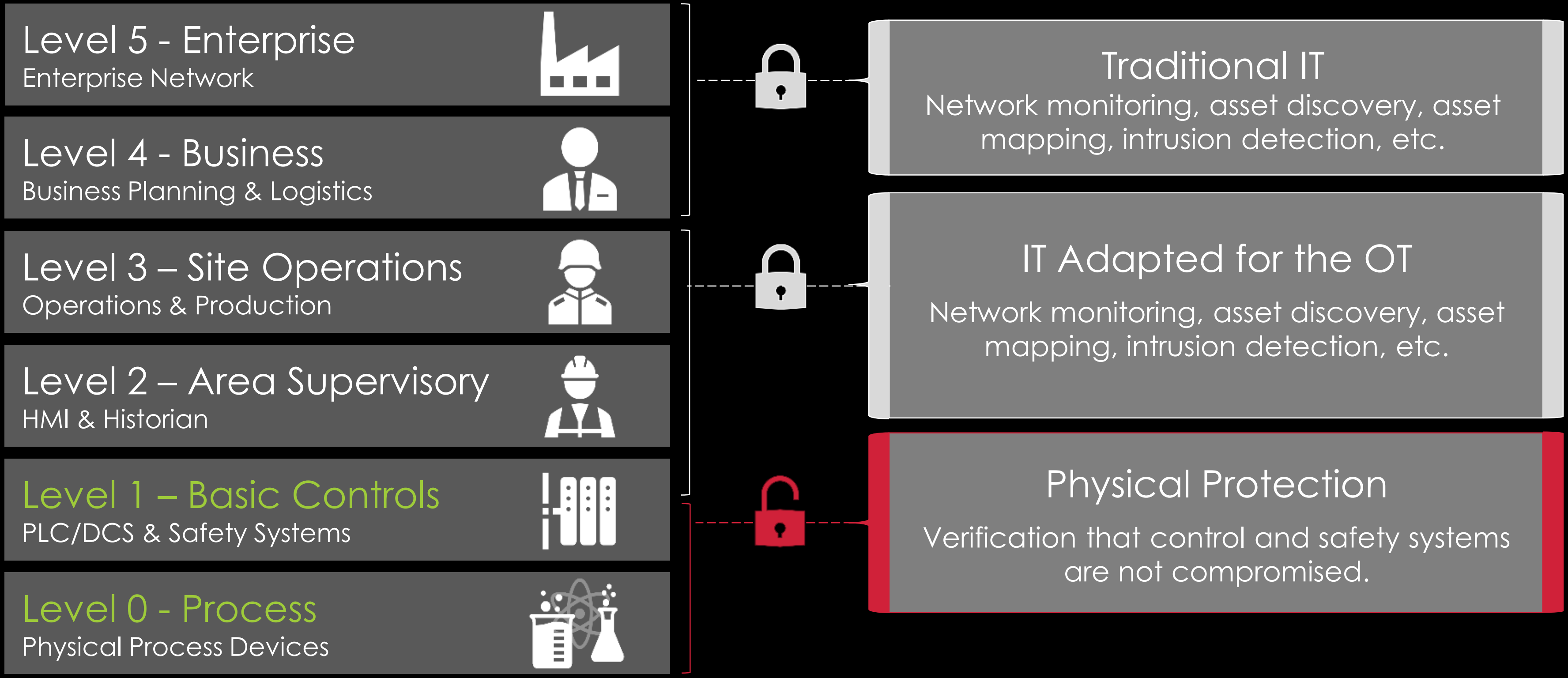
Level 0 – Field Device, Process

- Remotely configurable sensor
- Get between sensor and ATC
- Sending false data to/from ATC or CV/AV



Successful attacks impact public safety in traffic systems

How are you protecting your critical assets?



Level 5 - Enterprise
Enterprise Network

Level 4 - Business
Business Planning & Logistics

Level 3 – Site Operations
Operations & Production

Level 2 – Area Supervisory
HMI & Historian

Level 1 – Basic Controls
PLC/DCS & Safety Systems

Level 0 - Process
Physical Process Devices

Traditional IT
Network monitoring, asset discovery, asset mapping, intrusion detection, etc.

IT Adapted for the OT
Network monitoring, asset discovery, asset mapping, intrusion detection, etc.

Physical Protection
Verification that control and safety systems are not compromised.

Secure IT design & protection for the OT network

Design a cybersecurity architecture, including immediate risk mitigation, a roadmap and actionable plan with budgetary estimates.

People

Cyber Awareness &
Workforce Training
Training Assessment
Incident Response
Cybersecurity Audit

Process

Policies & Procedures
Cyber Incident
Response
Cyber Notations
Third-party Management
Insurance Premium
Reductions

Technology

OT Network
Segmentation
Network Visibility
Anomaly Detection
Protection for Level 2
down to Level 0 field
devices

Visibility Only – Common Cybersecurity for control systems

Monitor
Continuously monitor network IP levels, alongside digital and analog signals with our secure, multi-layered system.

Detect
Get real-time analysis and automated incident detection.

Restrict unauthorized access and block abnormal or malicious activity from reaching important controllers and Level 1 devices.

Inform
Keep trusted operators and cybersecurity professionals informed through dedicated communications systems.

Collect
Gather system data from digital and analog sensors and actuators, controllers, and OT network for forensic purposes

Carry out automated or operator-guided responses, mission restorations, and system functions to safe operating states

The patented MSi Platform is the only cybersecurity solution that provides operational visibility and protection, down to Level 0 devices.

*The Mission Secure Platform is a patented product of Mission Secure, Inc. covered by U.S. Patent Numbers 9697355, 9942262, 10205733 and 10250619.

Protection + Correction | Cybersecurity for control systems

Monitor

Continuously monitor network IP levels, alongside digital and analog signals with our secure, multi-layered system.

Detect

Get real-time analysis and automated incident detection.

Protect

Restrict unauthorized access and block abnormal or malicious activity from reaching important controllers and Level 1 devices.

Inform

Keep trusted operators and cybersecurity professionals informed through dedicated communications systems.

Collect

Gather system data from digital and analog sensors and actuators, controllers, and OT network for forensic purposes.

