THE AUTOMATION OF CYBER SECURITY

SOAR(Security Orchestration Automation and Response)

DaeHyeob Kim

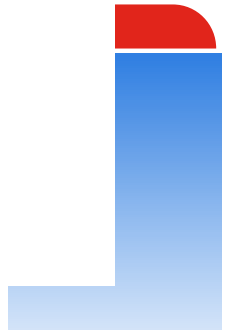
-

Agenda

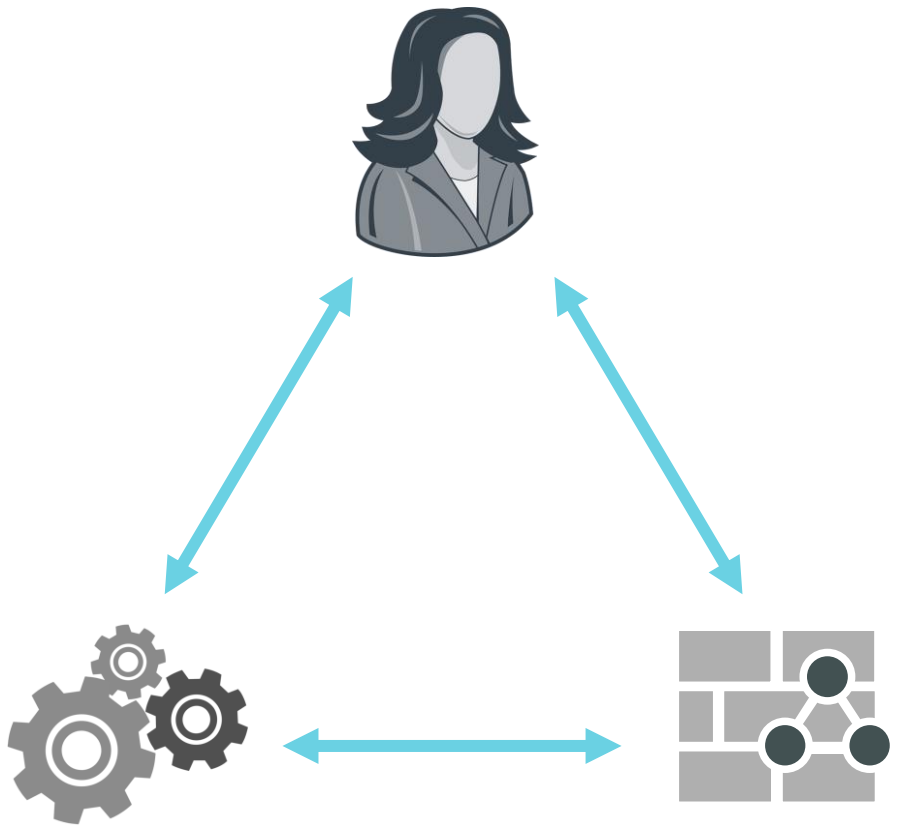
1. Current SOC Challenge
2. What is SOAR?
3. Playbook Use-cases of SOAR
4. Things to consider before using SOAR

Current SOC Challenge

and history of the SOC



SOC(Security Operation Center)

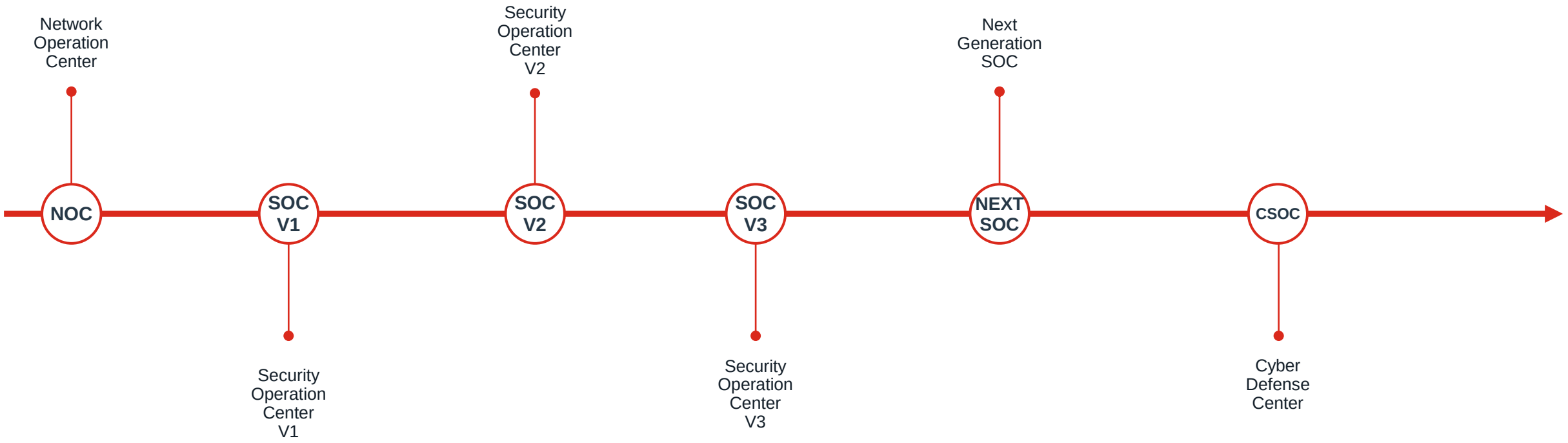


A Security Operations Center, or SOC, is an specialized organizational resource consisting of a specialized set of

- ***People***
- ***Processes***
- ***Technology***

dedicated to ***monitoring and defending organizational IT assets*** *and* ***detecting, containing, eradicating and assisting in the recovery from security threats*** *and associated incidents.*

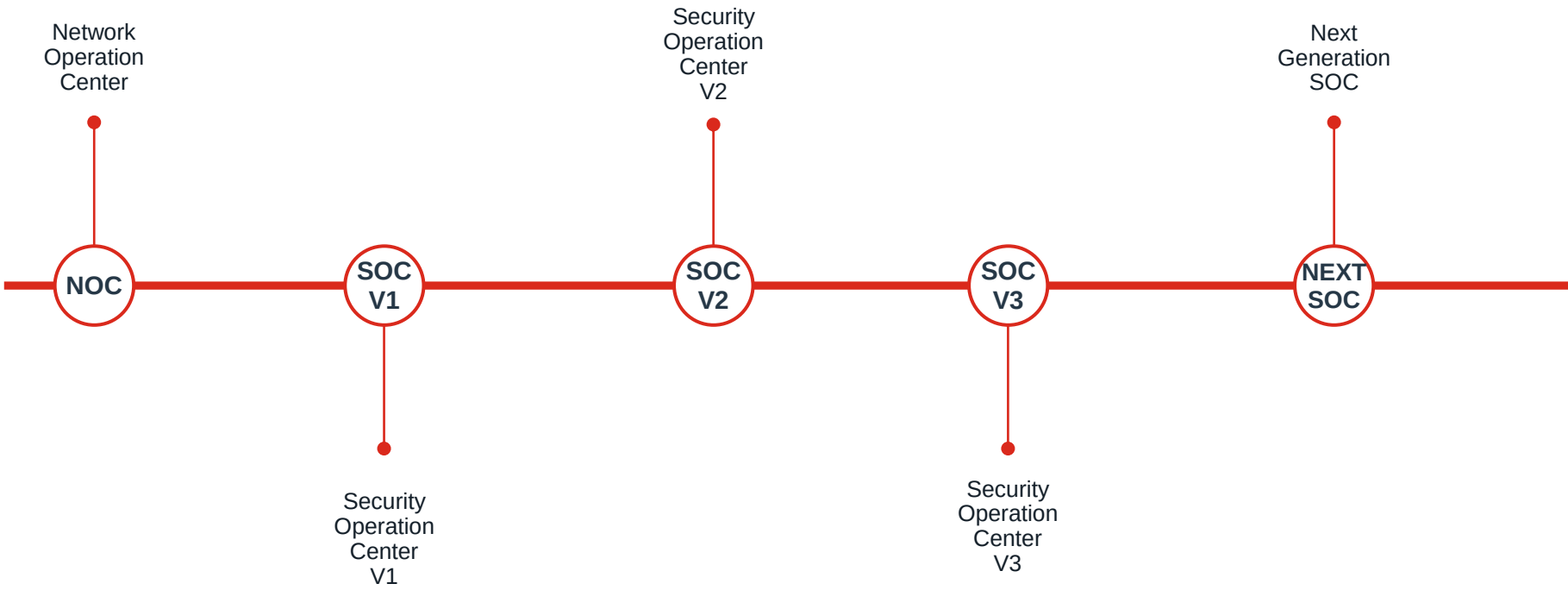
The history and evolution of the SOC



The history and evolution of the SOC

Network Operation Center

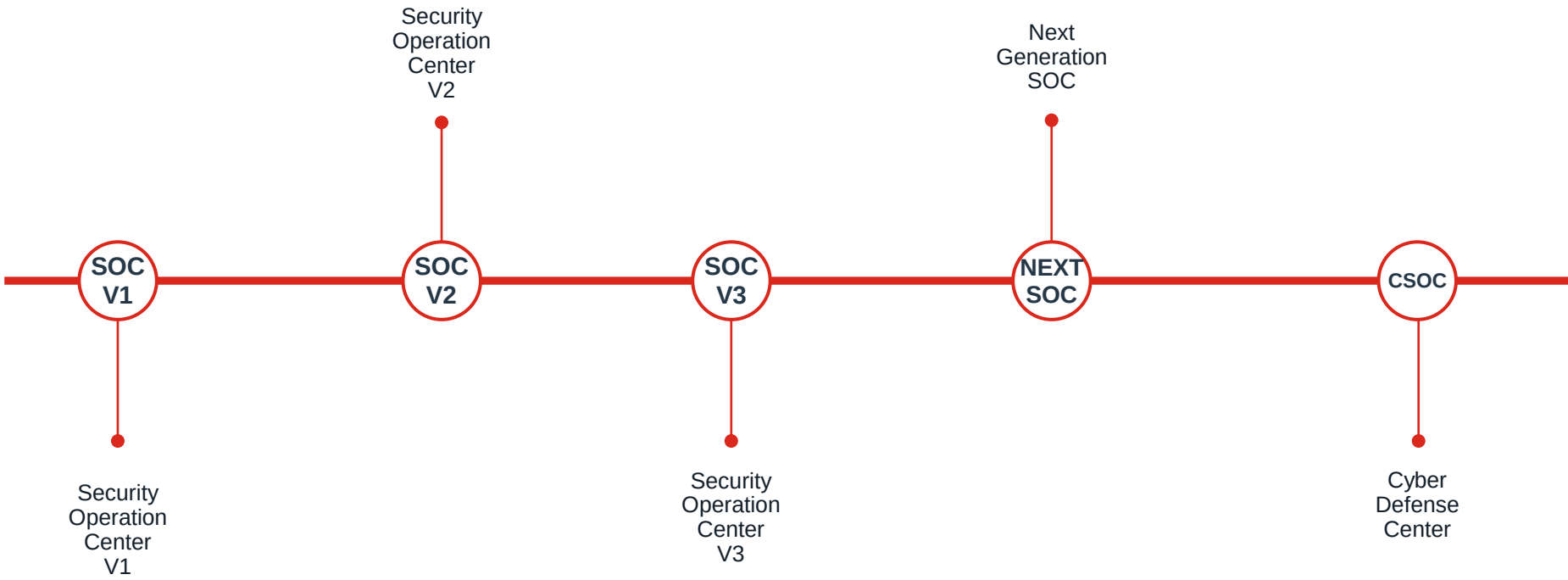
- Products
  - Network Alerts
- Used by:
  - Government
  - Military
- Timeline:
  - Before 1995
- Primary Jobs
  - Network Device Management
  - Malicious Code Analysis