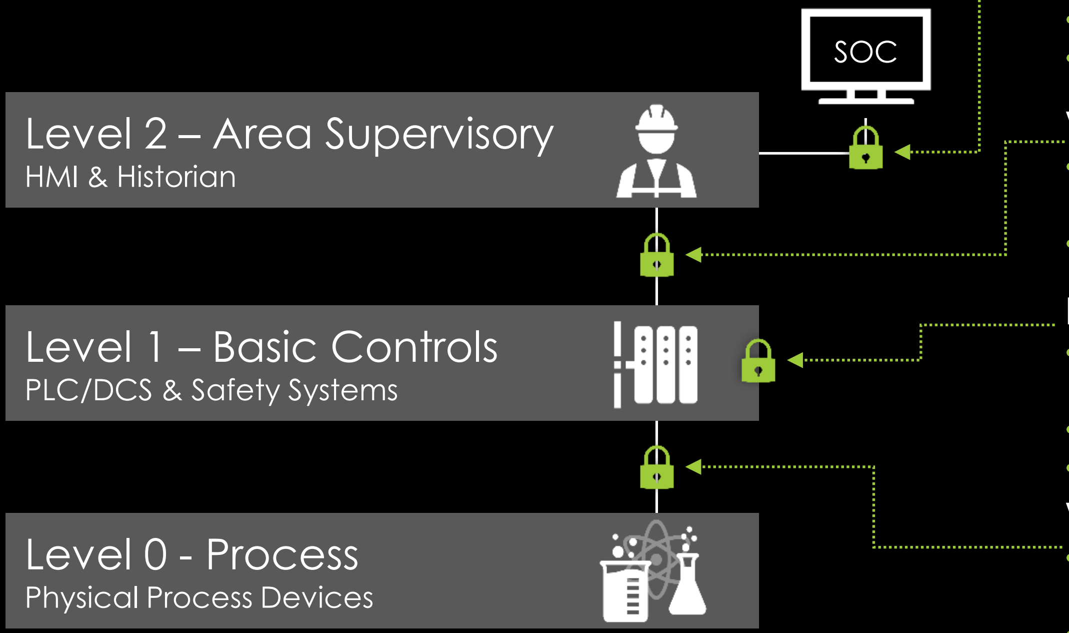
Correct

Carry out automated or operator-guided responses, mission restorations, and system functions to safe operating states.

The patented Mission Secure Platform is the only cybersecurity solution that provides operational visibility and protection, down to Level 0 devices.

*The Mission Secure Platform is a patented product of Mission Secure, Inc. covered by U.S. Patent Numbers 9697355, 9942262, 10205733 and 10250619.

Visibility and protection into the OT network



Central Management

- Visualize data and investigate incidents
- Manage rules and actions

Visibility

- Passively monitor OT traffic; detect abnormal OT network activities
- No impact to operations

Protection

- Protect PLCs, safety systems, building management systems, controllers
- White list, block or restrict access; encrypt
- Monitor settings of protected devices

Validation and Correction

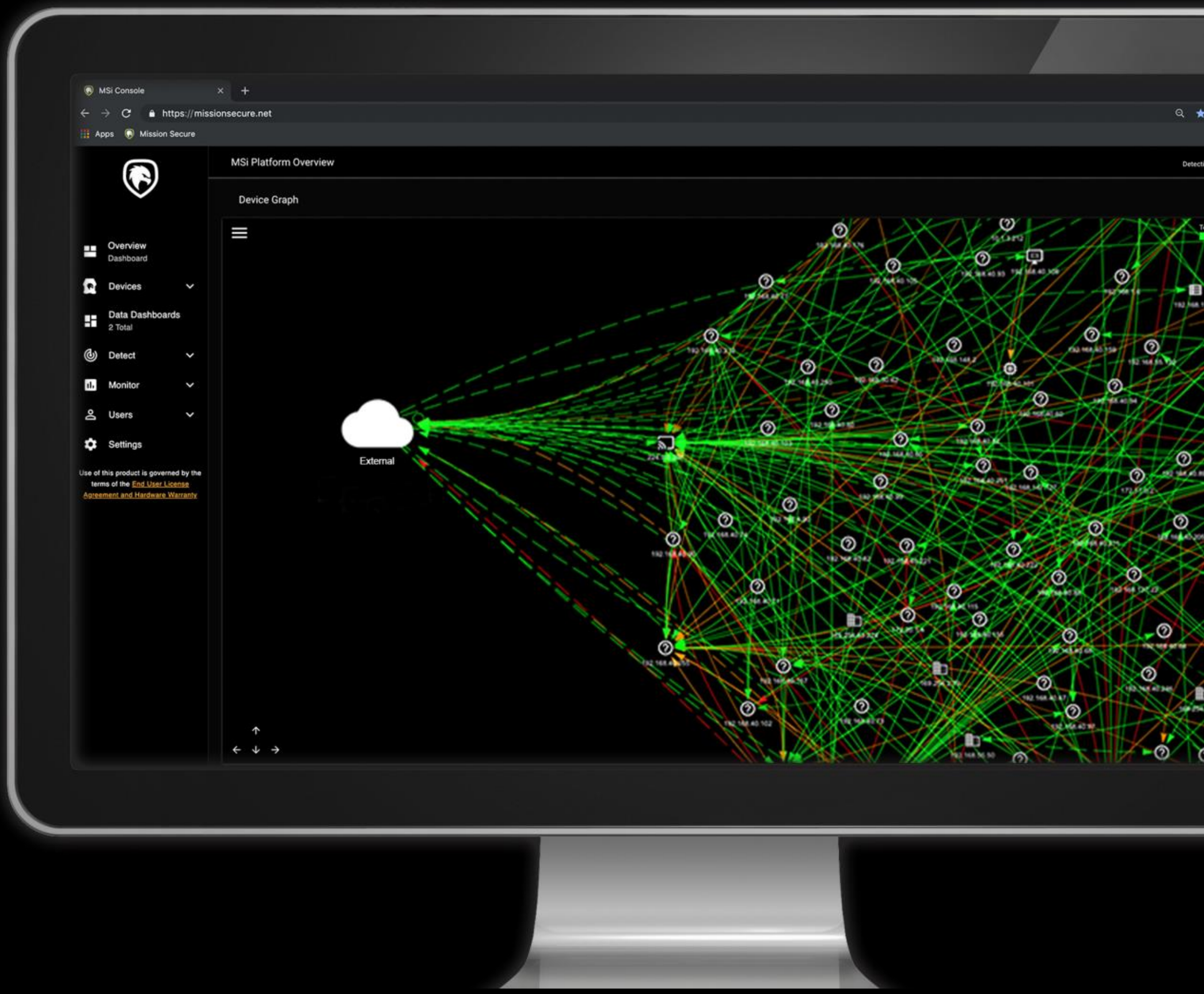
- Validate operational processes at digital and analog signals, controller and HMIs
- Horizontal and vertical analysis
- Monitor passively or in-line for corrective action

Monitor, Detect, Inform, Protect and Collect

Level 2

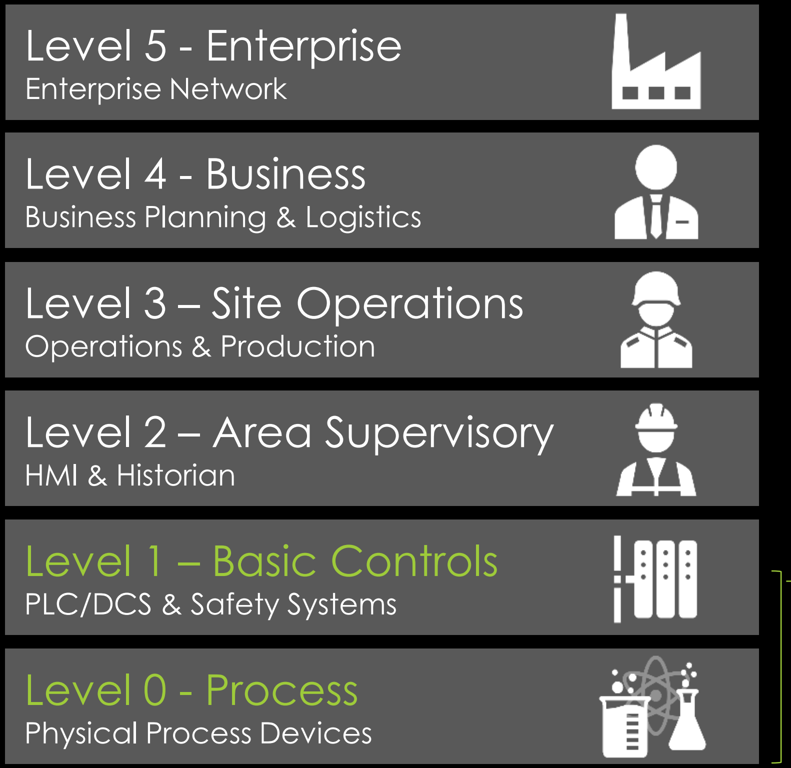
MSi Console

For Central Management



Use of this product is governed by the terms of the End User License Agreement and Hardware Warranty

Securing assets down to Level 0 & 1



Level 5 - Enterprise
Enterprise Network

Level 4 - Business
Business Planning & Logistics

Level 3 – Site Operations
Operations & Production

Level 2 – Area Supervisory
HMI & Historian

Level 1 – Basic Controls
PLC/DCS & Safety Systems

Level 0 - Process
Physical Process Devices

How low should you go?

- Identify an ongoing cyber attack
- Maintain operability during an attack
- Stop operations safely if required
- Recover & restore operations post-attack
- Analyze the attack & mitigate recurrence

These three elements begin and end with the Level 0 & 1 field devices controlling physical processes.

Level 2

MSi IDS

For Visibility

Level 1

MSi 1

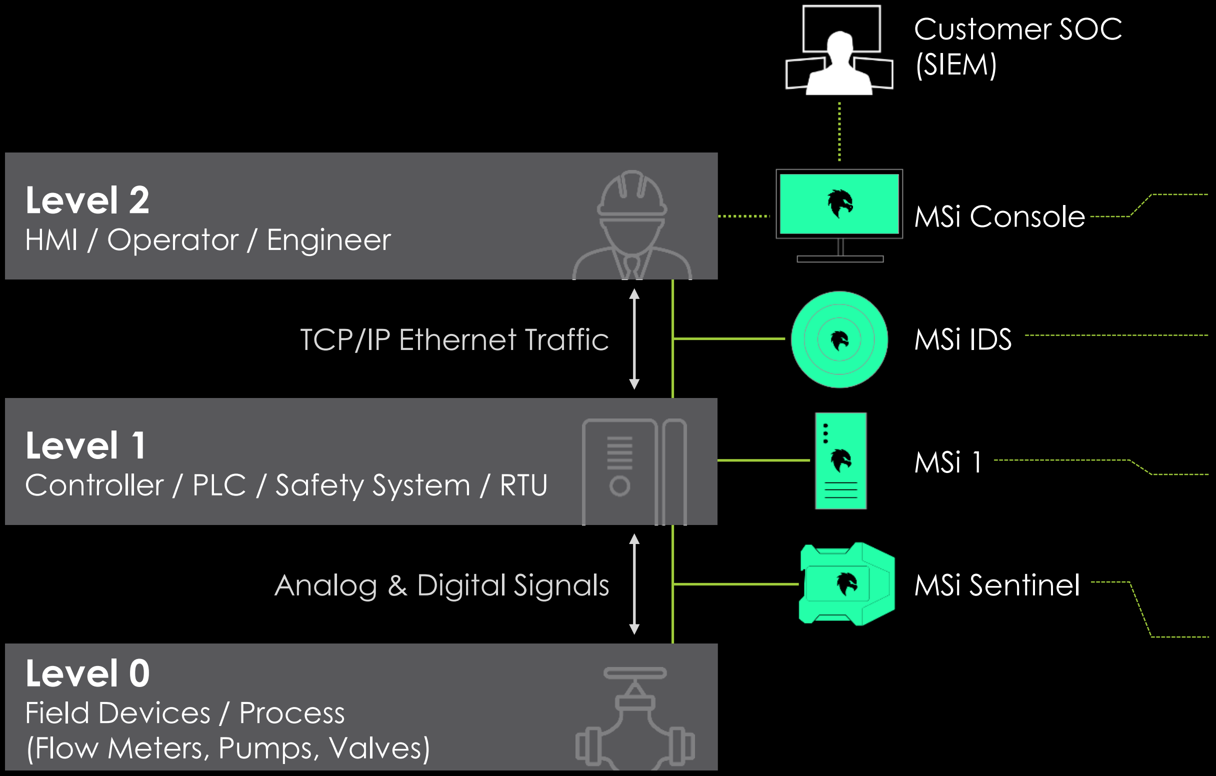
For Protection
& Correction

Level 0

MSi Sentinel

For Sensing
& Correcting

The Mission Secure Platform



Customer SOC (SIEM)

Level 2
HMI / Operator / Engineer

MSi Console

TCP/IP Ethernet Traffic

MSi IDS

Level 1
Controller / PLC / Safety System / RTU

MSi 1

Analog & Digital Signals

MSi Sentinel

Level 0
Field Devices / Process
(Flow Meters, Pumps, Valves)

Central Management

- Visualize data and manage MSi security devices
- Investigate incidents
- Manage rules and actions

Visibility

- Monitor OT traffic
- Detect abnormal OT network activities
- Ensure Zero impact to operations