The history and evolution of the SOC

NSOC/SOC V1

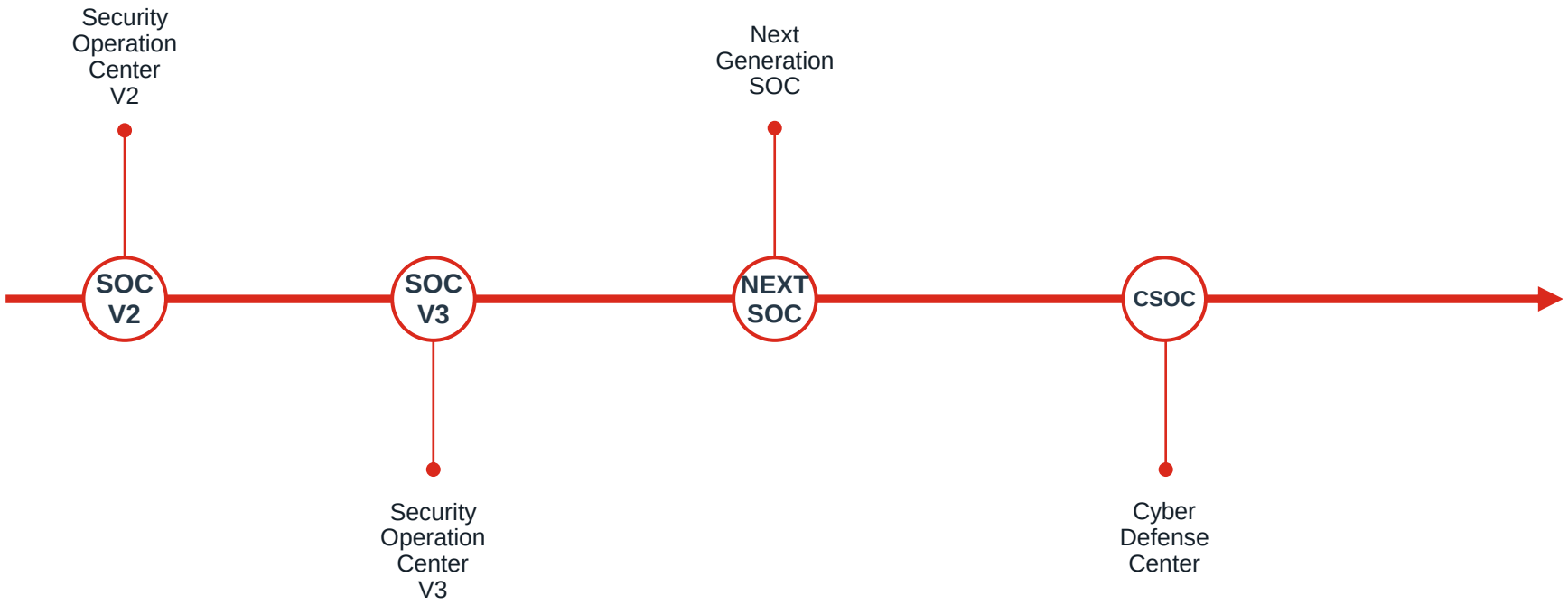
- Products
  - AntiVirus
  - IDS
  - Firewall
- Used by:
  - Government
  - Military
  - Large Enterprises
  - Banks
- Timeline:
  - 1996 ~ 2000
- Primary Jobs
  - Virus Alerts
  - Intrusion Detection and Response with IDS



The history and evolution of the SOC

SOC V2

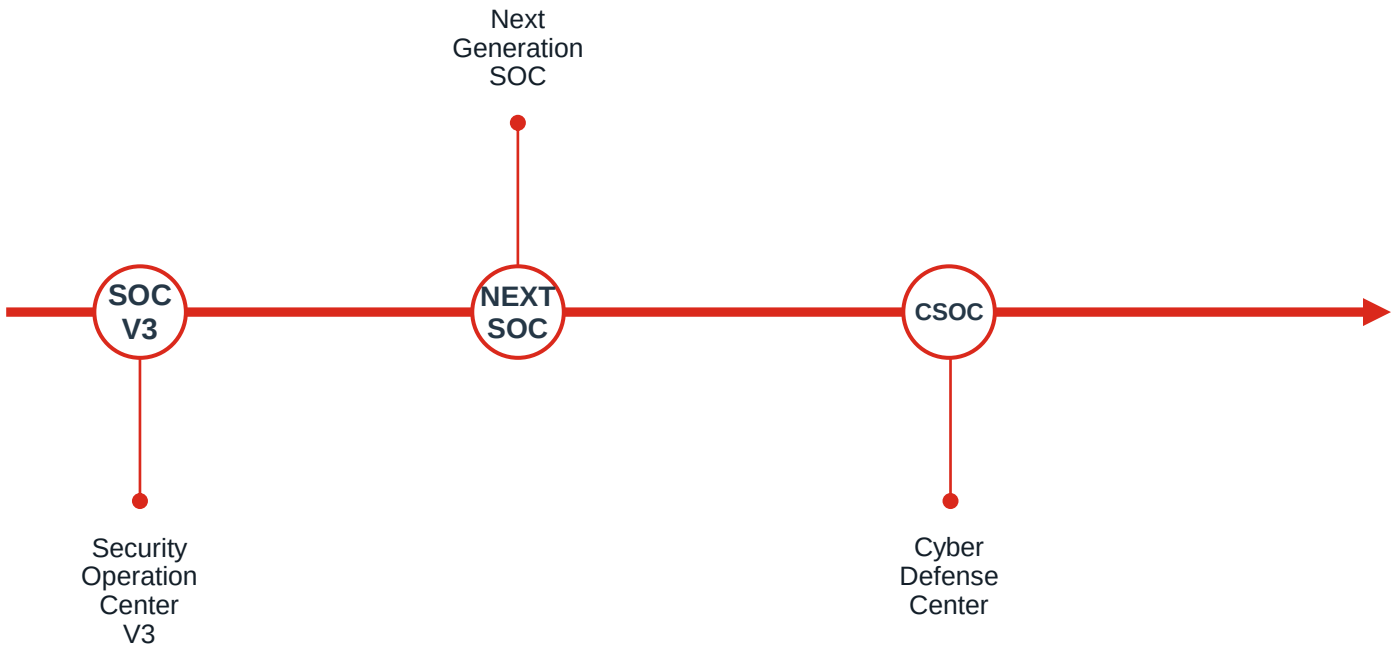
- Products
  - Vulnerability Management
  - Dynamic Packet Filtering
  - AntiSpam
  - IPS (Intrusion Prevention System)
- Used by:
  - Government
  - Military
  - Large Enterprises
  - Banks
- Timeline:
  - 2000 ~ 2006
- Primary Jobs
  - Malicious Code Analysis
  - Virus Alerts
  - Intrusion Detection and Response with IDS
  - Compliance
  - Incident Response



The history and evolution of the SOC

SOC V3

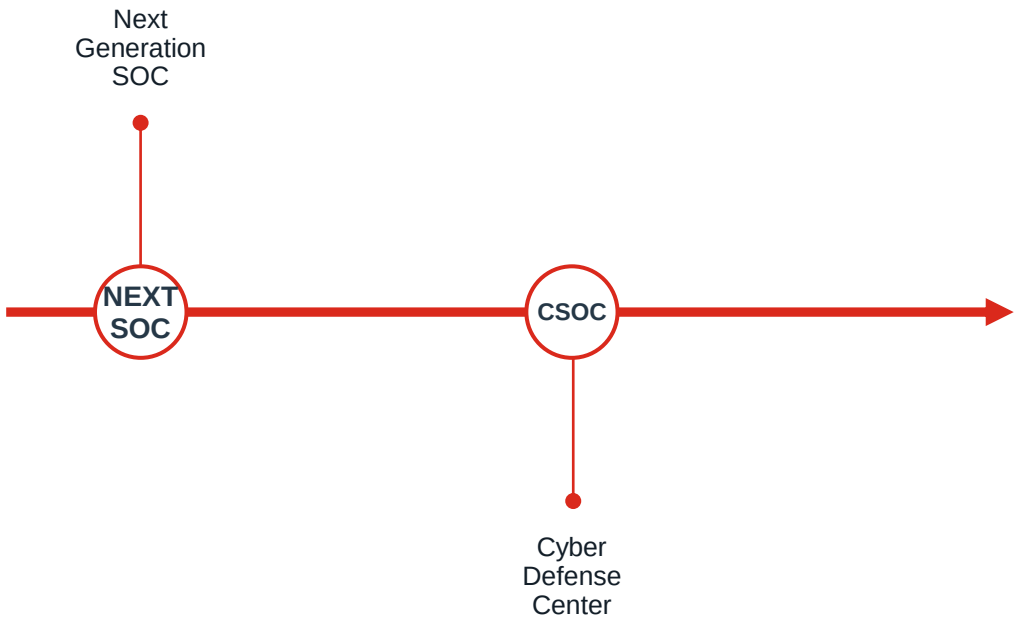
- Products
  - DLP (Data Loss Prevention)
  - APT (Advanced Persistent Threat)
  - SIEM
  - SecOPs
- Used by:
  - Government
  - Military
  - Large, Medium Enterprises
  - Banks, Pharmacys
- Timeline:
  - 2007 ~ 2013
- Primary Jobs
  - Previous Work
  - Regulatory Compliance
  - Log Monitoring
  - Malware Analysis



The history and evolution of the SOC

Next Generation SOC

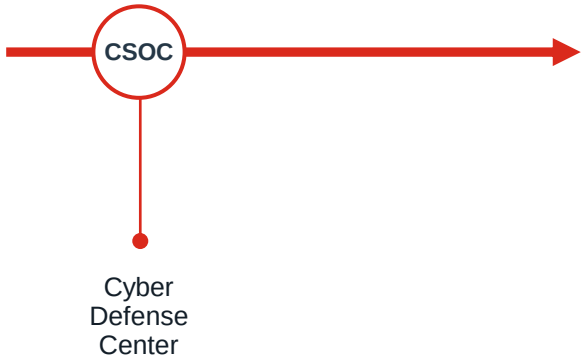
- Products
  - CASB (Cloud Access Security Broker)
  - Cloud Security
  - UEBA (User Behavior Analytics)
  - TIP (Threat Intelligence Platform)
  - Sandboxing
  - CERT
  - BYOD
- Used by:
  - Government
  - Military
  - All Industries
  - Banks
- Timeline:
  - 2013 ~ 2017
- Primary Jobs
  - Reverse Engineering
  - AL/ML Models
  - Threat Intelligence