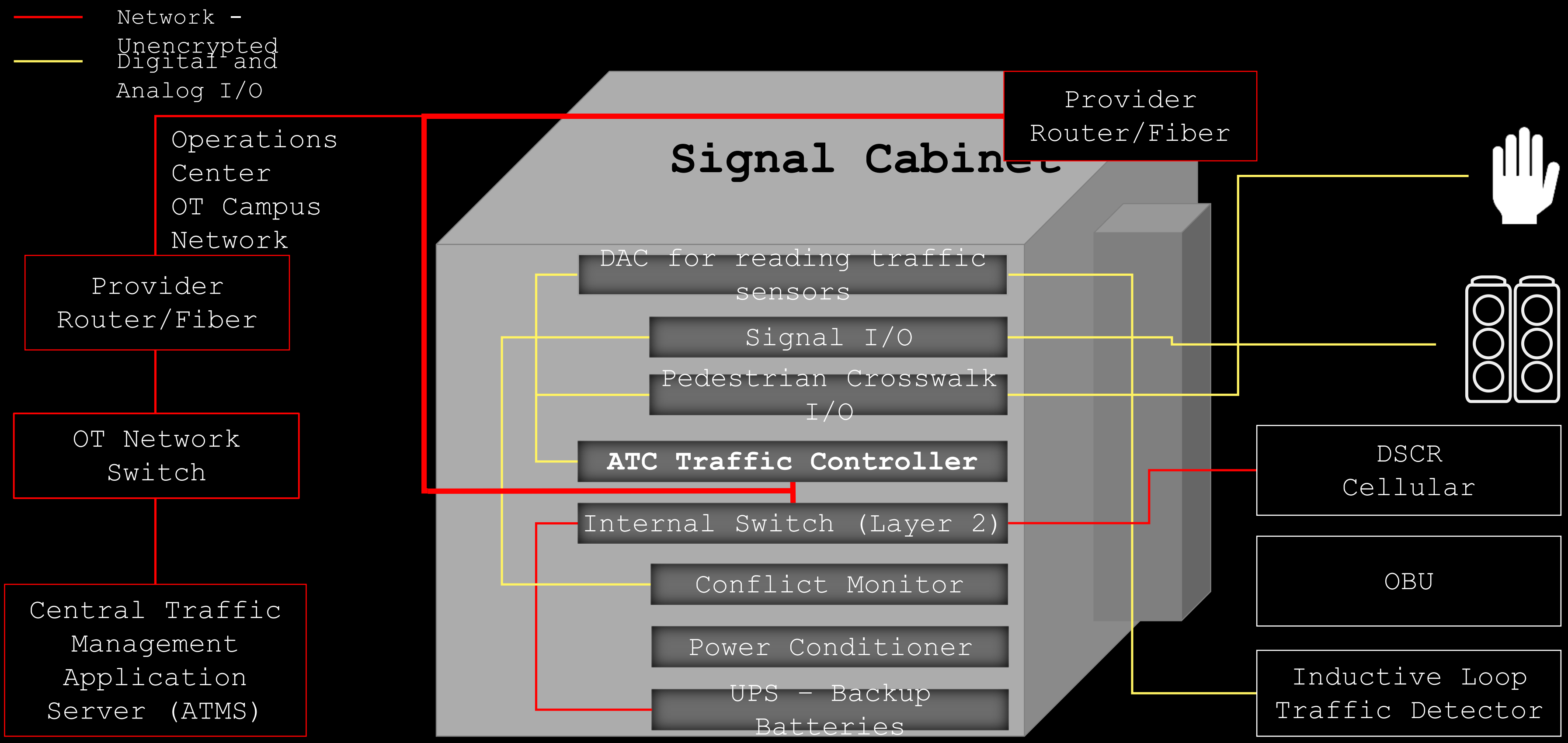
Protection

- Protect PLCs, safety and building management systems, controllers
- White list, block, restrict access, encrypt
- Monitor settings of protected devices

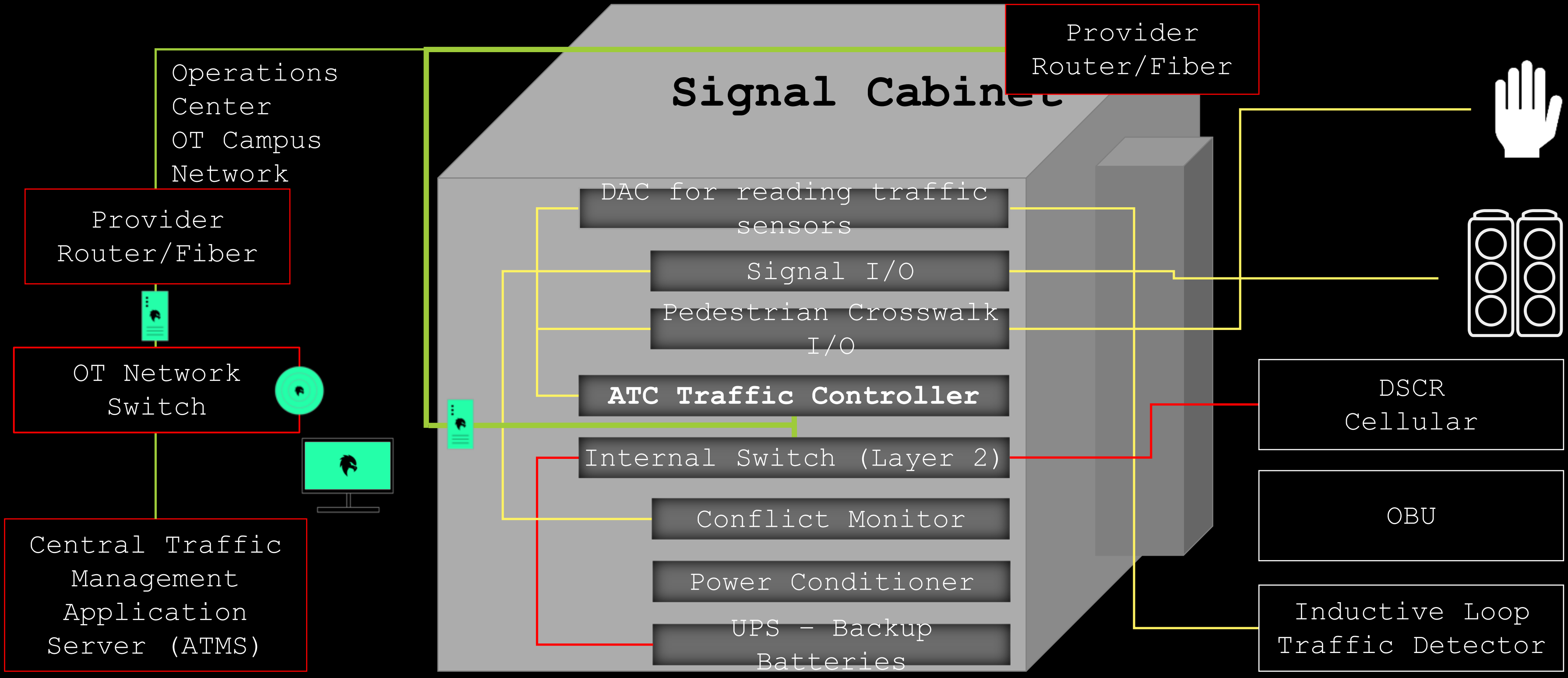
Sensing and Correction

- Validate operational processes at digital and analog
  signals, controllers, and HMI
- Get horizontal and vertical analyses
- Monitor passively, or In-line to take corrective action

Cyber Threats: A Vulnerable Traffic System



Cyber Threats: A Protected Traffic System



Industrial cybersecurity for industrial environments

Military Strength

✓ Lockheed Martin Pen Testing

✓ Millennium Corporation Pen Test

✓ Arizona Cyber Warfare Range - **Pen tested** & **endorsed** – by the Arizona Cyber Warfare Range for both the functional and component robustness of the platform's ICS protections

✓ U.S. Department of Defense Information Systems Agency (DISA)

- Applied DISA Security Technical Implementation Guide (STIG)
- Implemented detailed security features

✓ Industry Testing by a Fortune 10 Supermajor

- Integrated lab, red team and production tests and internal audits

Industrial Design

Withstand industrial temperature extremes

- Industrial computer boards designed to withstand temperatures from -20°C to +80°C

Extended failure rating

- Mean time to failure rated at 13+ years, with mechanical failover and conformal coating

Built for Control System & OT Networks

- Supports multiple OT protocols, digital and analog signals and ethernet and serial connections
- Inline failsafe design – in protect mode the security appliance automatically fails to wire and recovers on power outage or device failure

Battle-tested against the harshest environments to provide industrial devices Level 0-2 protection, anywhere in the world.

Securing control systems. Protecting operations.

Maintain control & operability Level 0 physical devices to Level 2 workstations.

Improve safety & reliability with a validated purpose-built solution.

Minimize risks—hackers, insiders or errors—with superior visibility & protection for OT networks in a single, easy-to-use platform.

Facilitate compliance with regulatory bodies, industry standards and best practices, avoiding costly penalties or fines.

Navigate an evolving threat landscape clearly with an economical & scalable platform built for, tested and deployed in harsh, industrial environments.

Protect operations, people & infrastructure with the next-generation of cybersecurity for control systems and OT networks.

SOC and Monitoring Services Approach

Mission Secure Services

Working with you every step of the way

Managed Services

24/7

Expert team with 2 threat management centers

Named managed services security engineer

Managed visibility – real-time asset, traffic, and threat monitoring

Managed protection – baselining, analysis, configs, and tuning

On-going OT network analysis and reporting

Threat detection / hunting, and incident response support

Incident Response (IR) Support

- Standalone IR support available as needed
- Sold in blocks of time/hours
- 3 named incident response support team members
- Support via phone, email and onsite it necessary

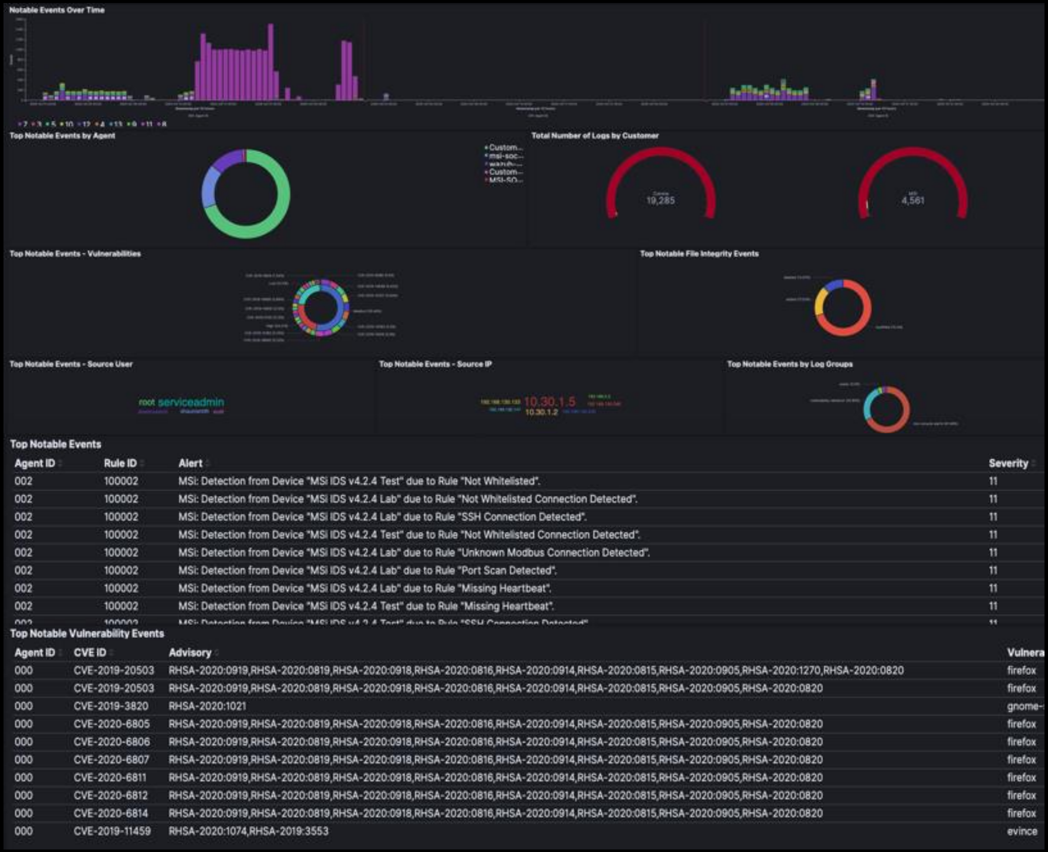
Customer Success Service (90-day)

- Named security engineer, remote site survey & design, installation support, assistance, training

Gold Maintenance and Support Service

Platinum Maintenance and Support Service

MSi Dashboard


Notable Events Over Time
7 3 5 10 12 4 13 9 11 8
Top Notable Events by Agent
Custom...
msi-soc...
wazuh-...
Custom...
MSI-SO...
Total Number of Logs by Customer
19,285
4,561
Top Notable Events - Vulnerabilities
Top Notable File Integrity Events
Top Notable Events - Source User
root serviceadmin
Top Notable Events - Source IP
10.30.1.5
10.30.1.2
Top Notable Events by Log Groups