The history and evolution of the SOC

Cyber Defense Center

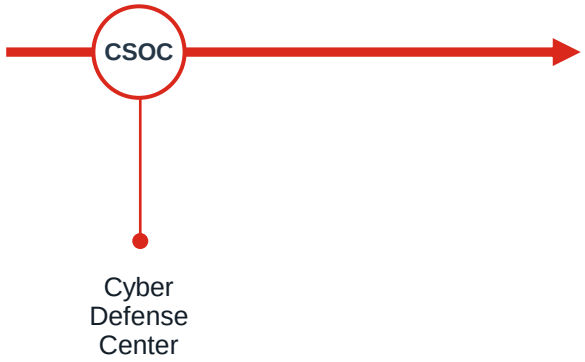
- Products
  - Big Data, Data Lake
  - CWPP
  - CSPM
  - SOAR
  - Deception (HoneyPot)
  - EDR (Endpoint Detection Response)
  - Cloud Native SIEM
- Used by:
  - All Industries
  - Smart Homes
  - Vehicles
- Timeline:
  - 2017 ~ Current Days
- Primary Jobs
  - Threat Hunting
  - Automation, Orchestration
  - Playbooks Workflow
  - Analytics
  - External Risk Scoring

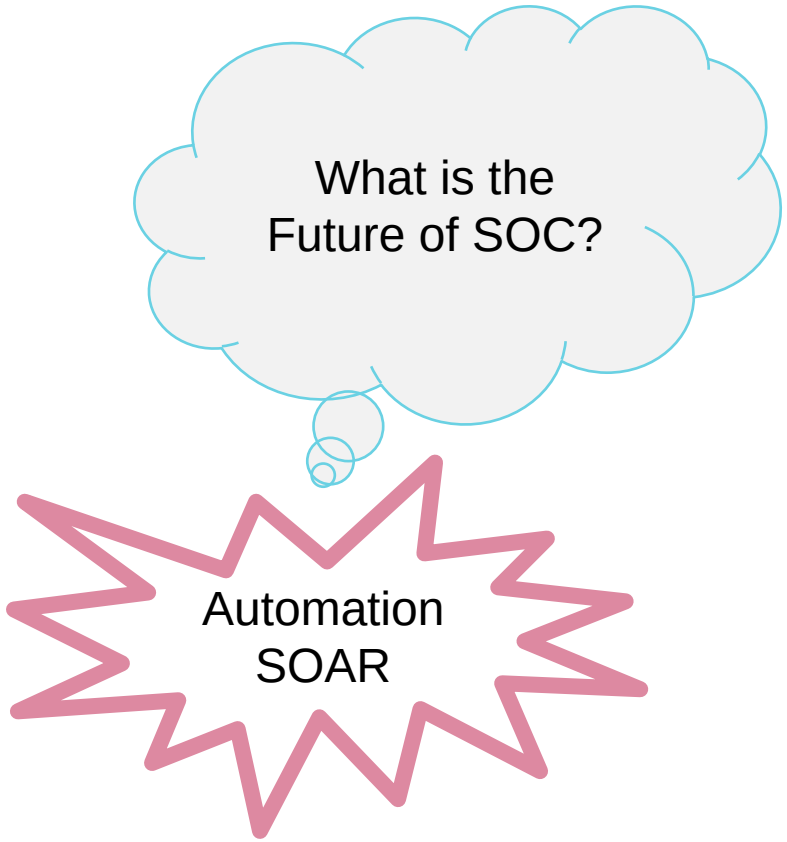


The history and evolution of the SOC

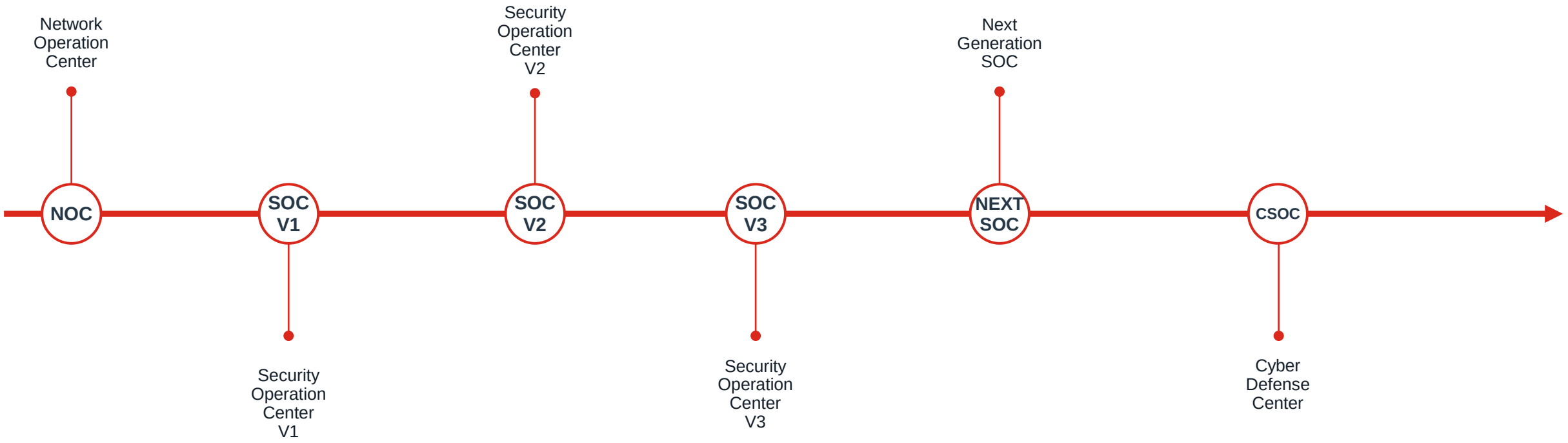
Cyber Defense Center

- Products
  - Big Data, Data Lake
  - CWPP
  - CSPM
  - SOAR
  - Deception (HoneyPot)
  - EDR (Endpoint Detection Response)
  - Cloud Native SIEM
- Used by:
  - All Industries
  - Smart Homes
  - Vehicles
- Timeline:
  - 2017 ~ Current Days
- Primary Jobs
  - Threat Hunting
  - Automation, Orchestration
  - Playbooks Workflow
  - Analytics
  - External Risk Scoring





The history and evolution of the SOC



People: Lack of Skilled Cyber Security Analysts

Capgemini

56% **Company said**

Cybersecurity analysts are overwhelmingly lacking[1]

(ISC)²

~3M

Global cybersecurity manpower shortage[2]

ESG

41% **Junior Recruitment**

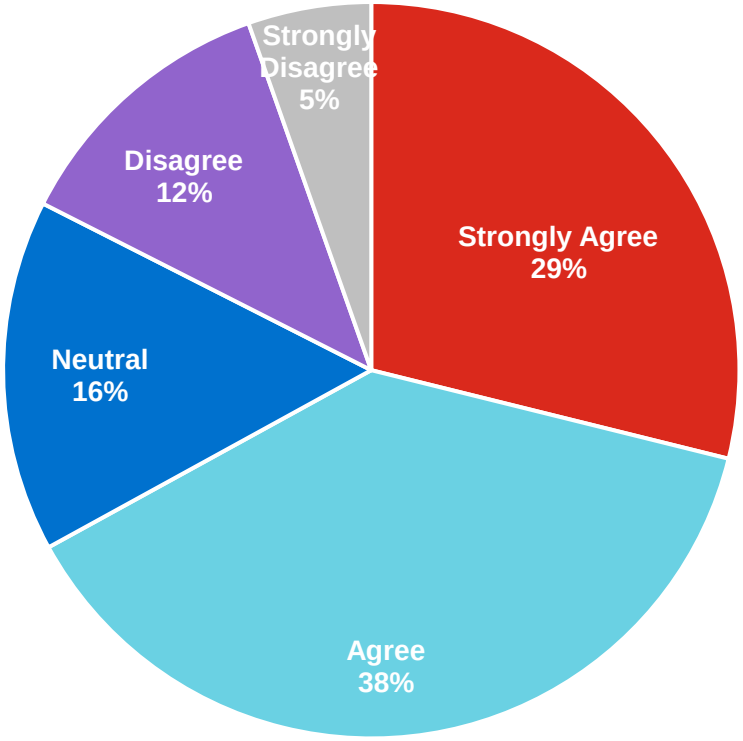
Because there are very little experienced cybersecurity experts in the market[3]

Sources:

1. "Reinventing Cybersecurity with Artificial Intelligence," Capgemini, accessed January 27, 2020
2. (ISC)² CYBERSECURITY WORKFORCE STUDY, 2018.
3. "Is the Cybersecurity Skills Shortage Getting Worse?" ESG, May 10, 2019

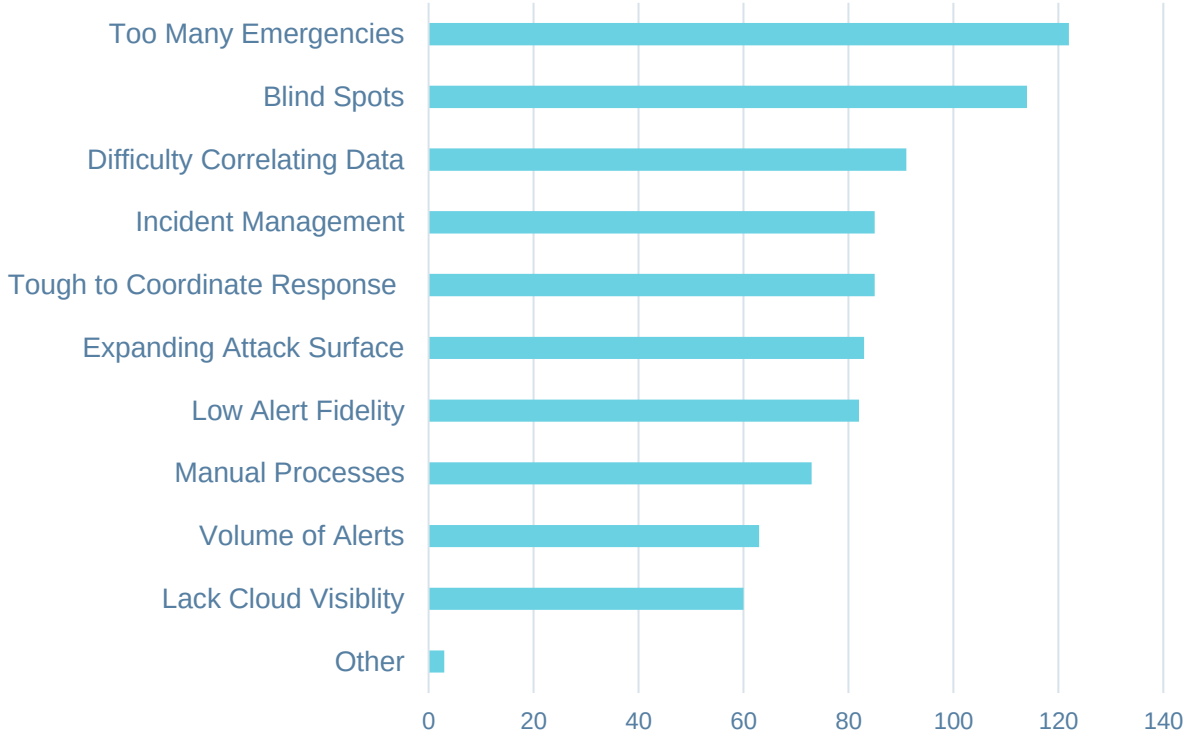
Process: Disconnected Security Products and Process

My organization manages threat detection and response using an assortment of disconnected security tools.