Top Notable Events

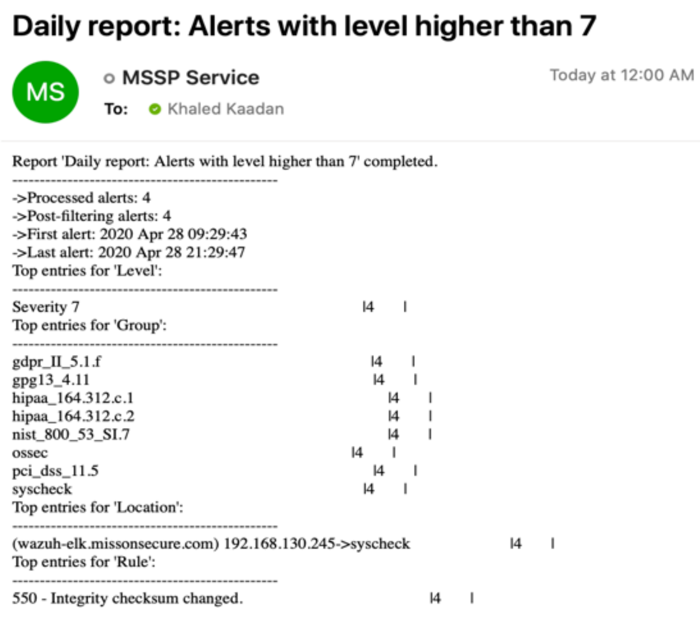
Agent ID	Rule ID	Alert	Severity
002	100002	MSi: Detection from Device "MSi IDS v4.2.4 Test" due to Rule "Not Whitelisted".	11
002	100002	MSi: Detection from Device "MSi IDS v4.2.4 Lab" due to Rule "Not Whitelisted Connection Detected".	11
002	100002	MSi: Detection from Device "MSi IDS v4.2.4 Lab" due to Rule "SSH Connection Detected".	11
002	100002	MSi: Detection from Device "MSi IDS v4.2.4 Test" due to Rule "Not Whitelisted Connection Detected".	11
002	100002	MSi: Detection from Device "MSi IDS v4.2.4 Lab" due to Rule "Unknown Modbus Connection Detected".	11
002	100002	MSi: Detection from Device "MSi IDS v4.2.4 Lab" due to Rule "Port Scan Detected".	11
002	100002	MSi: Detection from Device "MSi IDS v4.2.4 Lab" due to Rule "Missing Heartbeat".	11
002	100002	MSi: Detection from Device "MSi IDS v4.2.4 Test" due to Rule "Missing Heartbeat".	11
002	100002	MSi: Detection from Device "MSi IDS v4.2.4 Test" due to Rule "SSH Connection Detected".	11

Top Notable Vulnerability Events

Agent ID	CVE ID	Advisory	Vulnera
000	CVE-2019-20503	RHSA-2020:0919,RHSA-2020:0819,RHSA-2020:0918,RHSA-2020:0816,RHSA-2020:0914,RHSA-2020:0815,RHSA-2020:0905,RHSA-2020:1270,RHSA-2020:0820	firefox
000	CVE-2019-20503	RHSA-2020:0919,RHSA-2020:0819,RHSA-2020:0918,RHSA-2020:0816,RHSA-2020:0914,RHSA-2020:0815,RHSA-2020:0905,RHSA-2020:0820	firefox
000	CVE-2019-3820	RHSA-2020:1021	gnome-
000	CVE-2020-6805	RHSA-2020:0919,RHSA-2020:0819,RHSA-2020:0918,RHSA-2020:0816,RHSA-2020:0914,RHSA-2020:0815,RHSA-2020:0905,RHSA-2020:0820	firefox
000	CVE-2020-6806	RHSA-2020:0919,RHSA-2020:0819,RHSA-2020:0918,RHSA-2020:0816,RHSA-2020:0914,RHSA-2020:0815,RHSA-2020:0905,RHSA-2020:0820	firefox
000	CVE-2020-6807	RHSA-2020:0919,RHSA-2020:0819,RHSA-2020:0918,RHSA-2020:0816,RHSA-2020:0914,RHSA-2020:0815,RHSA-2020:0905,RHSA-2020:0820	firefox
000	CVE-2020-6811	RHSA-2020:0919,RHSA-2020:0819,RHSA-2020:0918,RHSA-2020:0816,RHSA-2020:0914,RHSA-2020:0815,RHSA-2020:0905,RHSA-2020:0820	firefox
000	CVE-2020-6812	RHSA-2020:0919,RHSA-2020:0819,RHSA-2020:0918,RHSA-2020:0816,RHSA-2020:0914,RHSA-2020:0815,RHSA-2020:0905,RHSA-2020:0820	firefox
000	CVE-2020-6814	RHSA-2020:0919,RHSA-2020:0819,RHSA-2020:0918,RHSA-2020:0816,RHSA-2020:0914,RHSA-2020:0815,RHSA-2020:0905,RHSA-2020:0820	firefox
000	CVE-2019-11459	RHSA-2020:1074,RHSA-2019:3553	evince

Alerting

Email alerts



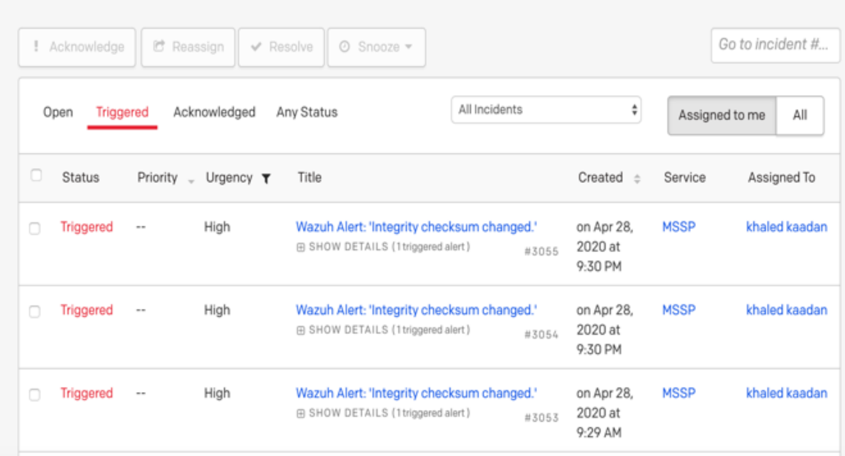
Daily report: Alerts with level higher than 7

MS ○ MSSP Service — Today at 12:00 AM

To: Khaled Kaadan

```
Report 'Daily report: Alerts with level higher than 7' completed.
------------------------------------------------
->Processed alerts: 4
->Post-filtering alerts: 4
->First alert: 2020 Apr 28 09:29:43
->Last alert: 2020 Apr 28 21:29:47
Top entries for 'Level':
------------------------------------------------
Severity 7                                    |4    |
Top entries for 'Group':
------------------------------------------------
gdpr_II_5.1.f                                 |4    |
gpg13_4.11                                    |4    |
hipaa_164.312.c.1                               |4    |
hipaa_164.312.c.2                               |4    |
nist_800_53_SI.7                                |4    |
ossec                                       |4    |
pci_dss_11.5                                  |4    |
syscheck                                     |4    |
Top entries for 'Location':
------------------------------------------------
(wazuh-elk.missonsecure.com) 192.168.130.245->syscheck         |4    |
Top entries for 'Rule':
------------------------------------------------
550 - Integrity checksum changed.                      |4    |
```

PagerDuty alerts

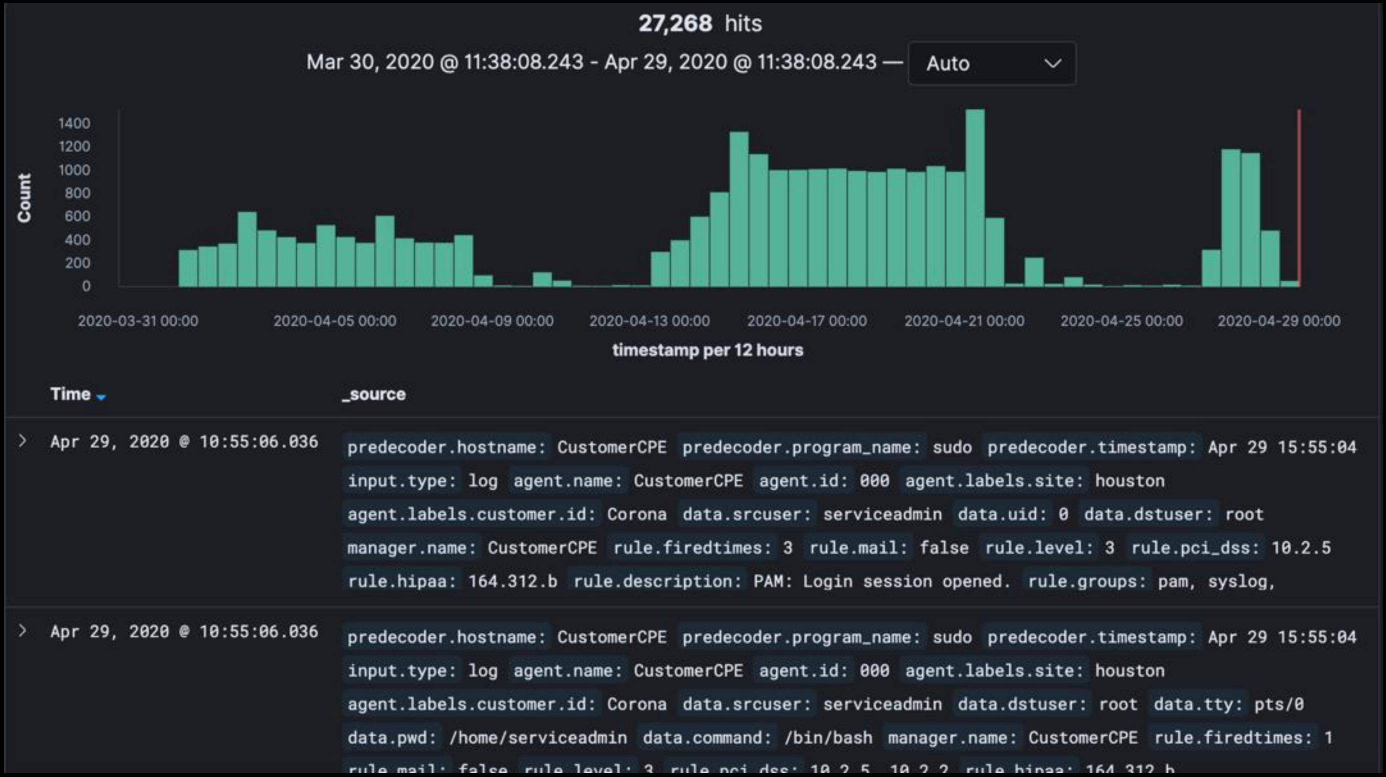


□	Status	Priority	Urgency	Title	Created	Service	Assigned To
□	Triggered	--	High	Wazuh Alert: 'Integrity checksum changed.' ⊞ SHOW DETAILS (1 triggered alert) #3055	on Apr 28, 2020 at 9:30 PM	MSSP	khaled kaadan
□	Triggered	--	High	Wazuh Alert: 'Integrity checksum changed.' ⊞ SHOW DETAILS (1 triggered alert) #3054	on Apr 28, 2020 at 9:30 PM	MSSP	khaled kaadan
□	Triggered	--	High	Wazuh Alert: 'Integrity checksum changed.' ⊞ SHOW DETAILS (1 triggered alert) #3053	on Apr 28, 2020 at 9:29 AM	MSSP	khaled kaadan

When alerts are generated analysts will receive an Email notification as well as a PagerDuty alert.

Log Analysis

- Analysts will be able to search logs to analyze.
- Logs are saved in Raw and JSON formats.



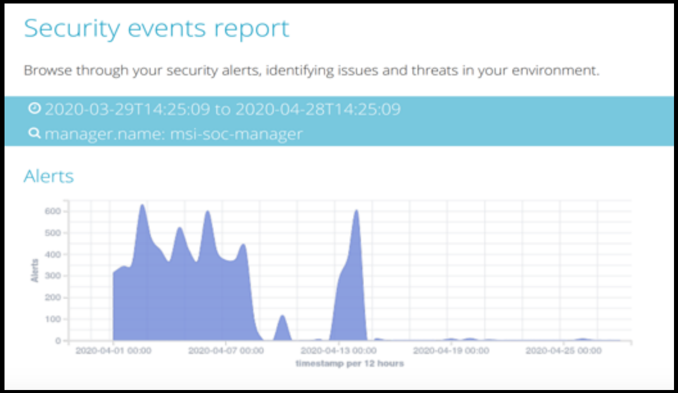
27,268 hits

Mar 30, 2020 @ 11:38:08.243 - Apr 29, 2020 @ 11:38:08.243 — Auto

```
Time                        _source
> Apr 29, 2020 @ 10:55:06.036   predecoder.hostname: CustomerCPE predecoder.program_name: sudo predecoder.timestamp: Apr 29 15:55:04
                                input.type: log agent.name: CustomerCPE agent.id: 000 agent.labels.site: houston
                                agent.labels.customer.id: Corona data.srcuser: serviceadmin data.uid: 0 data.dstuser: root
                                manager.name: CustomerCPE rule.firedtimes: 3 rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5
                                rule.hipaa: 164.312.b rule.description: PAM: Login session opened. rule.groups: pam, syslog,
> Apr 29, 2020 @ 10:55:06.036   predecoder.hostname: CustomerCPE predecoder.program_name: sudo predecoder.timestamp: Apr 29 15:55:04
                                input.type: log agent.name: CustomerCPE agent.id: 000 agent.labels.site: houston
                                agent.labels.customer.id: Corona data.srcuser: serviceadmin data.dstuser: root data.tty: pts/0
                                data.pwd: /home/serviceadmin data.command: /bin/bash manager.name: CustomerCPE rule.firedtimes: 1
                                rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5, 10.2.2 rule.hipaa: 164.312.b
```

Reporting

- Reports will be generated and emailed to analyst per defined schedule
- All reports are customizable to include any Notable Event

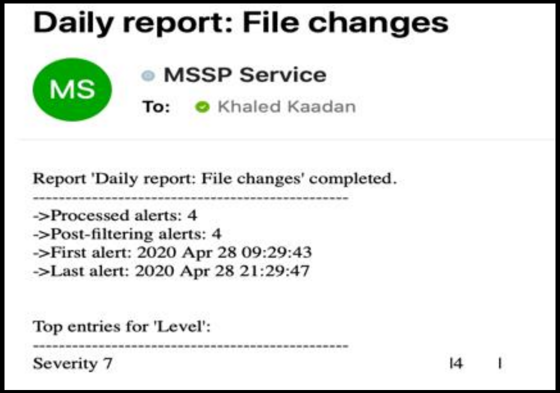


Security events report

Browse through your security alerts, identifying issues and threats in your environment.