67% of organizations use disconnnected security tools

Which of the following would you say are your organization's biggest challenges regarding threat detection/response?



Challenged by constant emergencies, blind spots and data inconsistency

Sources: ESG Research. Trends in XDR. October 2020.

Current SOC Challenge

➢ Complex system environment and slow incident response speed

Advanced Threat

Threats that rapidly become complex and sophisticated

APT, AI-driven Malware, MaaS, M2M ···

Staff shortages

Lack of skilled security engineer

41% of companies worldwide employ junior level security engineer

Disparate tools

Continuous growth of security systems within organizations

System expansion, introduction of next-generation solutions, advancement of business...

Repetitive tasks

Increased repetitive tasks, manual & slow response

Increased organizational fatigue in work, slow incident handling···

Too many Alert

Too many security events

Can one person process hundreds of event per seconds?

Self-Questions from SOC (Security Operation Center) perspective.

- Human: To analyze all the events and alerts in your organization··· Is it possible to secure(hire) manpower for the SOC team?
- Process: When you define a security process··· Can you SOC respond to all the alerts or incidents?

Technology => SOC needs the SOAR, an intelligent security control platform that can accelerate SOC work process

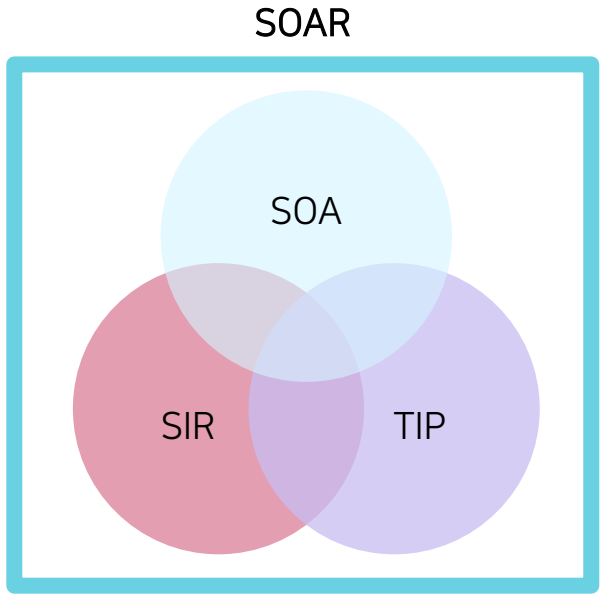
What is SOAR?

Security Orchestration, Automation and Response

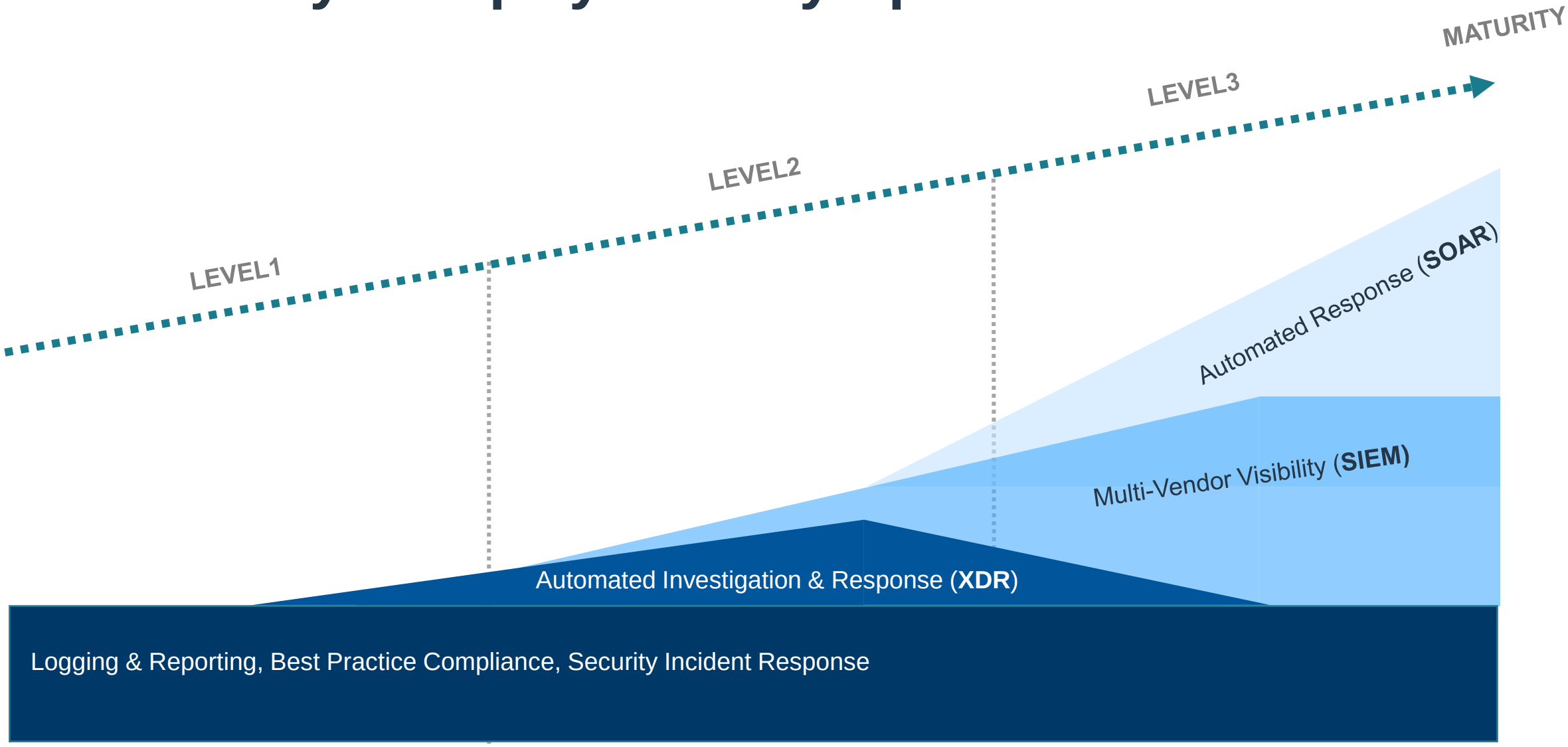
SOAR…

- SOAR(Security Orchestration, Automation and Response), 2017 Gartner

1. SOA : Security Orchestration and Automation
2. SIR : Security Incident Response
3. TIP : Threat Intelligence Platform



SOC Maturity - Simplify Security Operations



Ref: 2020 CISO Benchmark Study

SOAR - Intelligence SOC Platform

- Fundamental of SOAR

1. Orchestration & Automation
2. Threat Intelligence Management
3. Incident & Case Management
4. Workflow & Collaboration

What Complexities can SOAR Solve?

SOAR can solve - Security Operations Struggling To Keep Pace

Rise in Ransomware

“Two thirds of organizations report being targeted by ransomware. More than half brought in an incident response service and reported the incident to law enforcement.”

Fortinet, Global Ransomware Survey, 2021

Point Product Complexity

Eighty percent of organizations currently or plan to pursue a vendor consolidation strategy. 78% of CISOs have 16 or more tools in their cybersecurity vendor portfolio.

Gartner, Top Security and Risk Management Trends, 2021

Alert Overload

“70% of respondents say their home lives are being emotionally impacted by their work managing threat alerts. 51% feel their team is being overwhelmed by the volume of alerts.”

Security Magazine, 70% of SOC Teams are Overwhelmed by Alert Volume, 2021

Scarcity of Cyber Skills

“57% of organizations have been impacted by the global cybersecurity skills shortage. Among those, 62% said that the skills shortage has increased the workload on existing staff; and 38% said that the skills shortage has led to employee burnout and employee attrition.”

ESG and ISSA, The Life and Times of Cybersecurity Professionals, 2021

SOAR - Intelligence SOC Platform

➢ Expected effects of SOAR

Unified Incident Response Management

Alert Triage & Automation

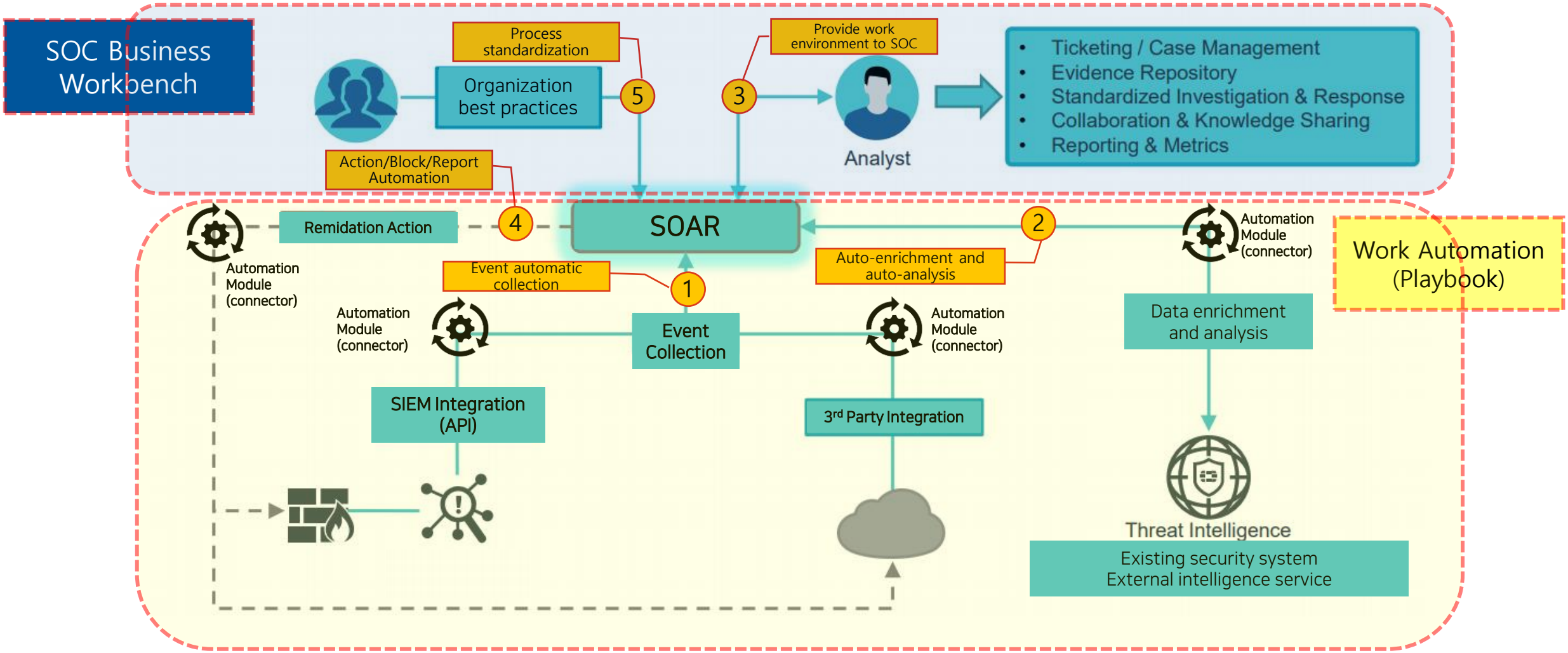
SOC Optimization

SOC Collaboration

1. Alerts, Incidents, Indicators, Assets, Tasks Classification and Integration
2. ROI(Return of Investment), MTTD(Mean Time to Detection), MTTR(Mean Time to Response) Improvements and Tracking
3. Change from the existing complex automation to an easy task automation environment(Visual Playbook Designer, Connectors, Playbook)
4. RBAC(Role-based access control), Clear R&R(Role and Responsibilities) setting by establishing standard business processes.
5. Minimize human skill gap and human error through work standardization through playbook, and minimize loss of operating experience due to personnel replacement
6. Apply distributed security work environment through single and multi-tenant environment configuration

SOAR - Intelligence SOC Platform

➢ SOAR Workflow



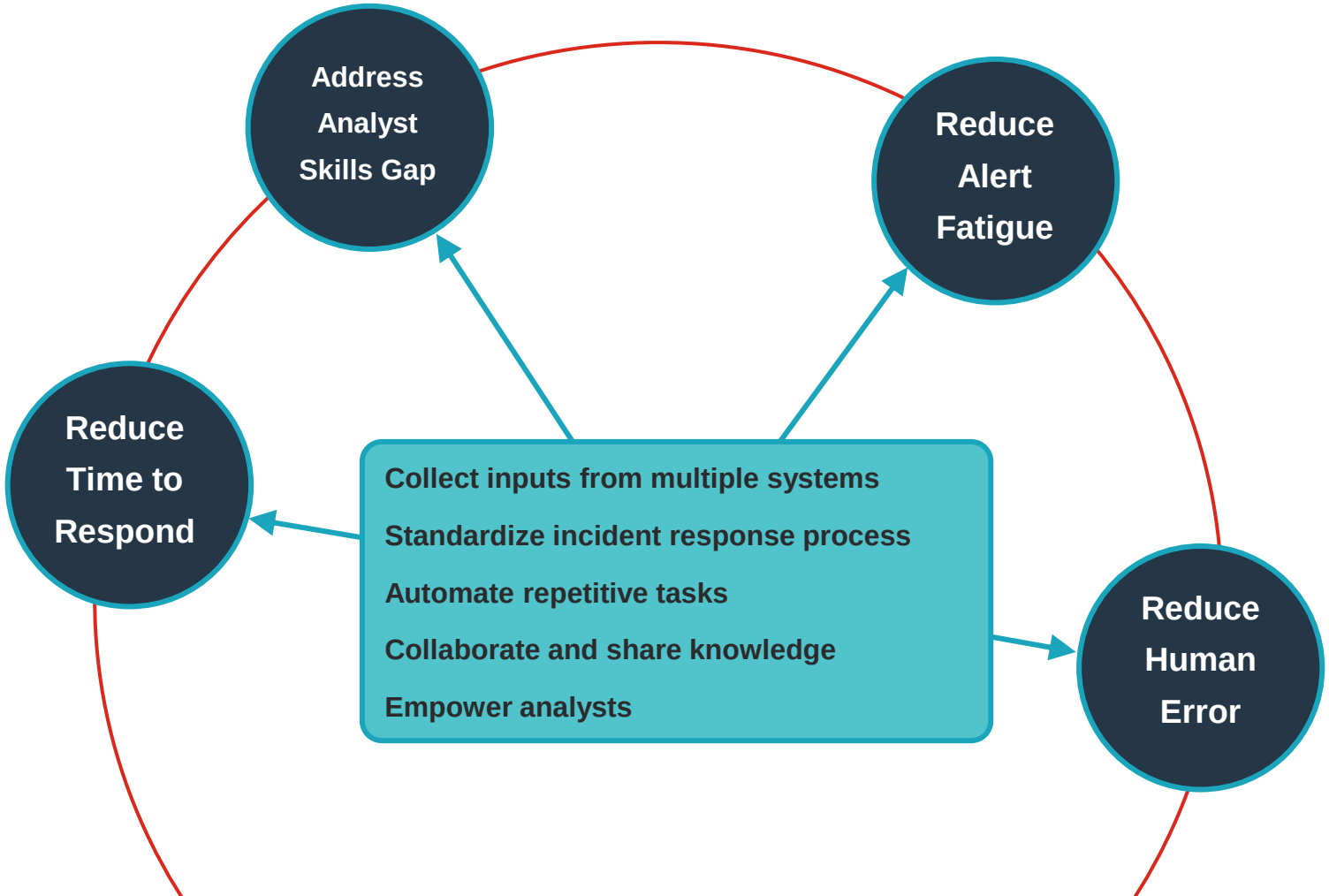
SOAR - Intelligence SOC Platform

➢ How does SOAR collect, process, and enrich data?

I. 3rd Party Products
II. REST API
III. Syslog
IV. SMNP
V. SMTP

SOAR - Intelligence SOC Platform

- Expected effects of SOAR



Integrated incident response management tool

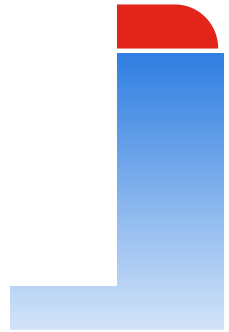
Alert classification and automatic response

Process standardization, Data integration

SOC Security Operations Collaborative Environment

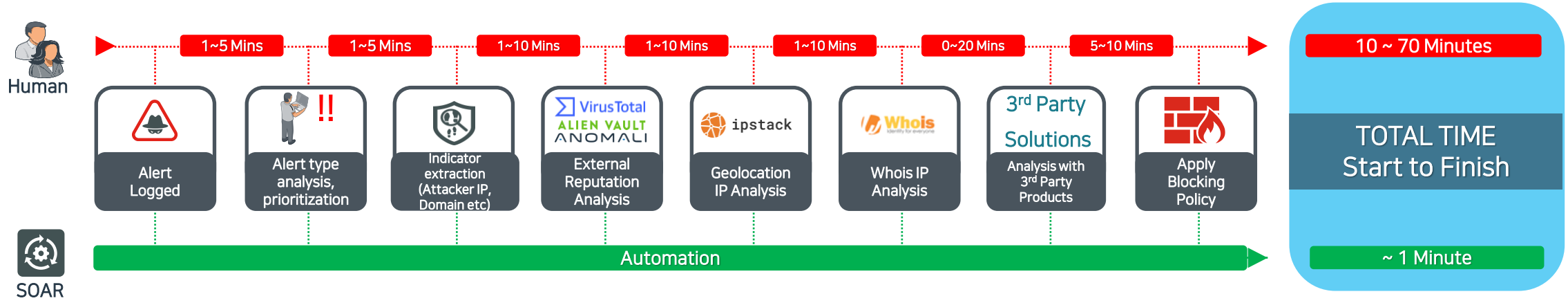
Playbook Use-cases of SOAR

How can SOAR benefit the SOC work process?

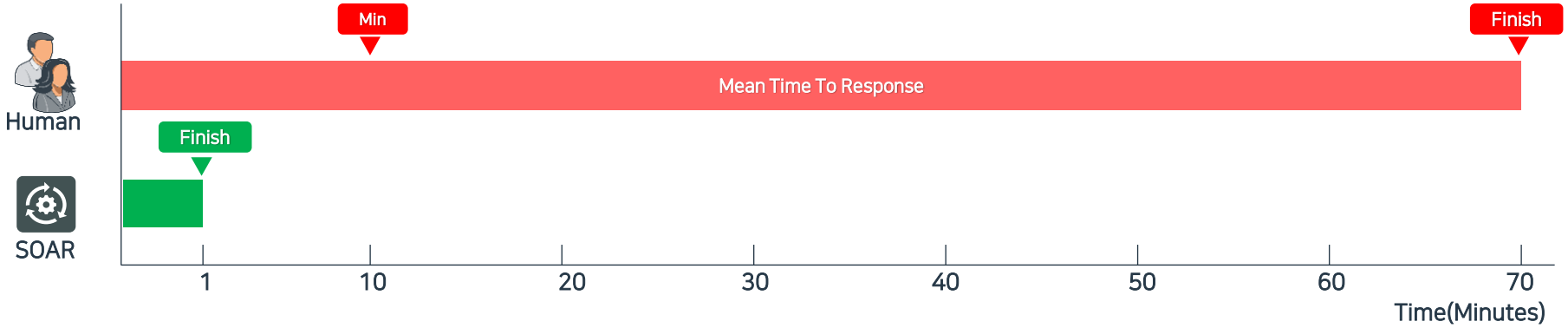


SOAR - Playbook Use Cases

➢ SOC Incident Response Workflow#1 : Network IOC Analysis(Detected breach information analysis)



➢ MTTR(Mean Time To Response) Time Comparison

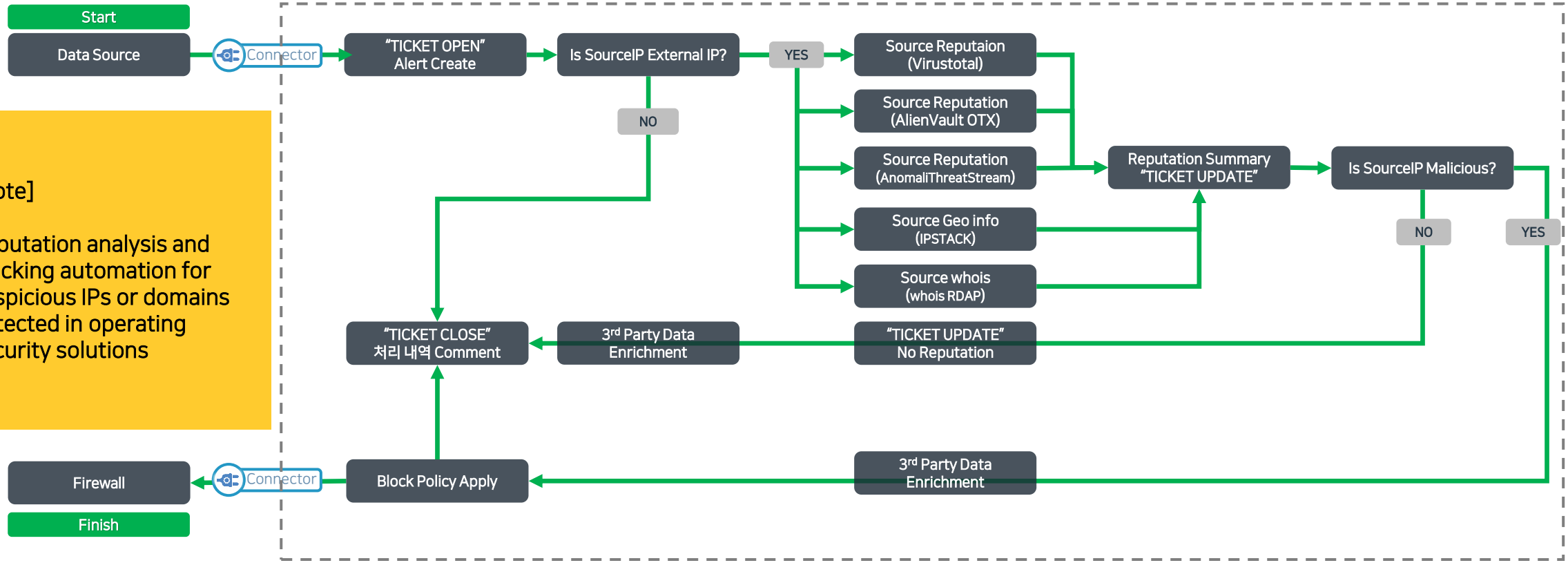


Using SOAR,
Up to 98% time
efficiency increase

SOAR - Playbook Use Cases

➢ SOC Incident Response Workflow#1 : Network IOC Analysis(Detected breach information analysis)

SOAR – Playbook Example

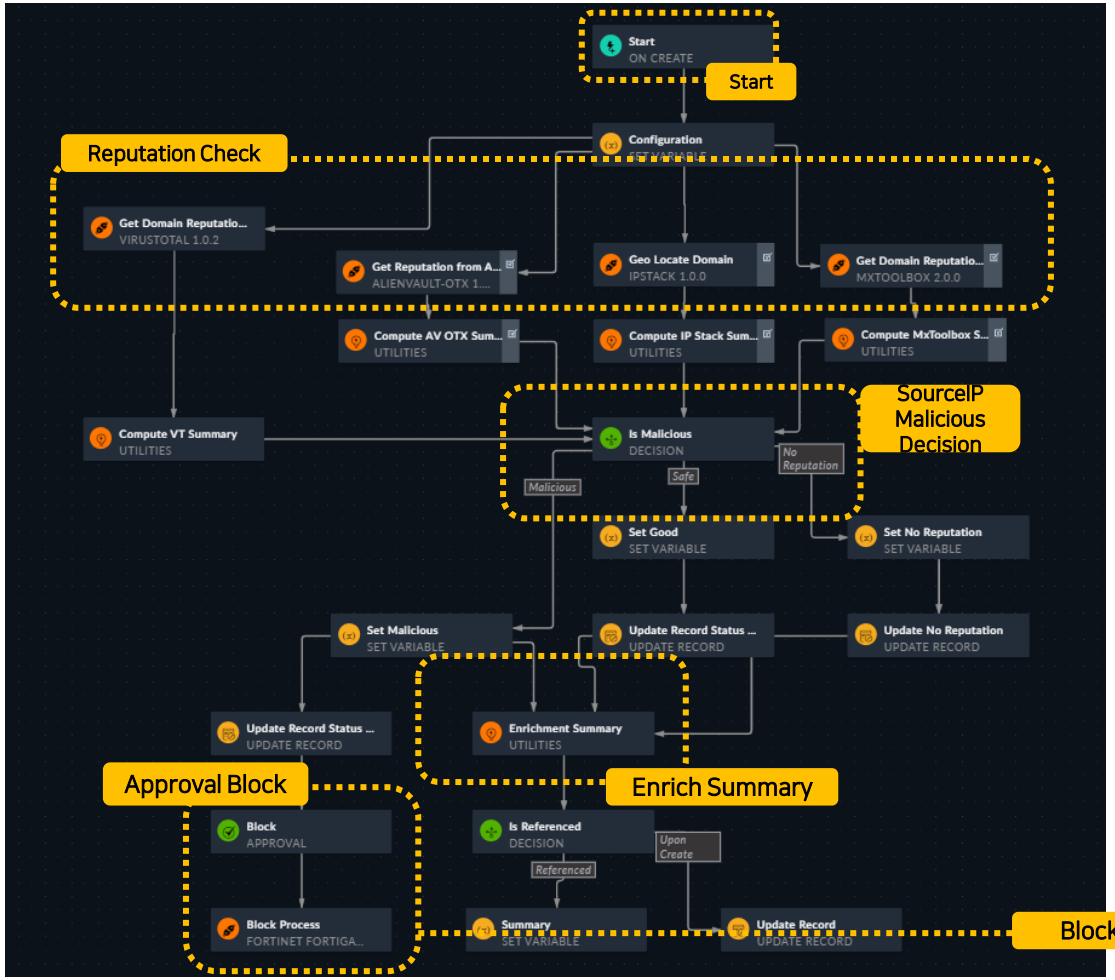


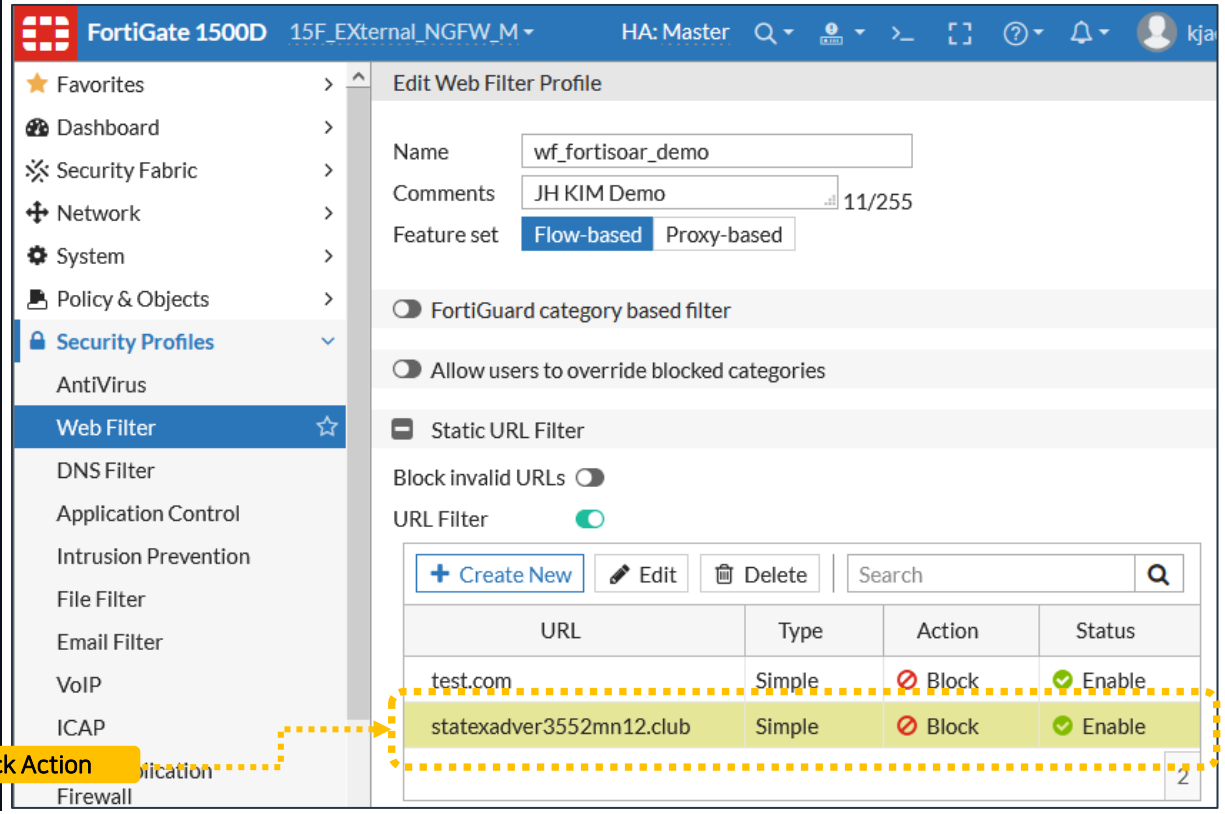
[Note]

Reputation analysis and blocking automation for suspicious IPs or domains detected in operating security solutions

SOAR - Playbook Use Cases

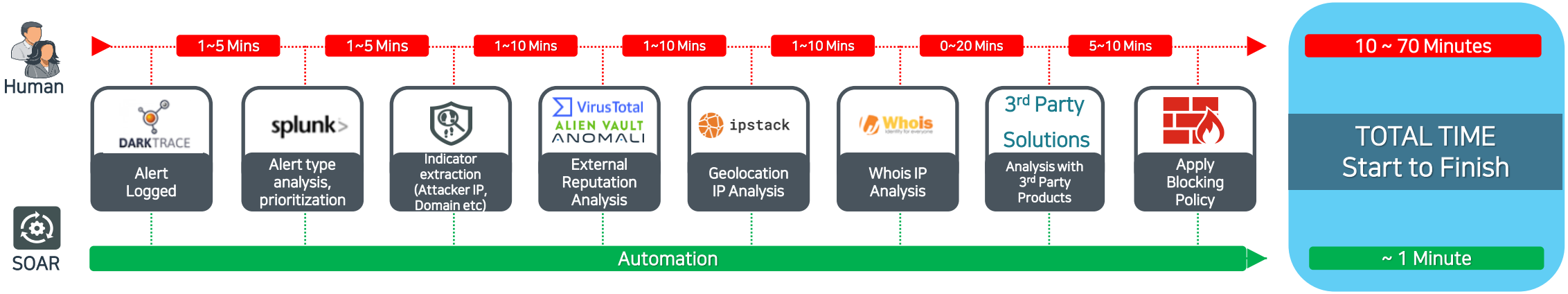
- SOC Incident Response Workflow#1 : Network IOC Analysis(Detected breach information analysis)



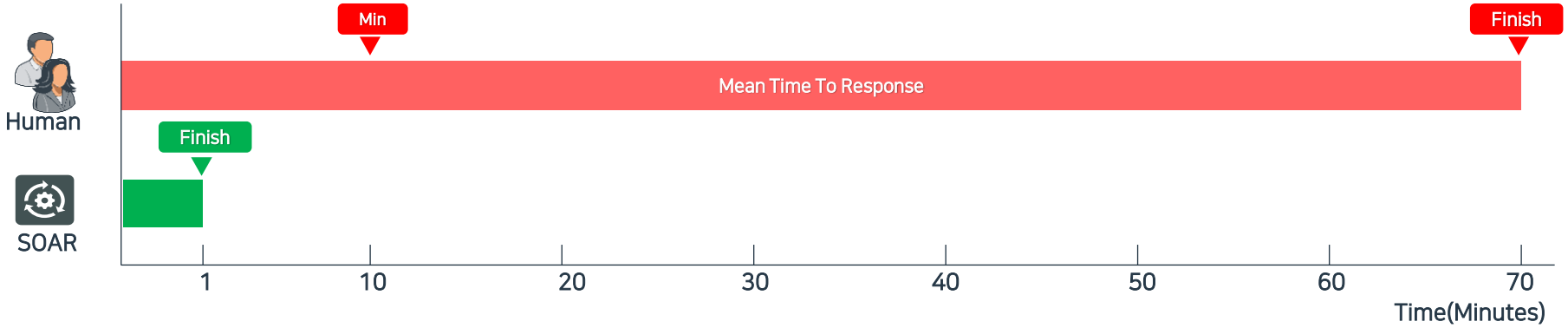


SOAR - Playbook Use Cases

➢ SOC Incident Response Workflow#2 : Suspicious External IP automated response with integrating NTA, SIEM



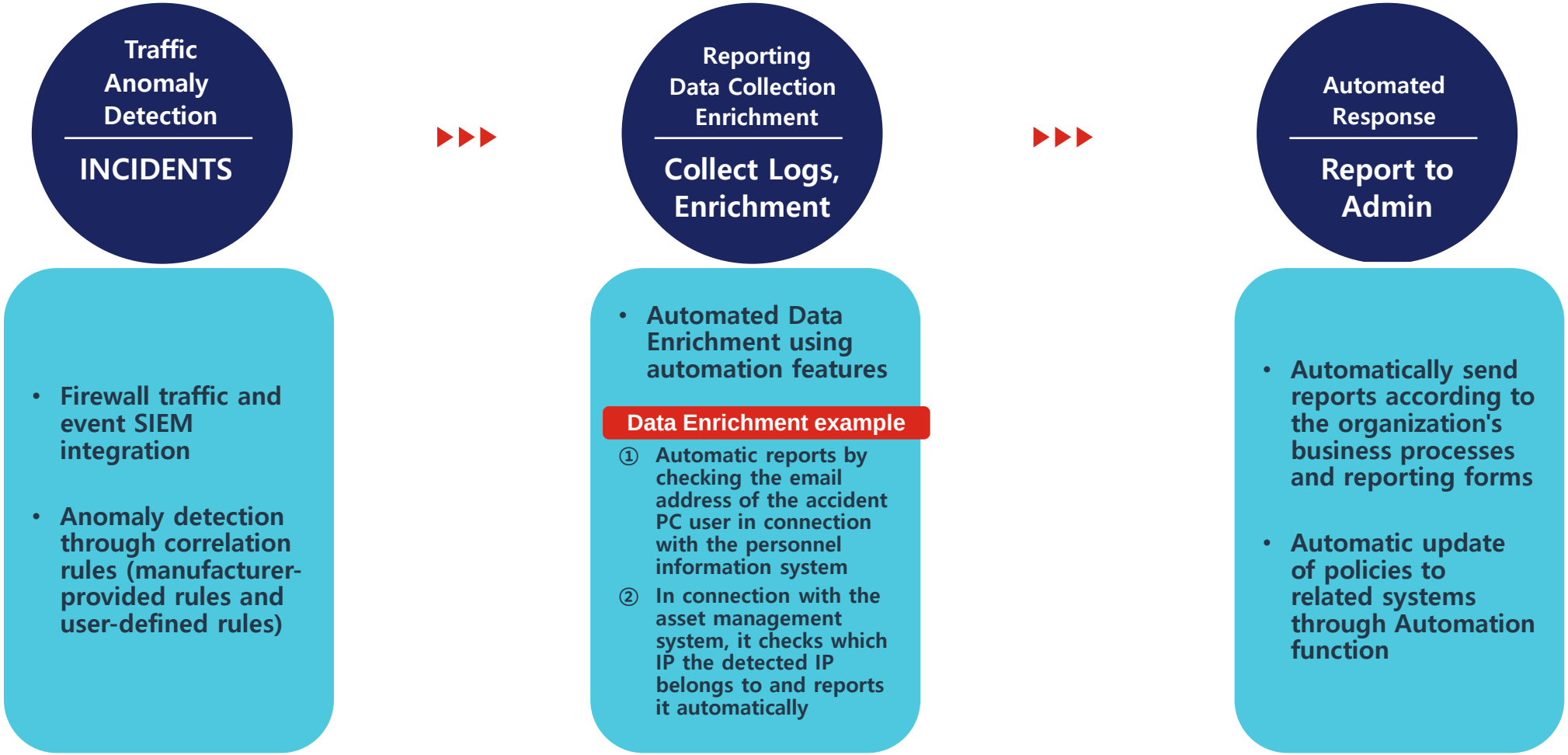
➢ MTTR(Mean Time To Response) Time Comparison



Using SOAR,
Up to 98% time
efficiency increase

SOAR - Playbook Use Cases

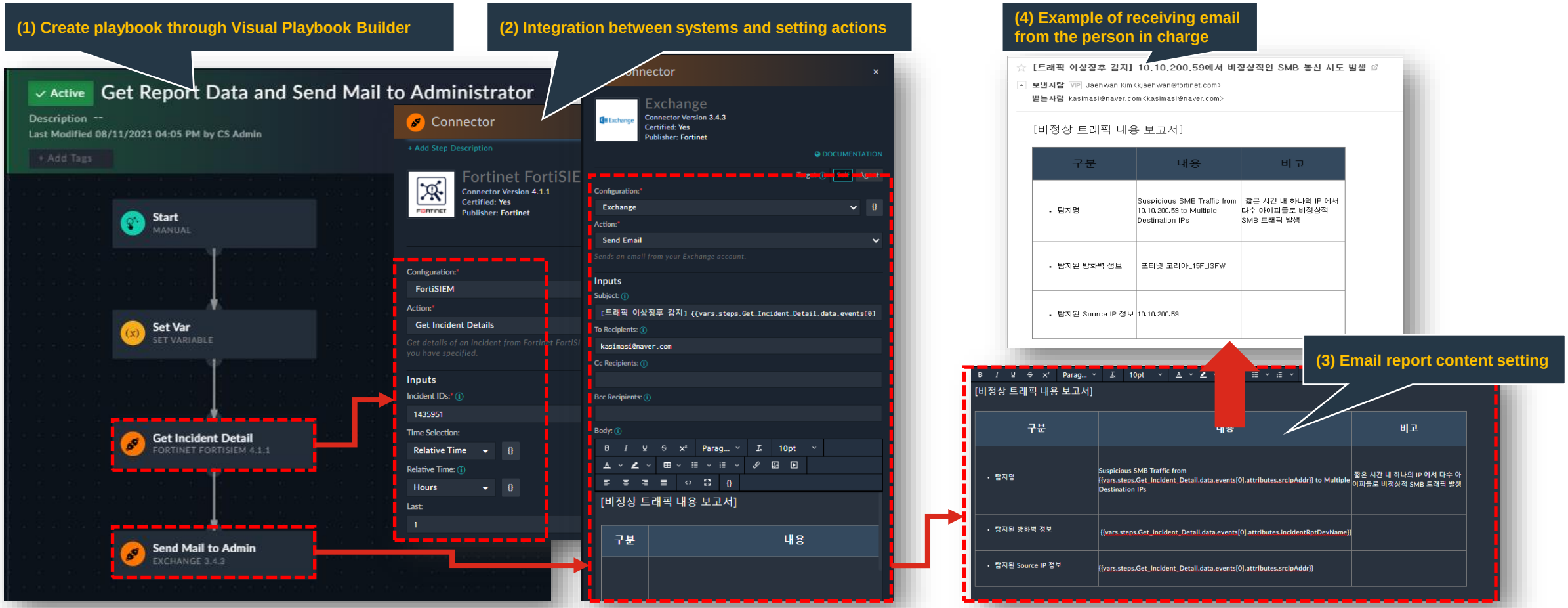
➢ SOC Incident Response Workflow#2 : Suspicious External IP automated response with integrating NTA, SIEM



SOAR - Playbook Use Cases

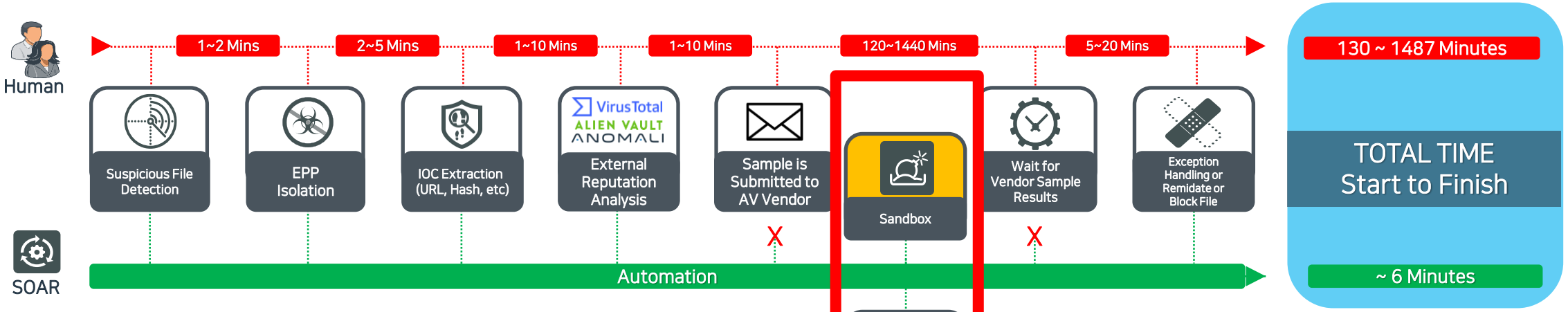
➢ SOC Incident Response Workflow#2 : Suspicious External IP automated response with integrating NTA, SIEM

FortiSOAR – Playbook Example

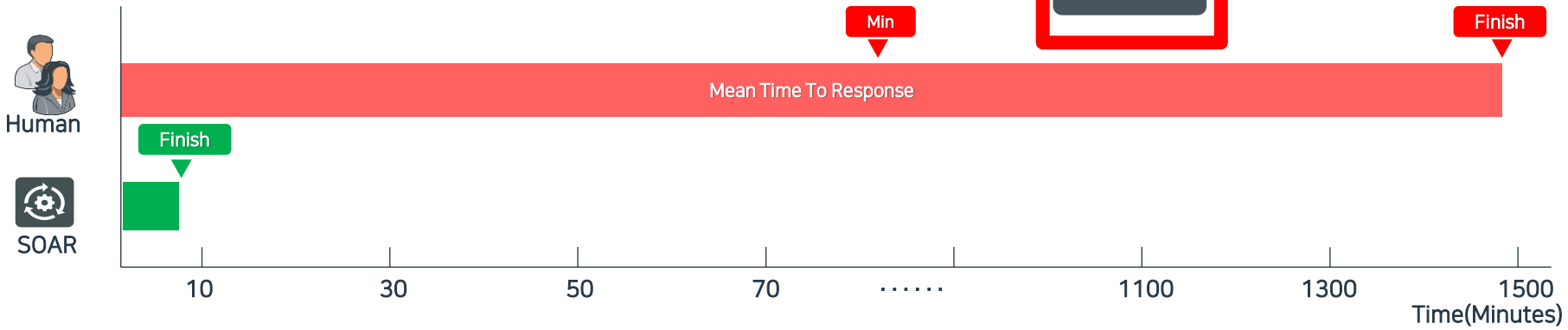


SOAR - Playbook Use Cases

➢ SOC Incident Response Workflow#3 : Unknown File Analysis



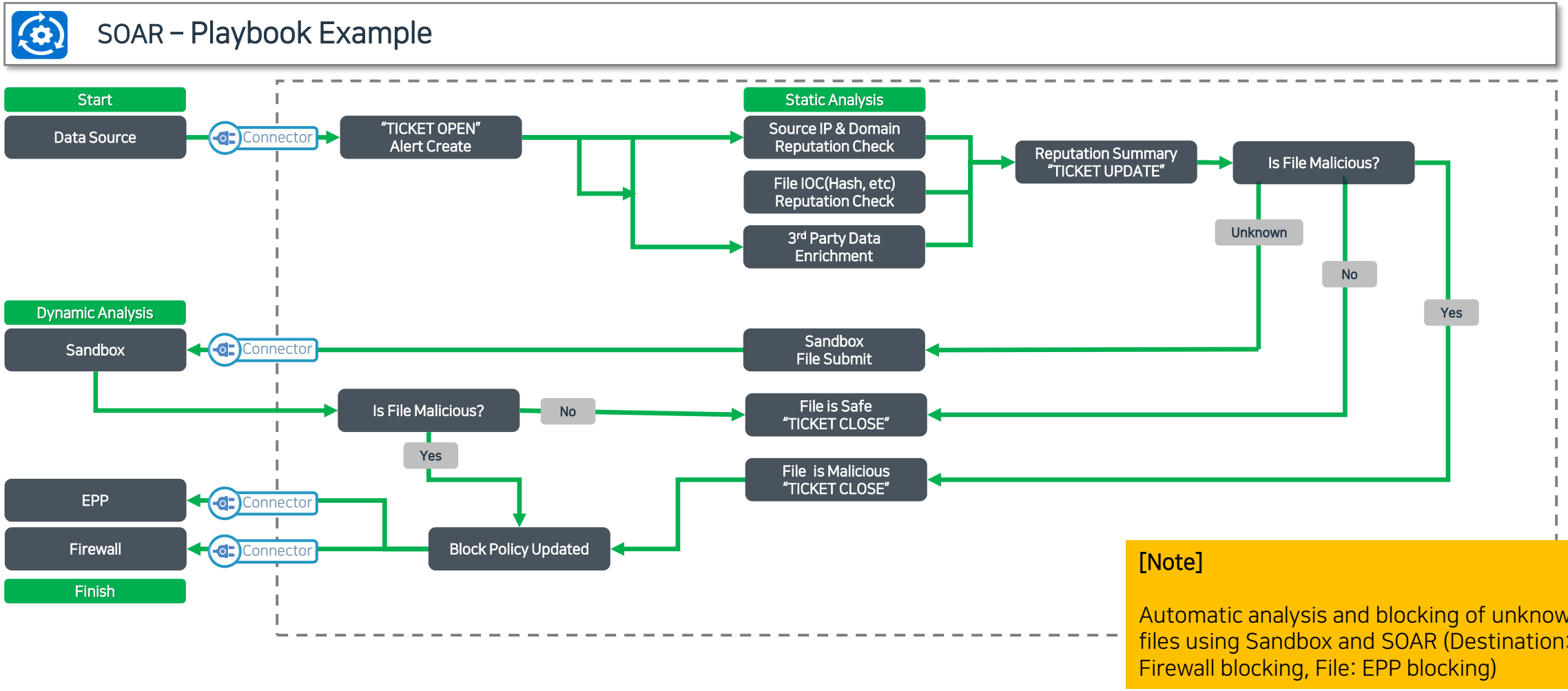
➢ MTTR(Mean Time To Response) Time Comparison



Using SOAR,
Up to 99% time
efficiency increase

SOAR - Playbook Use Cases

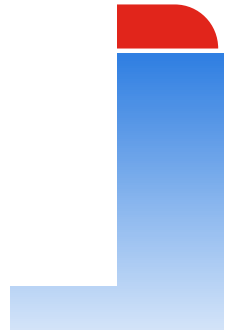
➢ SOC Incident Response Workflow#3 : Unknown File Analysis



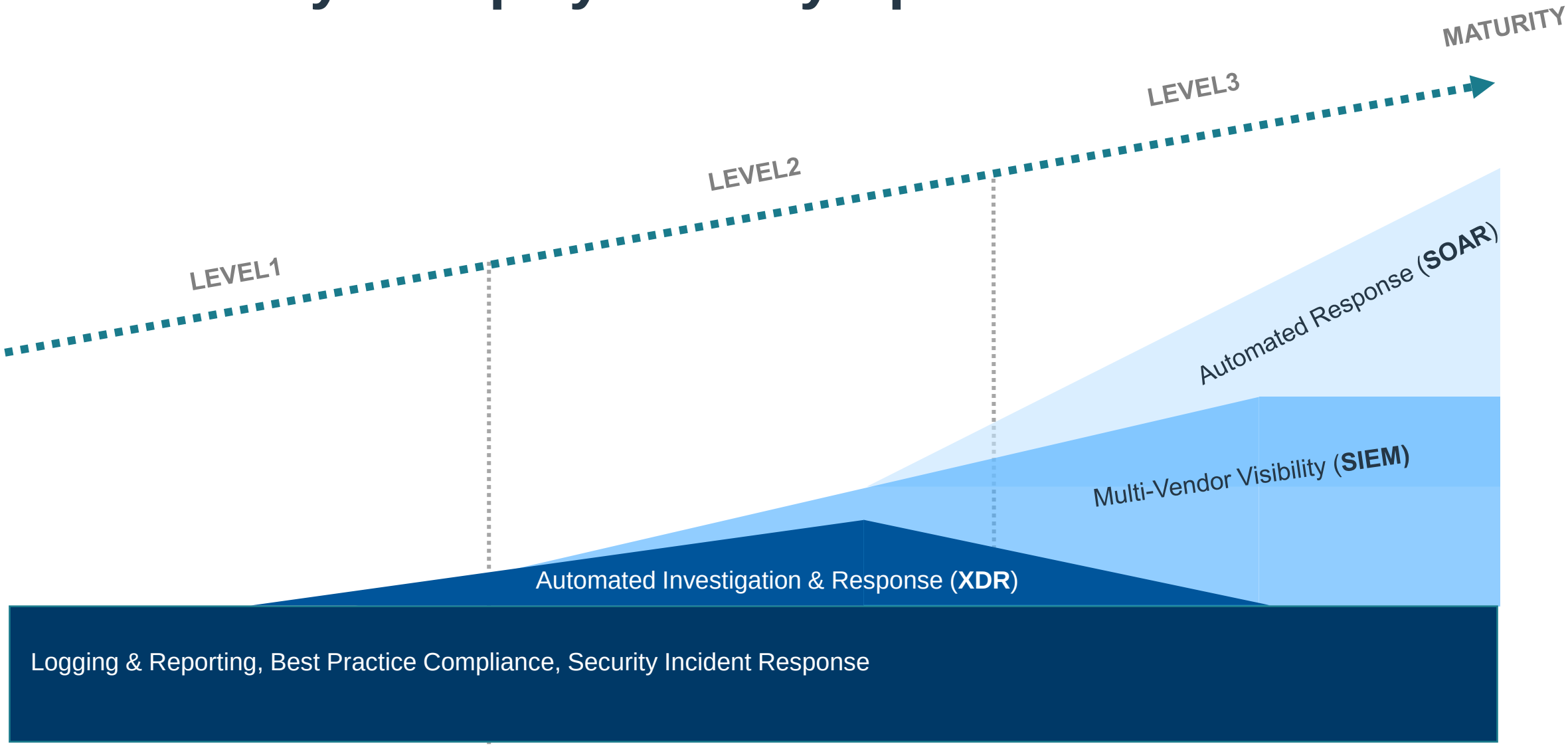
[Note]

Automatic analysis and blocking of unknown files using Sandbox and SOAR (Destination: Firewall blocking, File: EPP blocking)

Things to consider before using SOAR

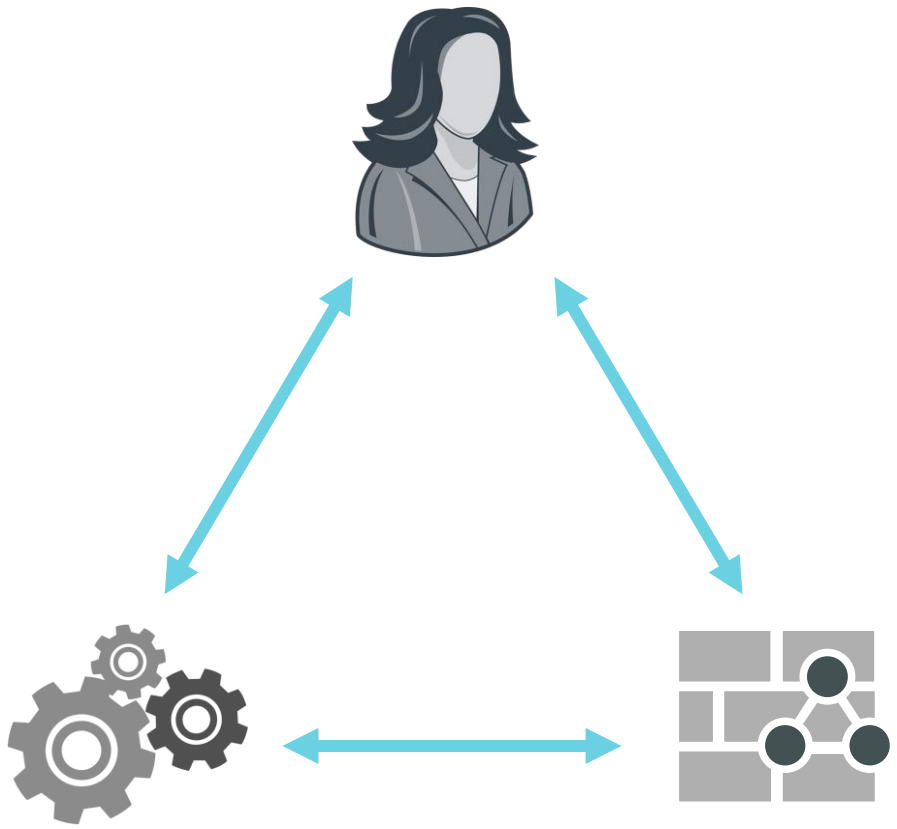


SOC Maturity - Simplify Security Operations



Ref: 2020 CISO Benchmark Study

SOC(Security Operation Center)



A Security Operations Center, or SOC, is an specialized organizational resource consisting of a specialized set of

- ***People***
- ***Processes***
- ***Technology***

dedicated to ***monitoring and defending organizational IT assets*** *and* ***detecting, containing, eradicating and assisting in the recovery from security threats*** *and associated incidents.*

Prerequisites for Effective SOAR Adoption

➢ Before introduction, what should be reviewed and how should it be approached?

① Necessity : Does my organization need SOAR?
- Identification of the total number of current events and the size of the analysis target = Cyber fatigue level of control personnel (workload)
- Identify trends and directions for data growth in your organization

② Know what to integrate : Among the systems/data used in our work, which ones will be integrated into the SOAR platform?
- List of systems and data used by the operating organization
- Find out which product you can integrate with SOAR
- Review of improved efficiency when integrated

③ Identify tasks to be automated: Among our tasks, which ones can be automated in SOAR?
- List of security processes
- Selecting highly effective tasks for automation through SOAR
- Proactive review of ROI that improves when tasks are automated

④ Interoperability: Is it possible to apply SOAR in our environment?
- Check whether interworking with existing operating systems