2020-03-29T14:25:09 to 2020-04-28T14:25:09
manager.name: msi-soc-manager

Alerts



Daily report: File changes

MS

MSSP Service
To: Khaled Kaadan

```
Report 'Daily report: File changes' completed.
--------------------------------------------------
->Processed alerts: 4
->Post-filtering alerts: 4
->First alert: 2020 Apr 28 09:29:43
->Last alert: 2020 Apr 28 21:29:47

Top entries for 'Level':
--------------------------------------------------
Severity 7                                    |4   |
```

Contact information

Mission Secure

Built by control system, IT & cyber experts.
Protecting OT & IT worlds—together.

cybersecurity for industrial control systems

Rick Tiene

VP Smart Cities, Government and Critical Infrastructure

rtiene@missionsecure.com

m. +1.703.618.9100

www.missionsecure.com

MSI Tabletop Exercise 2020

Stephone P. Dixon
SAIC MSI Security Incident Response Lead

SAIC®
Redefining Ingenuity

Agenda

- Overview
- Objectives
- Expected Outcomes

AGAINST CYBER THREATS
NATIONAL
CYBER SECURITY
AWARENESS
MONTH
PROTECT ALL INFORMATION AGAINST ATTACKS
PROTECT ALL INFORMATION AGAINST ATTACKS

Overview

The MSI Annual Tabletop Exercise is an unclassified, adaptable exercise developed by the MSI for the Platform, and the Commonwealth of Virginia. The main purpose is to evaluate performance of the multisupplier model, promote dialogue around opportunities for continuous improvement, and identify recommendations for improvement.

Objectives

- The Main Objective for this Tabletop is to uncover Strengths within SAIC Multisourcing Services:
  - Evaluate the Service Delivery capability for detecting, responding to, and recovering from simulated, realistic events
  - Evaluate Service Delivery communication and responsiveness
  - Run the event through the Service Delivery and State Agency Incident Response plans, identify opportunities for alignment, and any gaps in Service Delivery execution
  - Provide recommendations for corrective action to VITA-CSRM

Expected Outcomes

- Expected outcome from this event is to conduct a Tabletop event where Coordination of multiple Suppliers and Service Delivery ensures COV information systems will successfully operate in support of the exercise scenario, and when the managed environment is under attack.

  - Demonstrate successful coordination of multiple Supplier Service Delivery
  - Ensure COV information systems will successfully operate in support of the exercise scenario
  - Enhance awareness, readiness and coordination
  - Test capability to determine operational impacts of a cyberattack
  - Test participant's exercise playbooks, incident analysis, incident response plans and procedures, and incident reporting
  - Demonstrate compliance with MSI Security Incident Management Process SMM 4.1.5.7 and VITA Playbooks
  - Identify Enterprise-wide opportunities for improvement
  - Further integration of multi sourcing program between MSI, VITA-CSRM, Service Towers, and the Agencies

Please direct all questions about the exercise to MSI-Security-Operations@saic.com

Security Awareness Training

Ed Miller
VITA
Director IT Security Governance

New Legislation

Added to 2.2-2009, Additional duties of the CIO related to security of government information (its subsection I)

- Applies to executive, legislative, judicial and independent agencies

- VITA shall develop and annually update a curriculum for training all state employees in security awareness and in proper procedures for detecting, assessing, reporting and addressing information security risks.

New Legislation

Added to 2.2-2009, Additional duties of the CIO related to security of government information (subsection I)

- The curriculum shall include activities, case studies, hypothetical situations and other methods of instruction:

- i) that focus on forming good security habits and procedures
- ii) teach best practices for detecting, assessing, reporting and addressing information security threats

New Legislation

Added to 2.2-2009, Additional duties of the CIO related to security of government information (subsection I)

- Effective Jan 1, 2021, every agency shall provide annual information security training for each employee using the curriculum developed by VITA.

- State agencies may develop additional materials that address specific needs of the agency, provided that such materials do not contradict the training curriculum developed by VITA.

New Legislation

- VITA shall coordinate and assist state agencies with implementing the annual training requirement.

- Each state agency shall:

  (i) monitor & certify the training activity of its employees
- (ii) evaluate the efficacy of the IT security training program
- (iii) forward to VITA its certification and evaluation, along with suggestions for improving the program.

VITA's Approach

- VITA has formed a committee with some members of the ISO Council to address this requirement.

- The committee includes not only includes council members but also other commonwealth employees. All branches of state government are included.

- The committee will help VITA develop a curriculum to address IT security awareness training.

- The committee will also help VITA identify several software solutions that will meet or exceed the training requirements established in the curriculum.

VITA’s Approach

- Funding provided to VITA for this initiative is currently uncertain. So the committee will focus on developing the curriculum and identifying software solutions that will be acceptable.

- In all likelihood, most established IT security training software solutions will meet most of the curriculum requirements. However, there may be some curriculum items that may not be adequately addressed. VITA will try to identify other solutions and sources that agencies can use whenever gaps are indicated.
- Example:
  - SEC501 requires Agency Head training with some unique commonwealth components. Most commercial training solutions may not meet this requirement. However, Agency Head training is a module that is available on the DHRM Learning Center.

VITA’s Approach

- If adequate funding becomes available, VITA will consider and would like to implement a fully functional IT security awareness software solution for all state employees in-scope to this training requirement.

- In the meantime, at least for this year, agencies should follow the curriculum that is developed using their existing training and ensuring that it lines up with the established curriculum. The full curriculum will be available by the fall of 2020.

- The legislation also includes a reporting requirement that an agency’s employees have taken all required annual training. VITA will track that agencies have reported this using Archer.

VITA Deliverables

- A Curriculum of IT security training requirements for all employees

- Identification of additional (HIPAA, IRS, etc) training or role-based training that may be required (system owner, administrators, etc)

- A matrix identifying software solutions that are mapped to each required item in the curriculum

- A report will be delivered to the General Assembly in the fall of 2020. A new IT security standard or policy related to this requirement will be also be created.

Any Questions?

Upcoming Events

Future ISOAG Speakers

August 8, 2020

This meeting will be a joint meeting with members of the Virginia Cyber Security Partnership

Elliott Casey, Commonwealth's Attorneys' Services Council

Christopher Cope, U.S. Department of Justice

Robert Reese, VSP

Bob Austin, Korelogic

ISOAG meets the 1st Wednesday of each month in 2020

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk