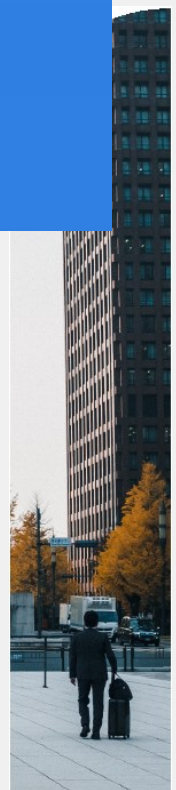
FortiSOAR - автоматизация реагирования на инциденты безопасности в неоднородном ИТ-окружении

Дмитрий Купецкий, SE



План

- Обзор
- Усовершенствование SOC с использованием FortiSOAR
- Архитектура
- Логика работы с событиями/алертами
- Особенности
- Q&A

Обзор

Сложность экосистемы увеличивает время реакции и устранения

И приводит к усложнению построения системы оркестрации, автоматизации и реагирования

Слишком много вендоров

Слишком много алертов

Ручной и медленный ответ

Недостаток квалифицированных специалистов

Как это решить?

Агрегировать

Сортировать

Приоритезировать

Связывать

Взаимодействовать

Обогащать

Эскалировать

Отлавливать

Восстанавливать

Обрабатывать

Документировать

Исполнять

Источник → Алерт → Расследование → Реакция

FortiSOAR – это независимое решение класса SOAR

Ключевой игрок класса SOAR в соответствии с Gartner’s Market Guide

Платформа управления SOC

- Управление кейсами организации
- Ролевое управление доступом
- Мультитенантность

Оркестрация и Автоматизация

- Плейбуки
- Коннекторы/Интеграции

Управление кейсами

- OOB модули для реагирования на инциденты, уязвимости и фрод
- Построение собственных модулей (Ex, GDPR, Legal)
- Контекстная визуализация

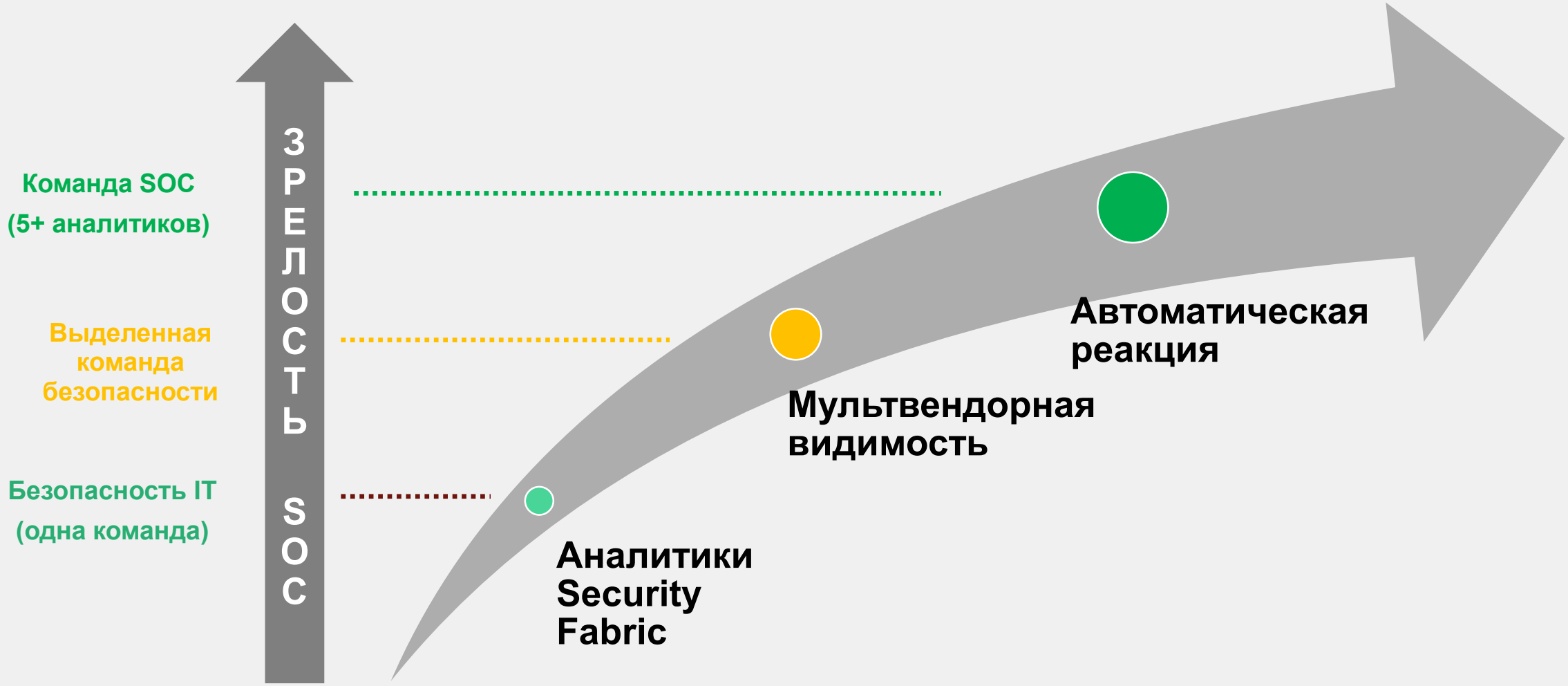
Упорядоченное реагирование

- Визуальный редактор для создания плейбуков
- 250+ коннекторов для автоматических действий
- Примеры реальных кейсов

Мультитенантность

- Распределенная/федеративная архитектура
- Контроль доступа к данным и плейбукам

Устранение сложности обеспечения безопасности за счет зрелости SOC



Обогащение данных об угрозах

Уведомления и алерты с отсутствующим контекстом, требующие расследования вручную и дополнения

Другие влияющие факторы

Сложность отслеживания исторических данных

Алерт

- Логирование угрозы (МСЭ, конечный узел, почта)

Автоматизированные API Feeds

- Дополнительный контекст события (погода, сбои питания, вирусы, и др.)
- Исторические данные по угрозе

Глобальная аналитика

- FortiGuard Labs
- Исторические данные и действия

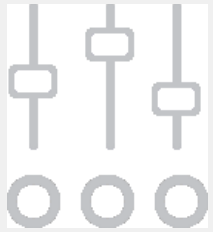
Обогащение

- Уточнение уровня/степени угрозы
- Отсеивание ложных срабатываний
- Передача достоверно определенных угроз

Соразмерная реакция

- Инструменты противодействия
- Расширенное расследование
- Блокировка угрозы на затрагиваемых активах
- Обогащение внутренней Базы знаний для дальнейшего использования

ROI операций обеспечения безопасности



Упорядочение

Оценка

Ускорение

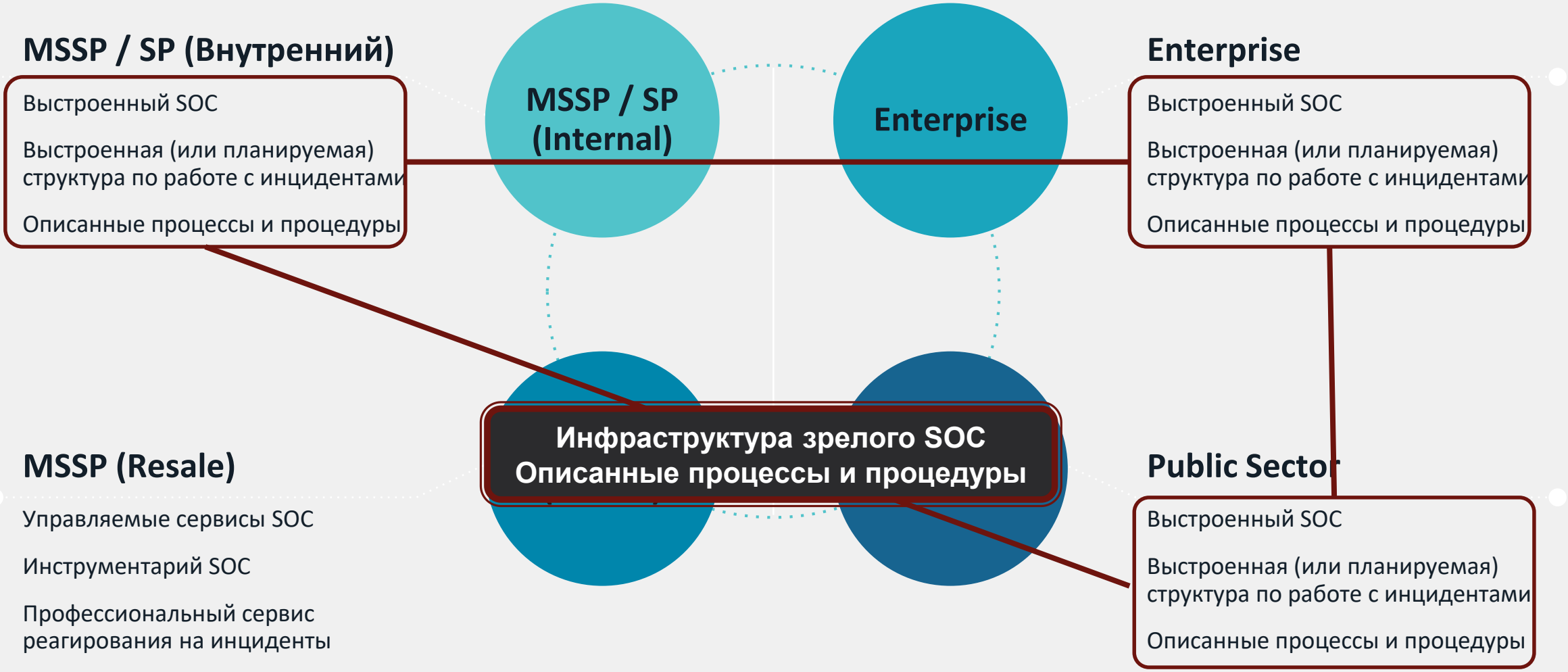
	Время устранения	Кол-во инцидентов/ неделю	Затраченное время В год	Время Сэкономленное (Часы)	Время Сэкономленное (%)	Сохраненные затраты ($150/h)
	45	50	390	0	0%	$0.00
	минуты	Инциденты	часы	часы		
	22	75	190	200	75%	$180,000
	минуты	Инциденты	часы	часы		
	1.4	100	12	378	98%	$472,800
Автоматически	минуты	Инциденты	часы	часы		

Сохраненные затраты

Окно угроз

Усовершенствование SOC с использованием FortiSOAR

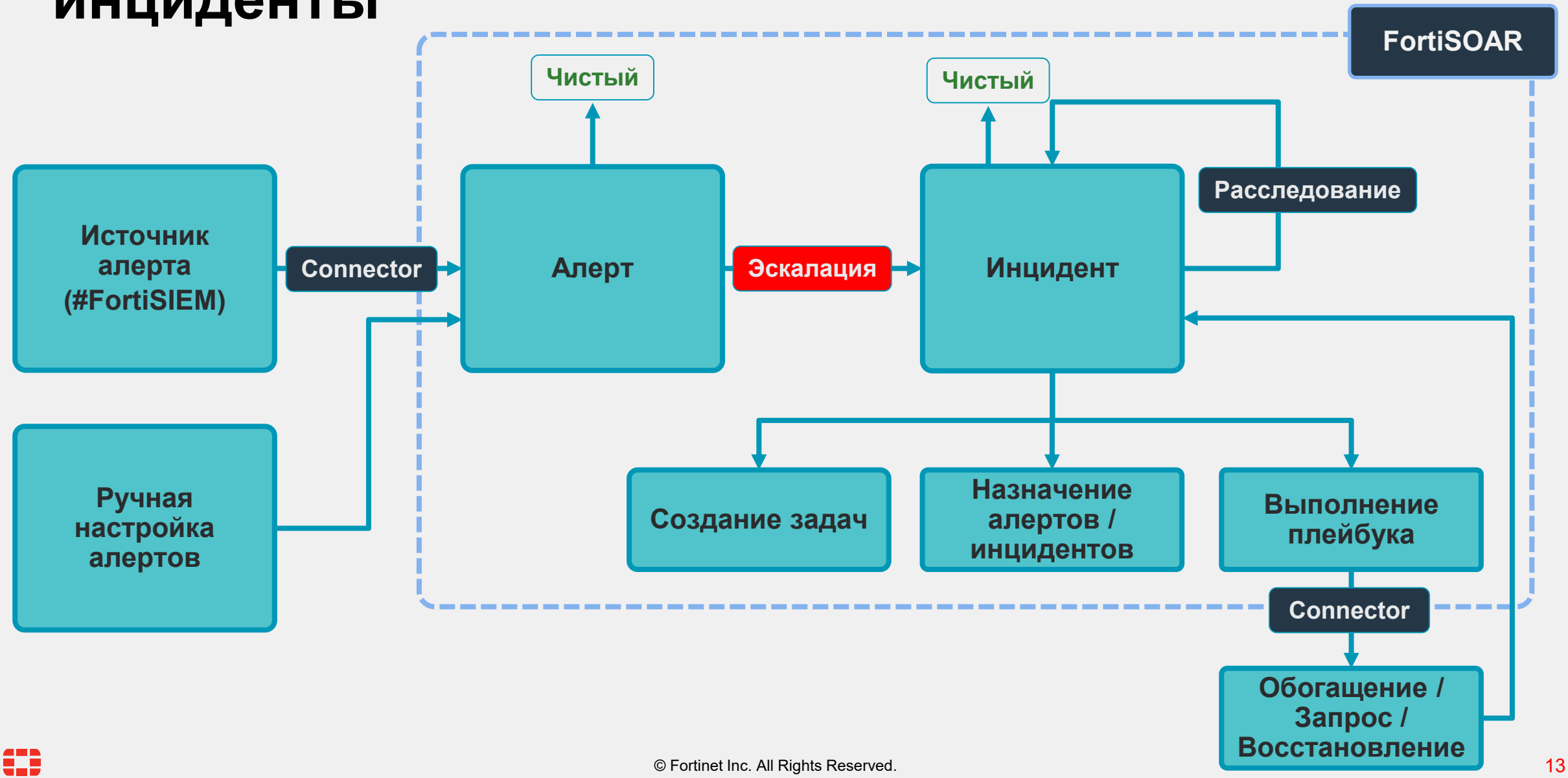
Кто выиграет с SOAR?



Процесс ручного реагирования на инциденты на примере индикатора вредоносного ПО

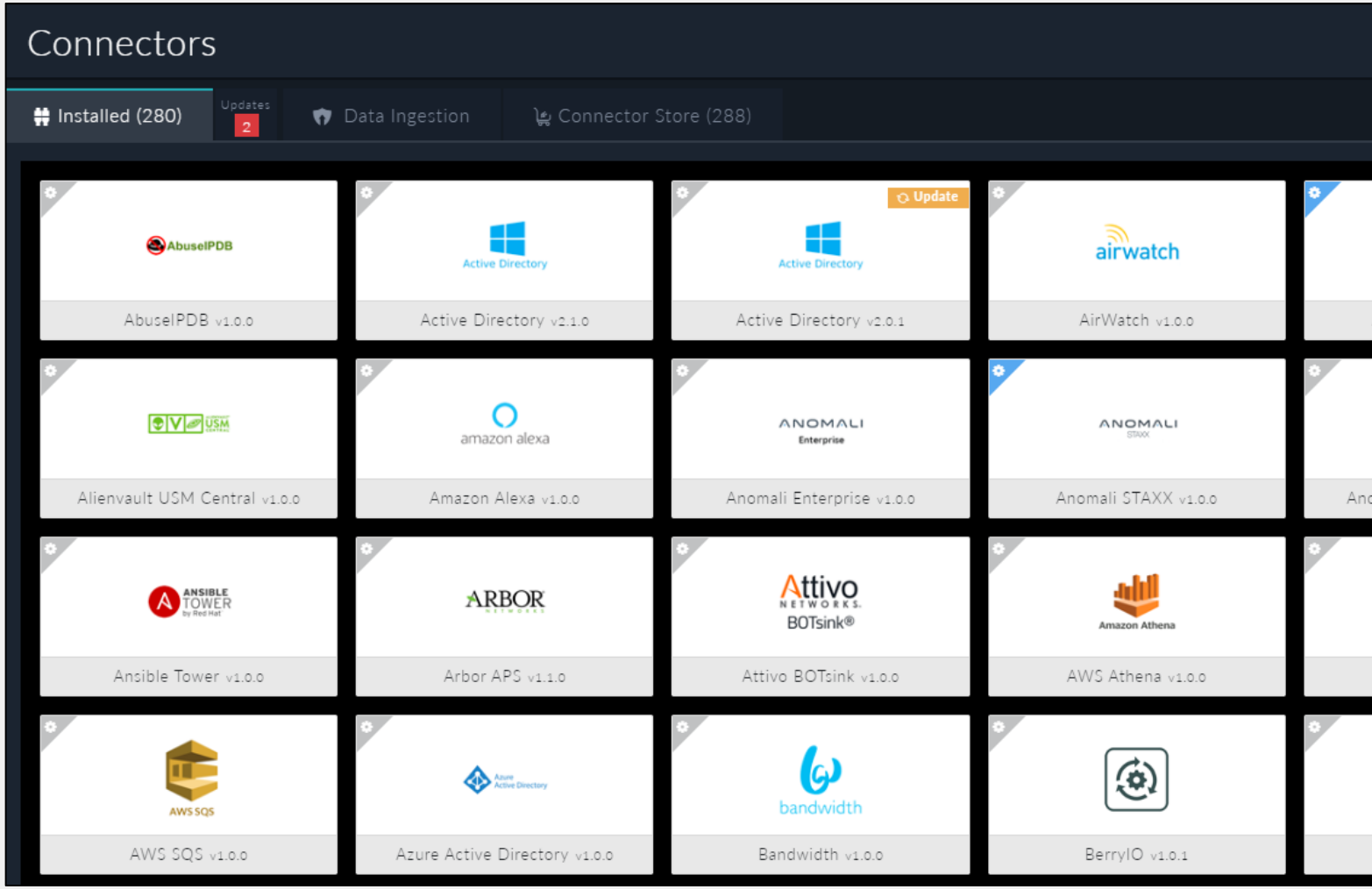
20-30 инцидентов/день

FortiSOAR Тикетинг / Реагирование на инциденты



Коннекторы

- Интеграция с множеством 3rd party
- 250+ коннекторов
- Связность для:
  - Прием данных (Алерты)
  - Действия плейбук
    - Получить объект
    - Отключить аккаунт
    - Получить данные для обогащения
    - и т.д.
- Поддерживается кастомизация
  - Connector SDK



Workbench > Alerts List

rtiSOAR™

DARD

MANAGEMENT

TY ANALYTICS

NT RESPONSE

RTS

IDENTS

KS

ICATORS

MPAIGNS

NTS

ABILITY MANAGEMENT

ATION

RCES

TS

™ 4.12.2-42

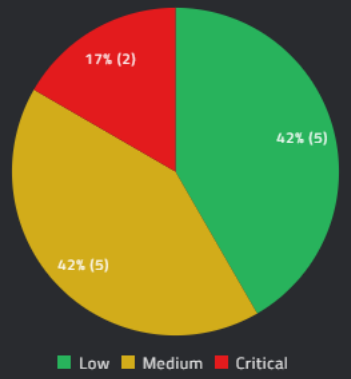
Search

+ QUICK ADD

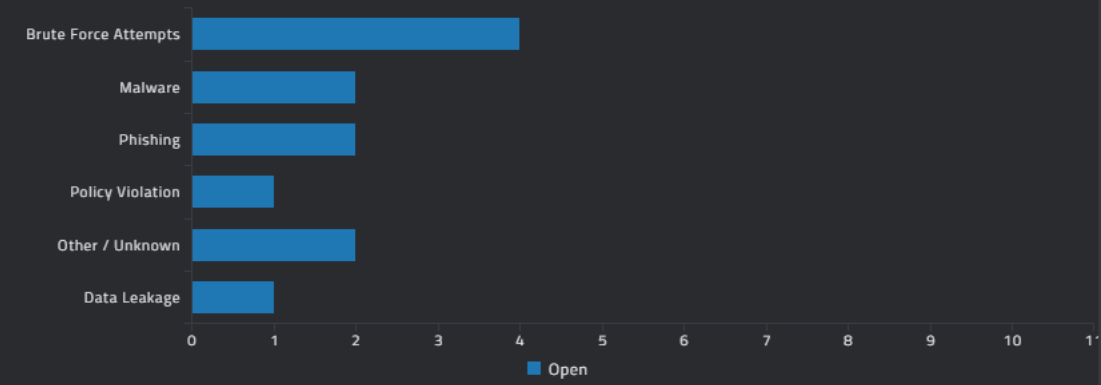
ALERTS

EDIT TEMPLATE

OPEN ALERTS BY SEVERITY



ALERTS BY TYPE



12 Items

+ ADD ALERT

EXECUTE ACTIONS

EXECUTE

Search

ID	SEVERITY	NAME	SOURCE	DUE DATE	TYPE	STATUS	ASSIGNED TO	ESCALATED	KILL CHAIN ...
7947	CRITICAL	Repeated Login Failures on 192.168.50.19	Splunk	03/13/2019 09:...	Brute Force A...	Open	CS Admin	NO	
8049	MEDIUM	AIE: CyberSponse Login Failure	LogRhythm	03/16/2019 09:...	Other / Unkn...	Open	CS Admin		
8037	CRITICAL	Symantec Cloud.SOC -> Policy Violation -> External File Sharing	Symantec Cloud.SOC	03/16/2019 09:...	Data Leakage	Open	CS Admin		
8030	MEDIUM	Symantec ATP Incident :epmp_incident-2018-04-17/incident	Symantec ATP	03/16/2019 09:...	Malware	Open	CS Admin		Exploitation
8017	MEDIUM	Suspicious Email:Urgent: Requesting CEO Level Demo Environment	User Reported	03/16/2019 06:...	Phishing	Open	CS Admin		Delivery
7952	LOW	OutBound Connection - PaloAlto Network Traffic Alert	Splunk	03/13/2019 09:...	Policy Violati...	Open	CS Admin		
7951	LOW	IMAP -WIN-EXCH.cyops.local	Splunk - IMAP	03/13/2019 09:...	Phishing	Open	CS Admin		Delivery
7950	MEDIUM	WIN-EP2 - XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	Splunk	03/12/2019 09:...	Other / Unkn...	Open	CS Admin		
7949	LOW	Repeated Login Failure on Win-EP2	Splunk	03/13/2019 09:...	Brute Force A...	Open	CS Admin		
7948	MEDIUM	Malware Detected on WIN-EP2	Splunk	03/12/2019 09:...	Malware	Open	CS Admin	NO	

Workbench > Alert Details

rtiSOAR™ REPEATED LOGIN FAILUR... VIEW EXECUTED PLAYBOOKS EDIT TEMPLATE COLLABORATE

CRITICAL **ALERT-7947** Repeated Login Failures on 192.168.50.19

Last Modified by CS Admin on 03/11/2019 11:10 PM

Description

Suspicious Login Failures on asset ip-192-168-149-25 from 43.225.46.25

Assigned To	CS Admin	Source	Splunk	Due Date	03/13/2019 09:04 AM
Status	Open	Source ID	343431@343211	Assigned Date	03/07/2019 08:04 AM
Kill Chain Phase	Select	Escalated	NO	Resolved Date	--

TYPE DETAILS

Type	Brute Force Attempts	Source IP	43.225.46.25	Target Asset	ip-192-168-149-25
		Destination IP	--	Source Port	--

OBSERVABLES | RELATED RECORDS | TASKS | SOURCE DATA | ACCESS CONTROL | AUDIT LOG

1 Items + ADD INDICATOR LINK INDICATORS EXECUTE ACTIONS EXECUTE Search

TYPE	REPUTATION	VALUE	STATUS	TAGS	KILL CHAIN PHASE
Select	Select	Search	Select	Search	Select
IP Address	MALICIOUS	43.225.46.25	TBD		

Description

11

Detected URLs: 100

VirusTotal

Location Map:

ESCALATE RESOLVE EXECUTE EDIT RECORD EXPORT DELETE

PLAYBOOK

Investigating Potential Brute Force Alert
- Originating from: **43.225.46.25**
- Target asset: **ip-192-168-149-25**

ABOUT 2 HOURS AGO

PLAYBOOK

Source IP **43.225.46.25** is External

ABOUT 2 HOURS AGO

PLAYBOOK

VirusTotal Reports **43.225.46.25** to be Malicious with an aggregated score of 11

ABOUT 2 HOURS AGO

PLAYBOOK

Queried Splunk, and found same SourceIP: 43.225.46.25 attempted to log in on following **5** systems
- LinEp31
- LinEp41
- LinEp51
- LinEp61
- LinEp71

ABOUT 2 HOURS AGO

PLAYBOOK

In addition, login to following systems were successful:
- LinEp71

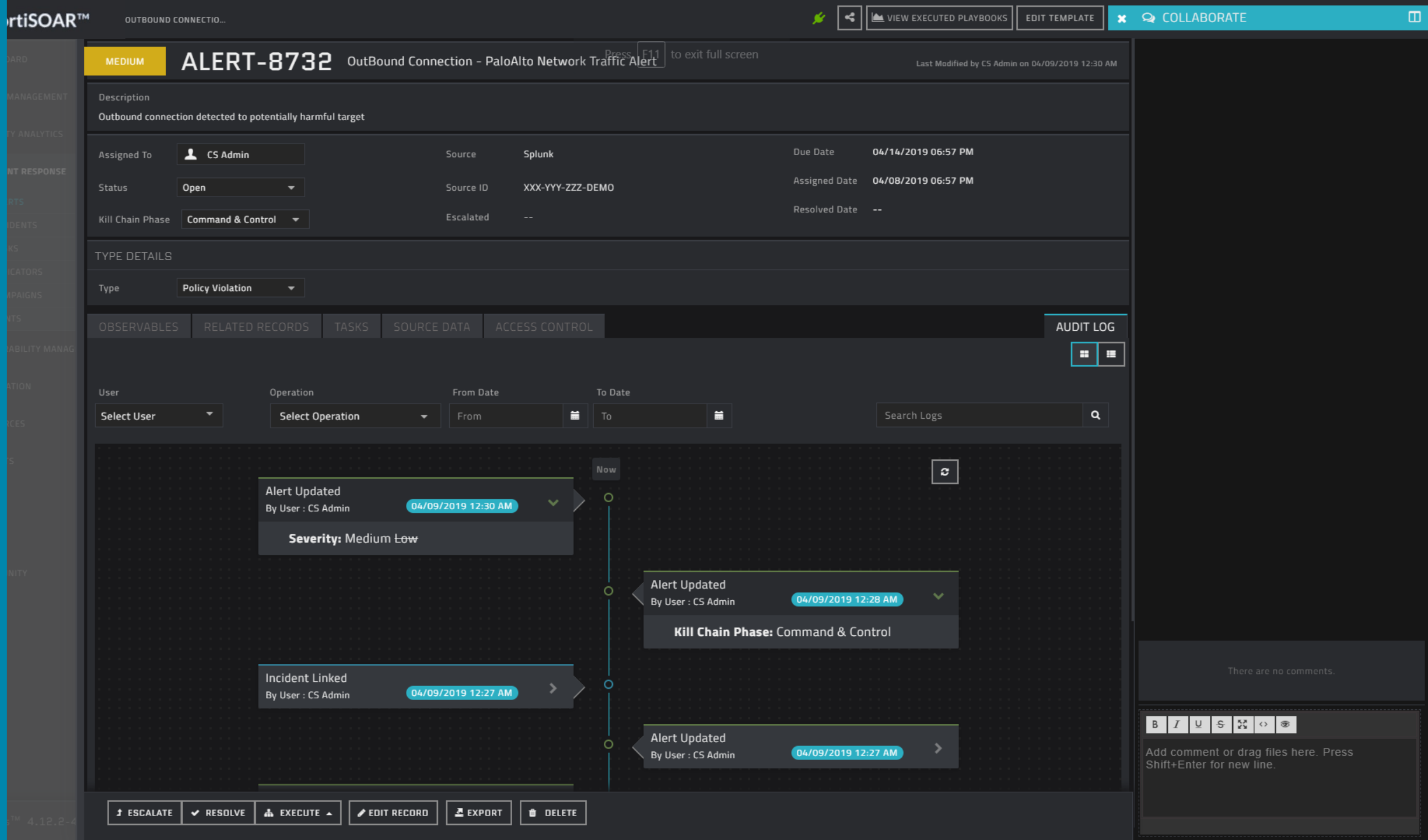
This is an Indication of Breach

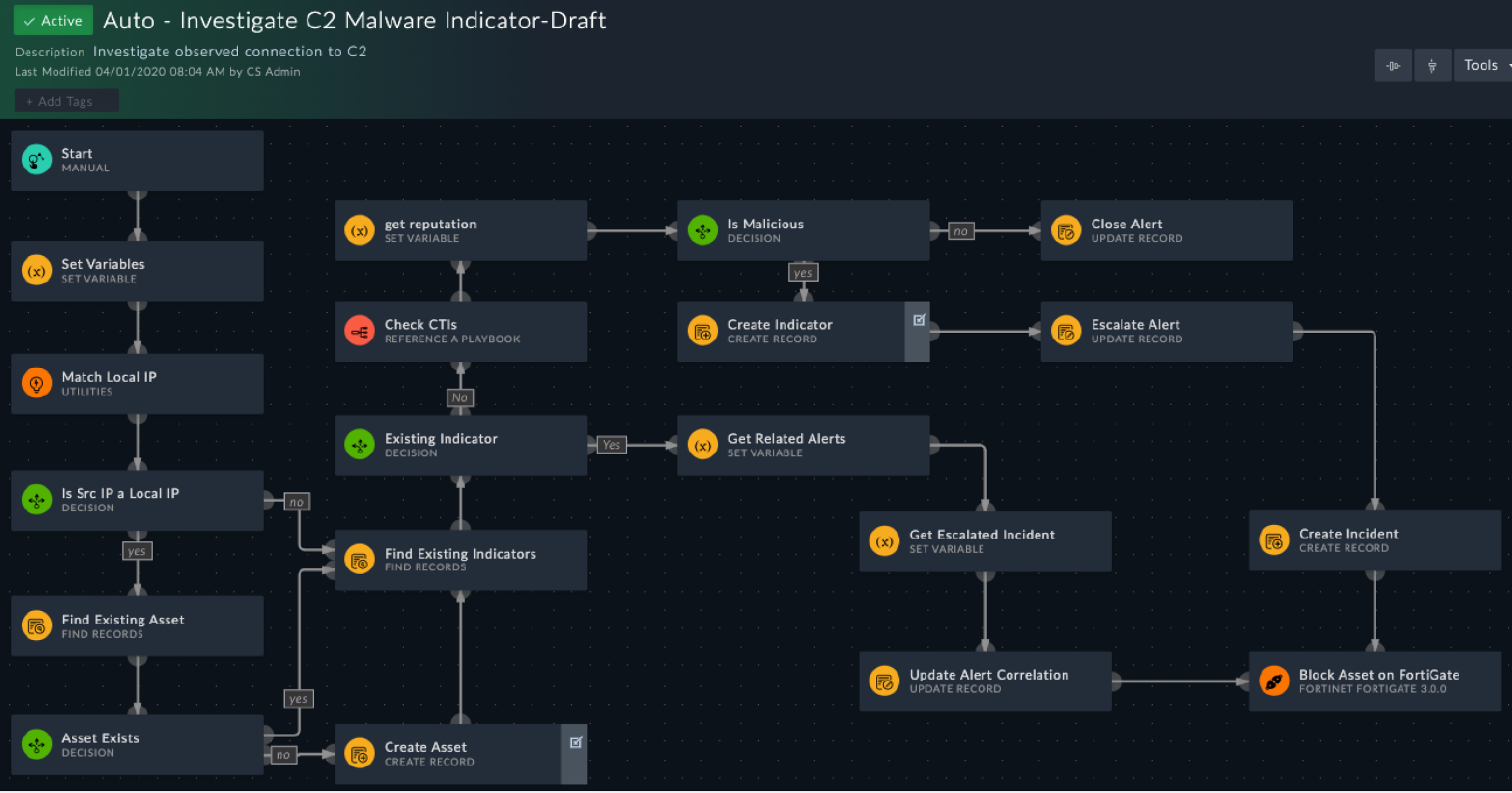
ABOUT 2 HOURS AGO

B I U S

Add comment or drag files here. Press Shift+Enter for new line.

Audit Logs


rtiSOAR™
OUTBOUND CONNECTIO...
VIEW EXECUTED PLAYBOOKS
EDIT TEMPLATE
COLLABORATE
Press F11 to exit full screen
MEDIUM
ALERT-8732
OutBound Connection - PaloAlto Network Traffic Alert
Last Modified by CS Admin on 04/09/2019 12:30 AM
Description
Outbound connection detected to potentially harmful target
Assigned To
CS Admin
Status
Open
Kill Chain Phase
Command & Control
Source
Splunk
Source ID
XXX-YYY-ZZZ-DEMO
Escalated
--
Due Date
04/14/2019 06:57 PM
Assigned Date
04/08/2019 06:57 PM
Resolved Date
--
TYPE DETAILS
Type
Policy Violation
OBSERVABLES
RELATED RECORDS
TASKS
SOURCE DATA
ACCESS CONTROL
AUDIT LOG
User
Select User
Operation
Select Operation
From Date
From
To Date
To
Search Logs
Now
Alert Updated
By User : CS Admin
04/09/2019 12:30 AM
Severity: Medium ~~Low~~
Alert Updated
By User : CS Admin
04/09/2019 12:28 AM
Kill Chain Phase: Command & Control
Incident Linked
By User : CS Admin
04/09/2019 12:27 AM
Alert Updated
By User : CS Admin
04/09/2019 12:27 AM
There are no comments.
Add comment or drag files here. Press Shift+Enter for new line.
ESCALATE
RESOLVE
EXECUTE
EDIT RECORD
EXPORT
DELETE



Workbench > Incident

rtiSOAR™ | IT: MALWARE EXPLOITED | VIEW EXECUTED PLAYBOOKS | EDIT TEMPLATE | COLLABORATE

HIGH **INCIDENT-8063** Malware Exploited

Last Modified by Playbook on 03/11/2019 11:35 PM

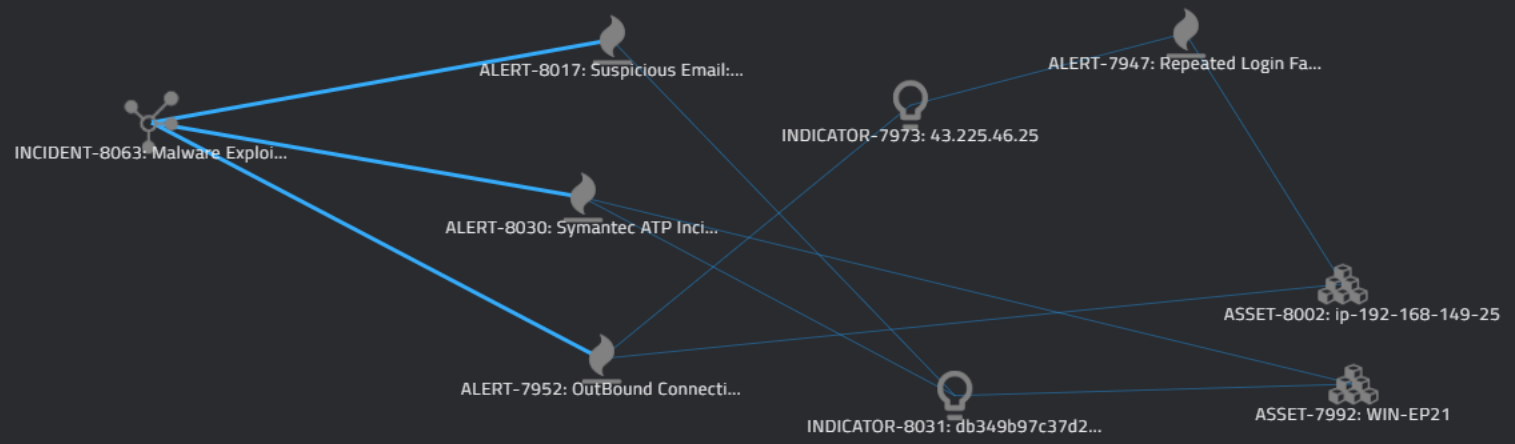
Phase

Detection | Identification | Confirmation | Containment | Eradication | Recovery | Aftermath

Description

Splunk Alert For PaloAlto Network Traffic policy violation.

Correlation Graph



Incident Lead: CS Admin

Status: Open

Source: Paloalto

Campaign: Dummy Campaign

Phase: Containment

SLA

Created On: 03/11/2019 11:22 PM

Date Of Incident: 03/10/2019 12:00 AM

Discovered Date: 03/12/2019 12:00 AM

Resolved Date: --

TYPE DETAILS

Type: Other

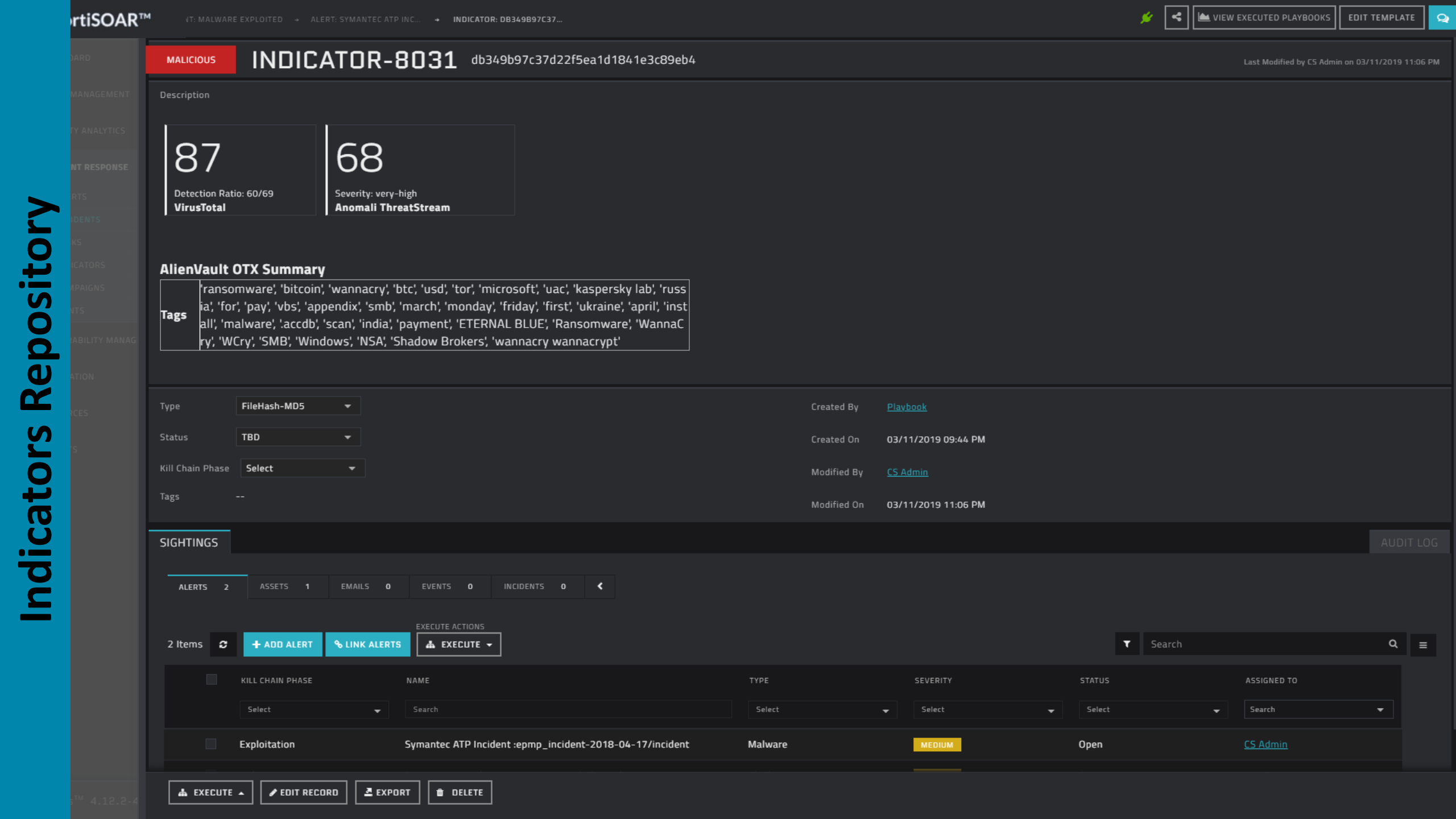
OBSERVABLES | RELATED RECORDS | TASKS | ATTACHMENTS | ACCESS CONTROL | AUDIT LOG

EXECUTE ACTIONS

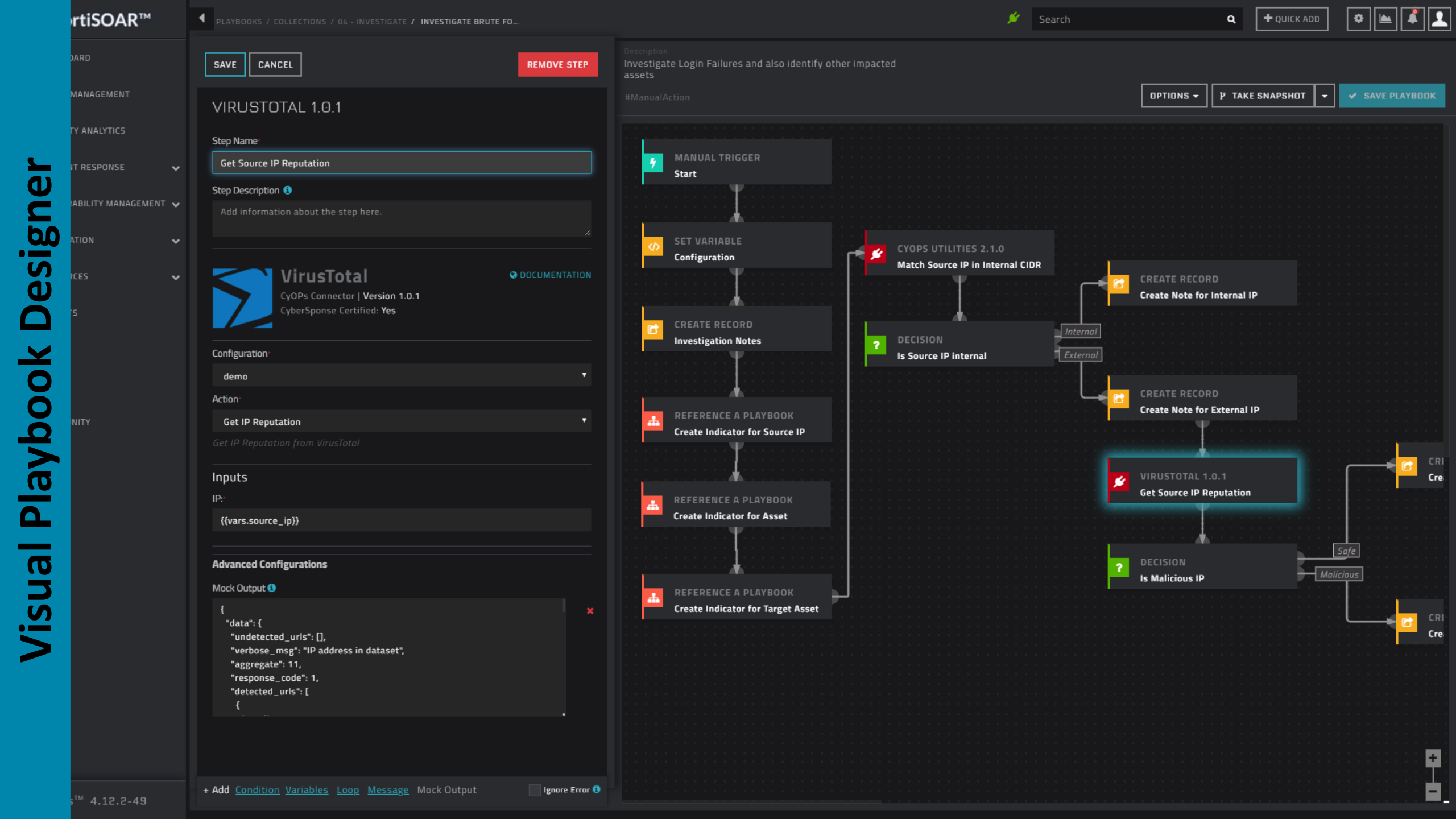
GENERATE INCIDENT SUMMARY REPORT | EXECUTE | EDIT RECORD | EXPORT | DELETE

CS ADMIN
Requesting Block IP for 43.225.46.25
LESS THAN A MINUTE AGO

Visual Correlation:
full view of Incident to Alerts to Assets to Vulnerabilities to Users


Indicators Repository
rtiSOAR™
VIEW EXECUTED PLAYBOOKS
EDIT TEMPLATE
MALICIOUS
INDICATOR-8031
db349b97c37d22f5ea1d1841e3c89eb4
Last Modified by CS Admin on 03/11/2019 11:06 PM
Description
87
Detection Ratio: 60/69
VirusTotal
68
Severity: very-high
Anomali ThreatStream
AlienVault OTX Summary
Tags
'ransomware', 'bitcoin', 'wannacry', 'btc', 'usd', 'tor', 'microsoft', 'uac', 'kaspersky lab', 'russ ia', 'for', 'pay', 'vbs', 'appendix', 'smb', 'march', 'monday', 'friday', 'first', 'ukraine', 'april', 'inst all', 'malware', '.accdb', 'scan', 'india', 'payment', 'ETERNAL BLUE', 'Ransomware', 'WannaC ry', 'WCry', 'SMB', 'Windows', 'NSA', 'Shadow Brokers', 'wannacry wannacrypt'
Type
FileHash-MD5
Status
TBD
Kill Chain Phase
Select
Tags
--
Created By
Playbook
Created On
03/11/2019 09:44 PM
Modified By
CS Admin
Modified On
03/11/2019 11:06 PM
SIGHTINGS
AUDIT LOG
ALERTS 2
ASSETS 1
EMAILS 0
EVENTS 0
INCIDENTS 0
EXECUTE ACTIONS
2 Items
+ ADD ALERT
LINK ALERTS
EXECUTE
Search
KILL CHAIN PHASE
NAME
TYPE
SEVERITY
STATUS
ASSIGNED TO
Exploitation
Symantec ATP Incident :epmp_incident-2018-04-17/incident
Malware
MEDIUM
Open
CS Admin
EXECUTE
EDIT RECORD
EXPORT
DELETE

Visual Playbook Designer



Role Based Dashboards

rtiSOAR™

DARD

MANAGEMENT

TY ANALYTICS

T MANAGEMENT

ABILITY MANAGEMENT

ATION

RCES

MANAGEMENT

TS

4.11.1-468

Search

+ QUICK ADD

cS

DASHBOARD

EXECUTIVE VIEW

TOTAL ALERTS RESOLVED

30 1,400%

In Last 15 Days

ALERTS ESCALATION RATIO

37.2% 37%

In Last 15 Days

AUTOMATED ACTIONS RUN

467220 5,083%

In Last 15 Days

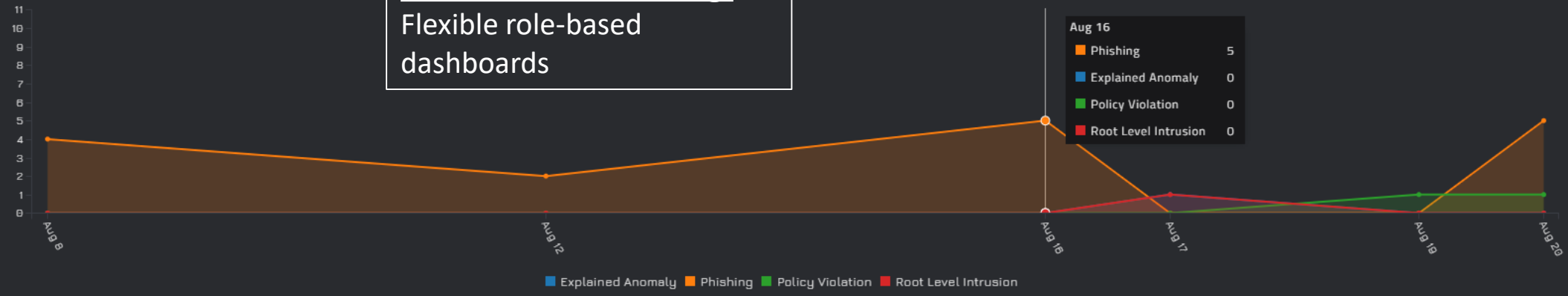
ROI

$2,336,100 5,083%

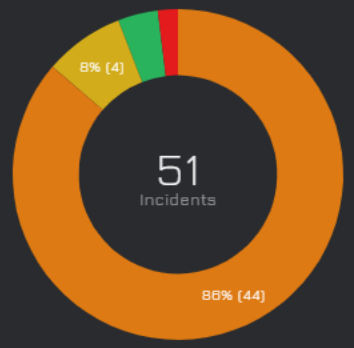
In Last 15 Days

INCIDENTS TIMELINE

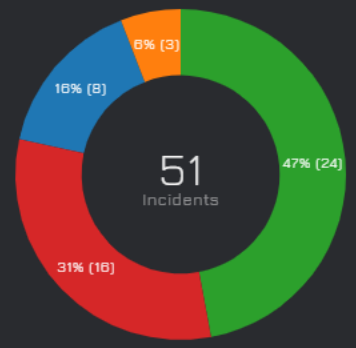
Real-Time Monitoring:
Flexible role-based dashboards



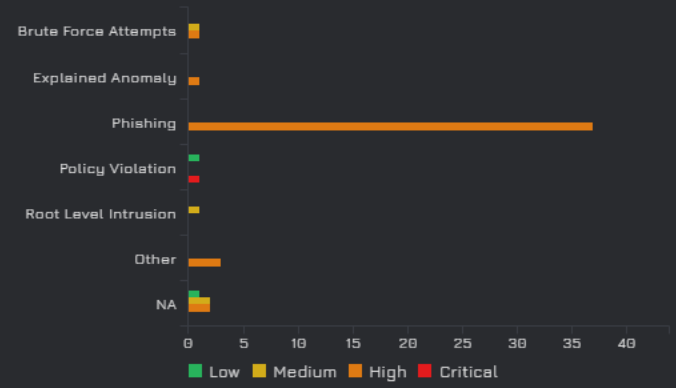
UNRESOLVED INCIDENTS BY SEVERITY



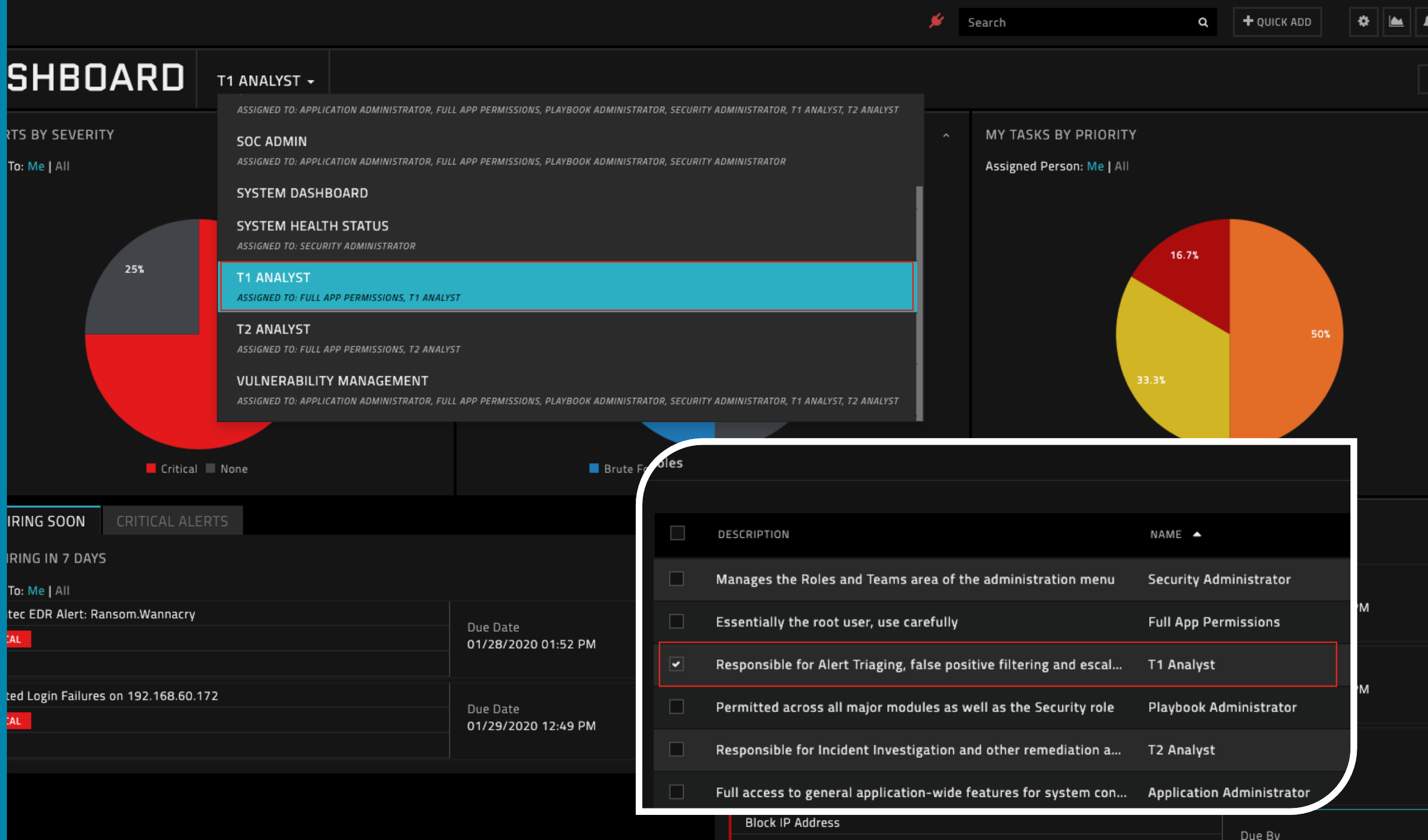
UNRESOLVED INCIDENTS BY PHASE



UNRESOLVED INCIDENTS BY TYPE



Tiered Process



Custom Modules

TION EDITOR / MODULES

Search

+ QUICK ADD

PLICATION EDITOR

Configuration

g

Manager

MANAGEMENT

erarchy

es

ication

ION EDITOR

on

MODULES

Last published: 9 days ago

REVERT ALL

PUBLISH ALL MODULES

Select a module to edit or create new module

+ Create new module

REVERT

SAVE

SUMMARY | FIELDS EDITOR

Type, Table Name, Singular Name & Plural Name cannot be modified, once it is saved

Type *

Table Name *

Singular Name *

Plural Name *

Display Template *

Ownable

Trackable

Record Uniqueness

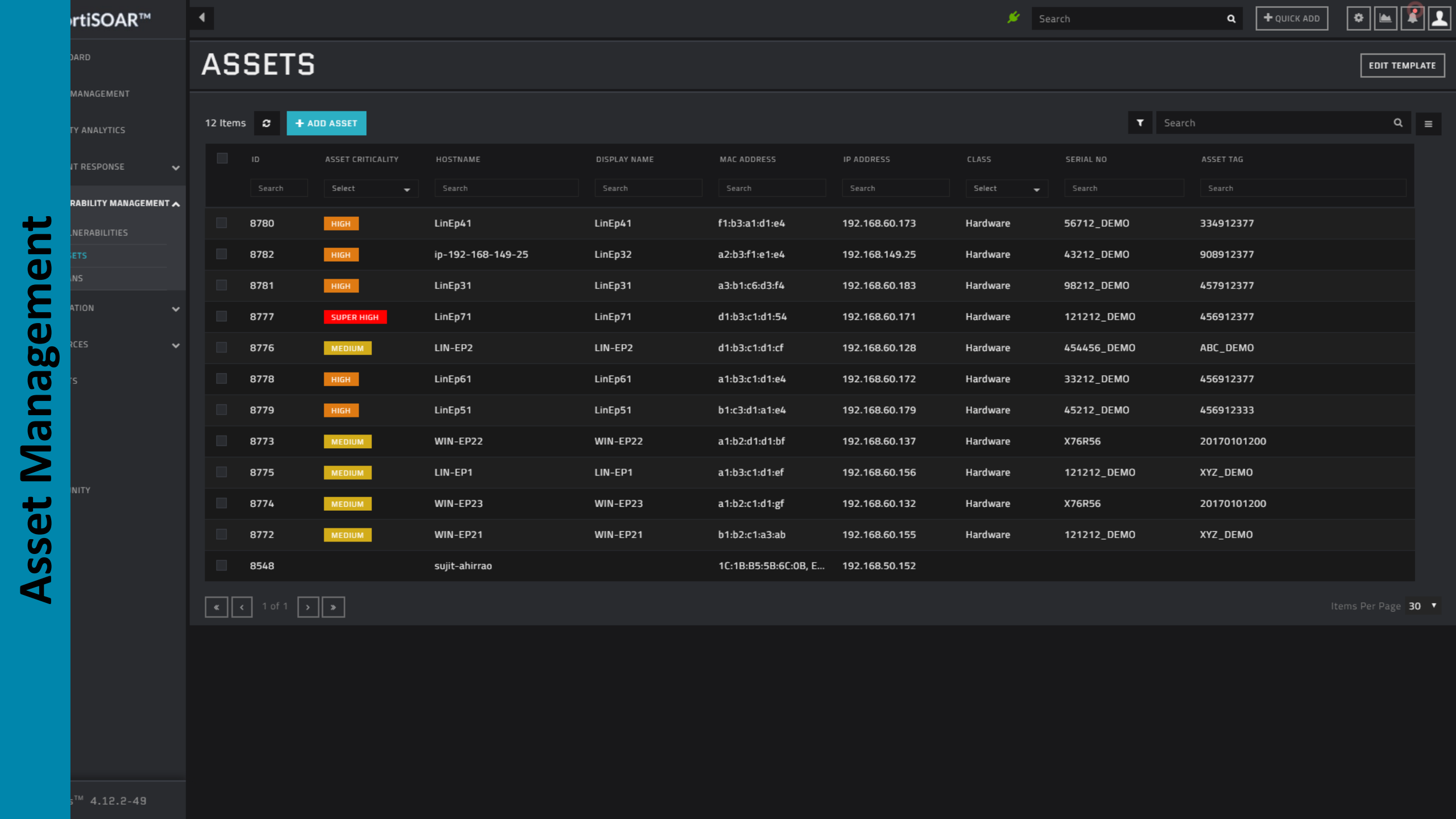
Choose from one or more existing module fields to define a composite unique condition. For e.g. combination of 'Name' and 'Source ID' will ensure no other records with same combination can be created.

Select a field

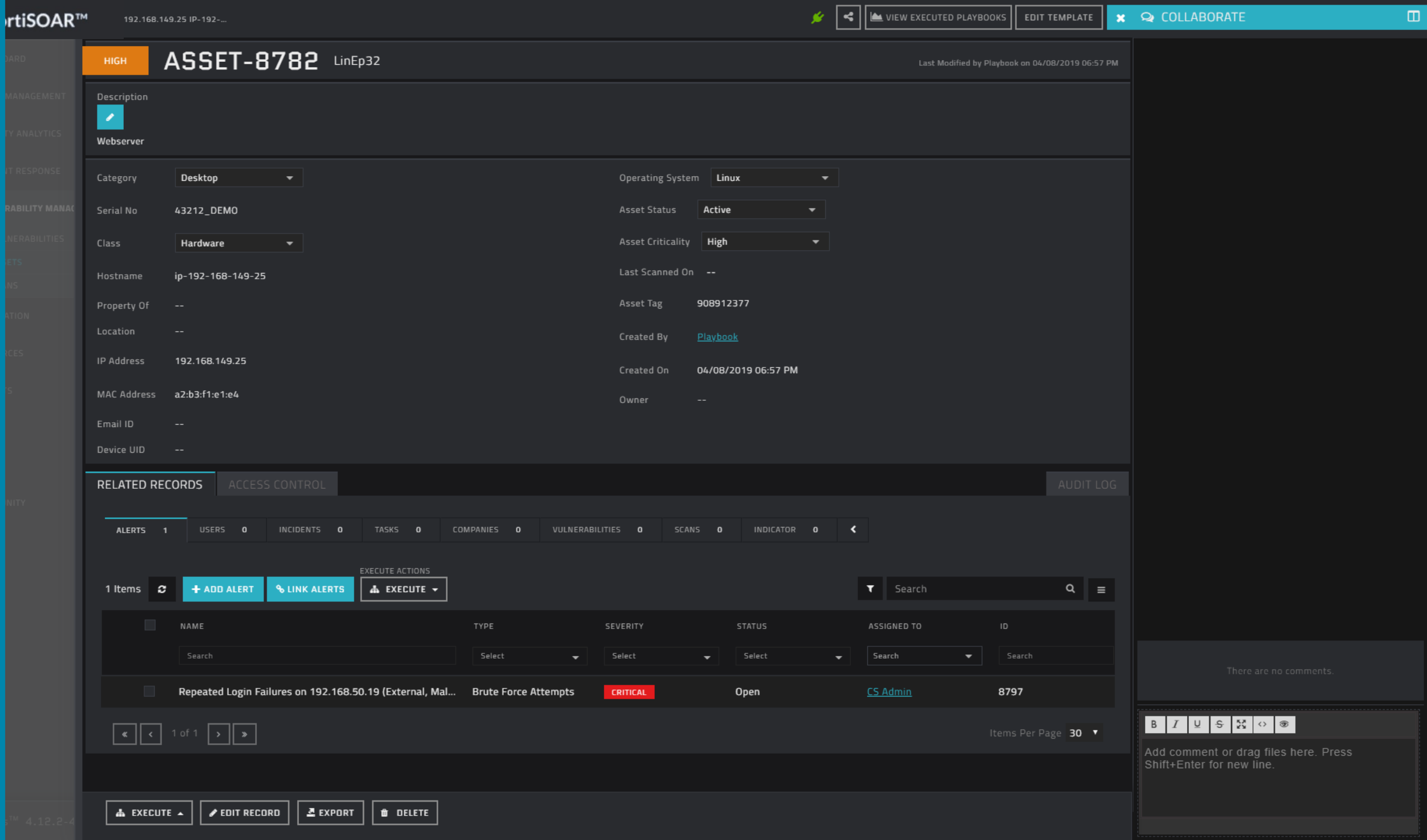
Default Sort

Add field to set as default sort.

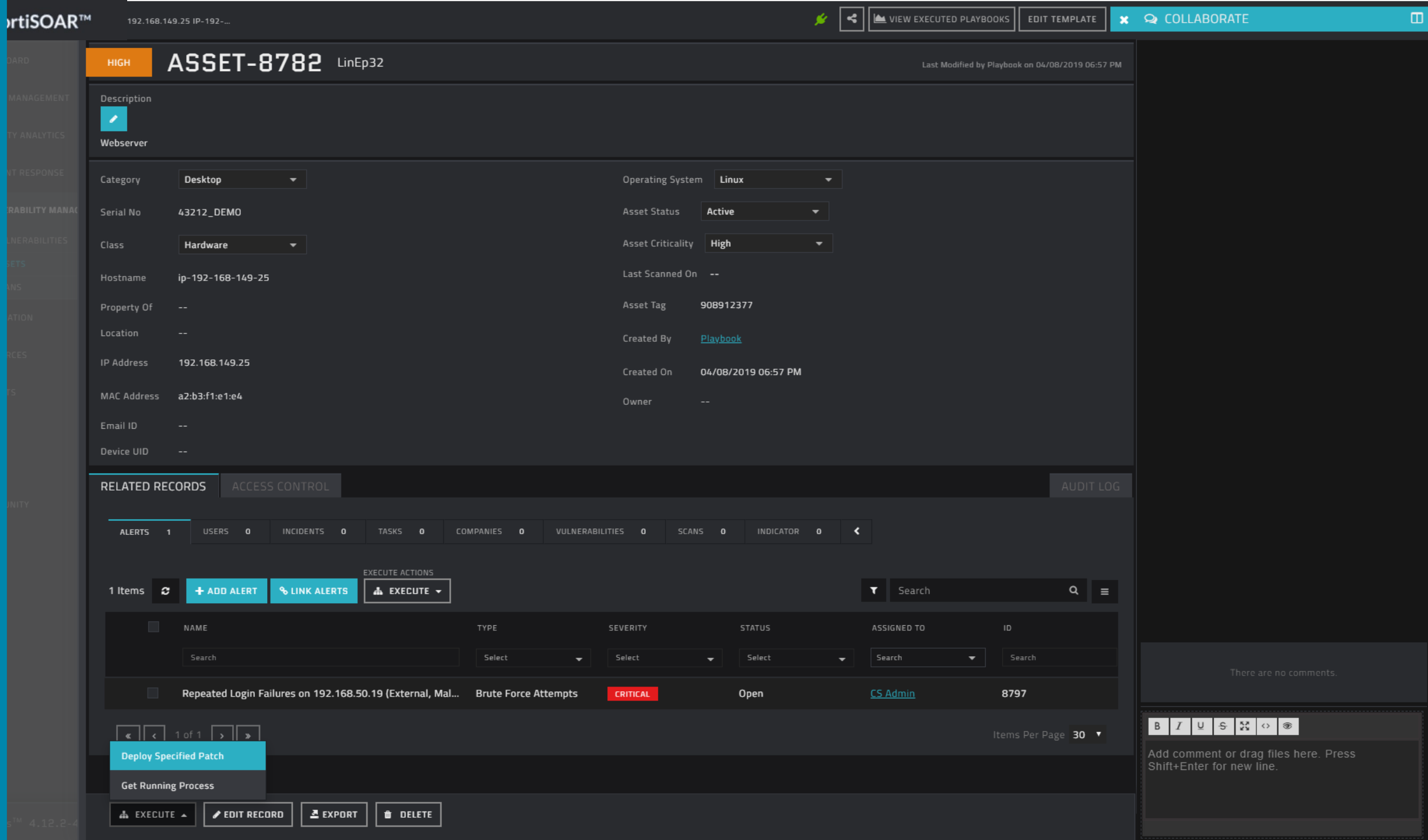
Asset Management



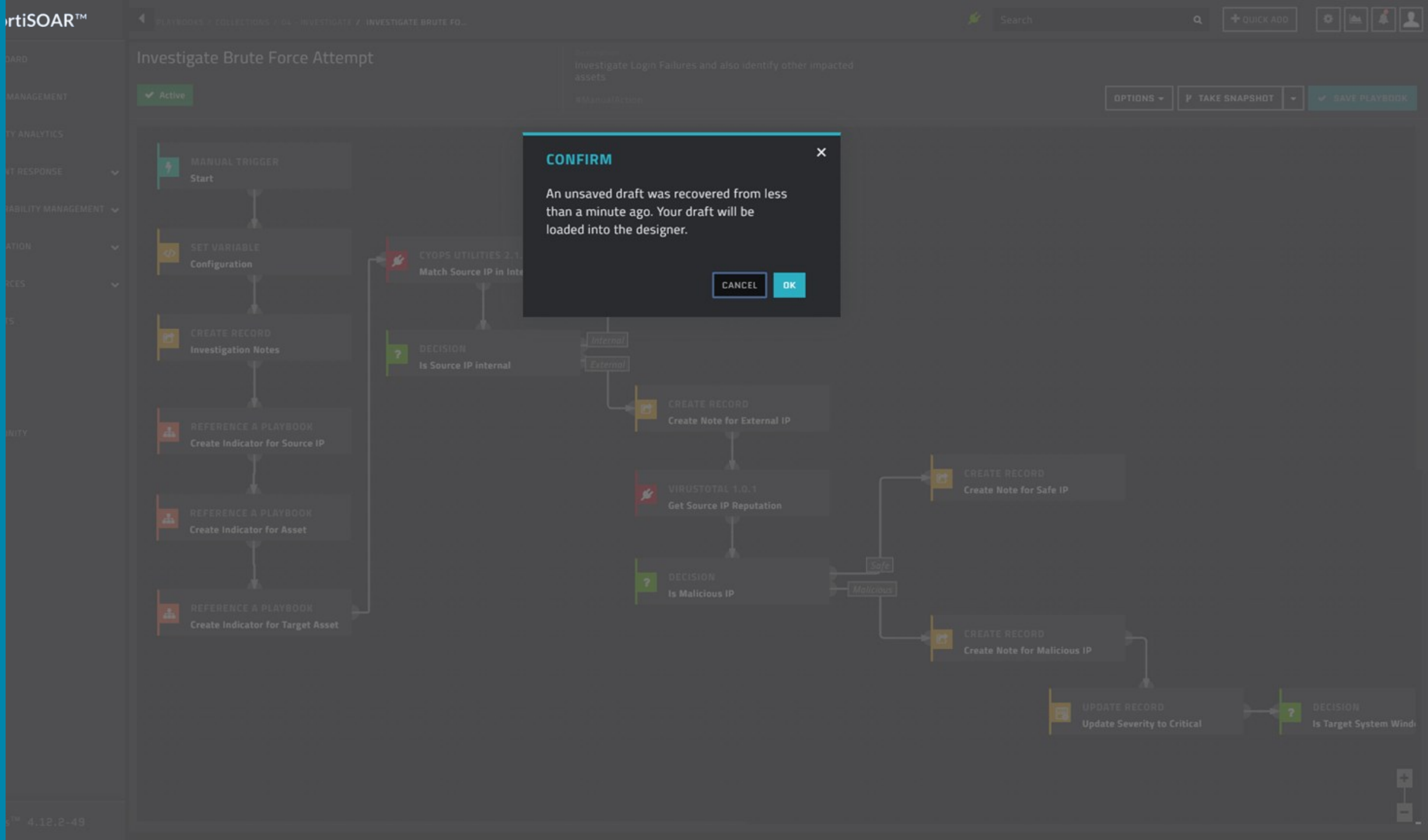
Asset Details



Asset Patching

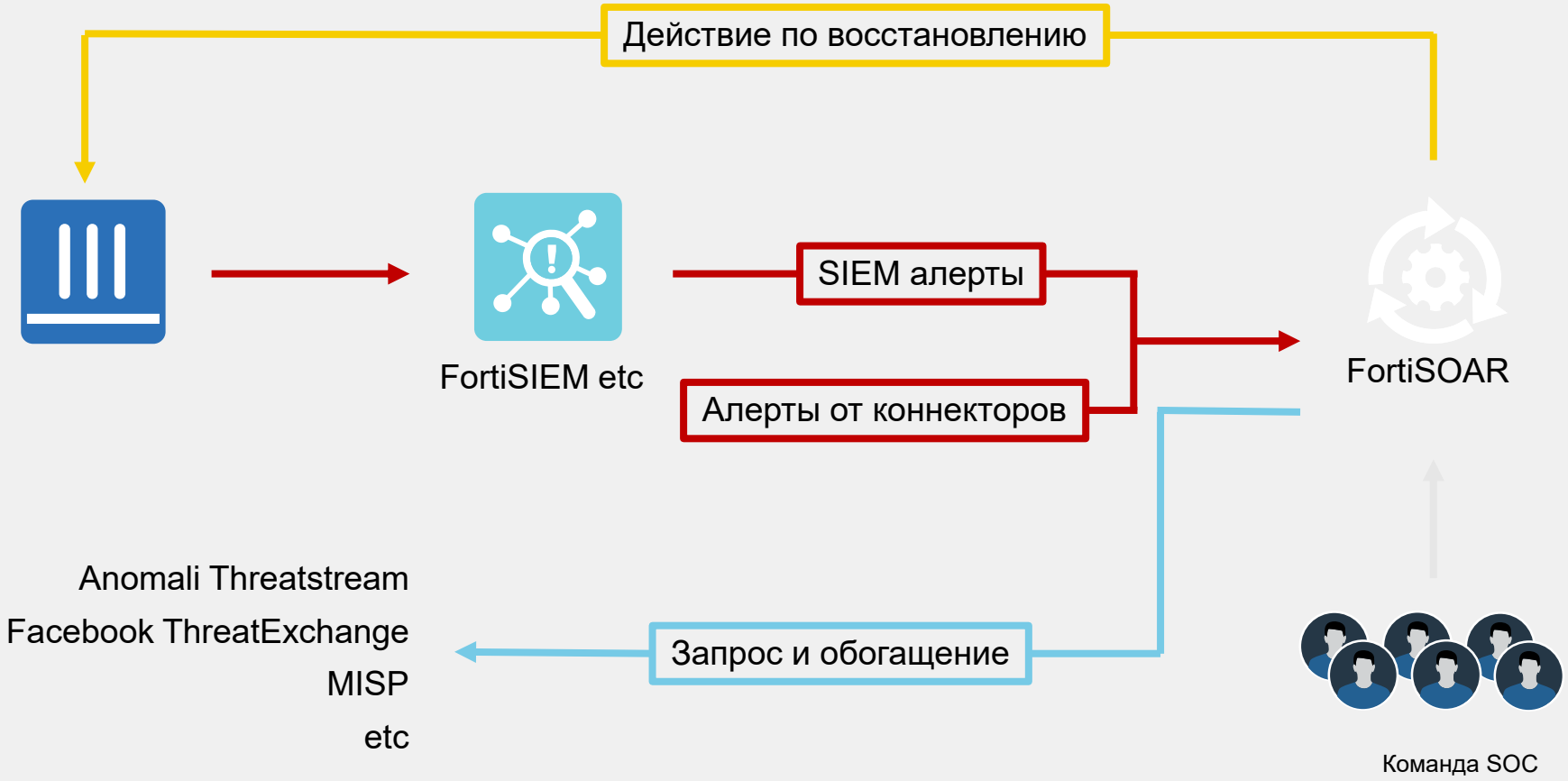


GUI Resilience & Input Control



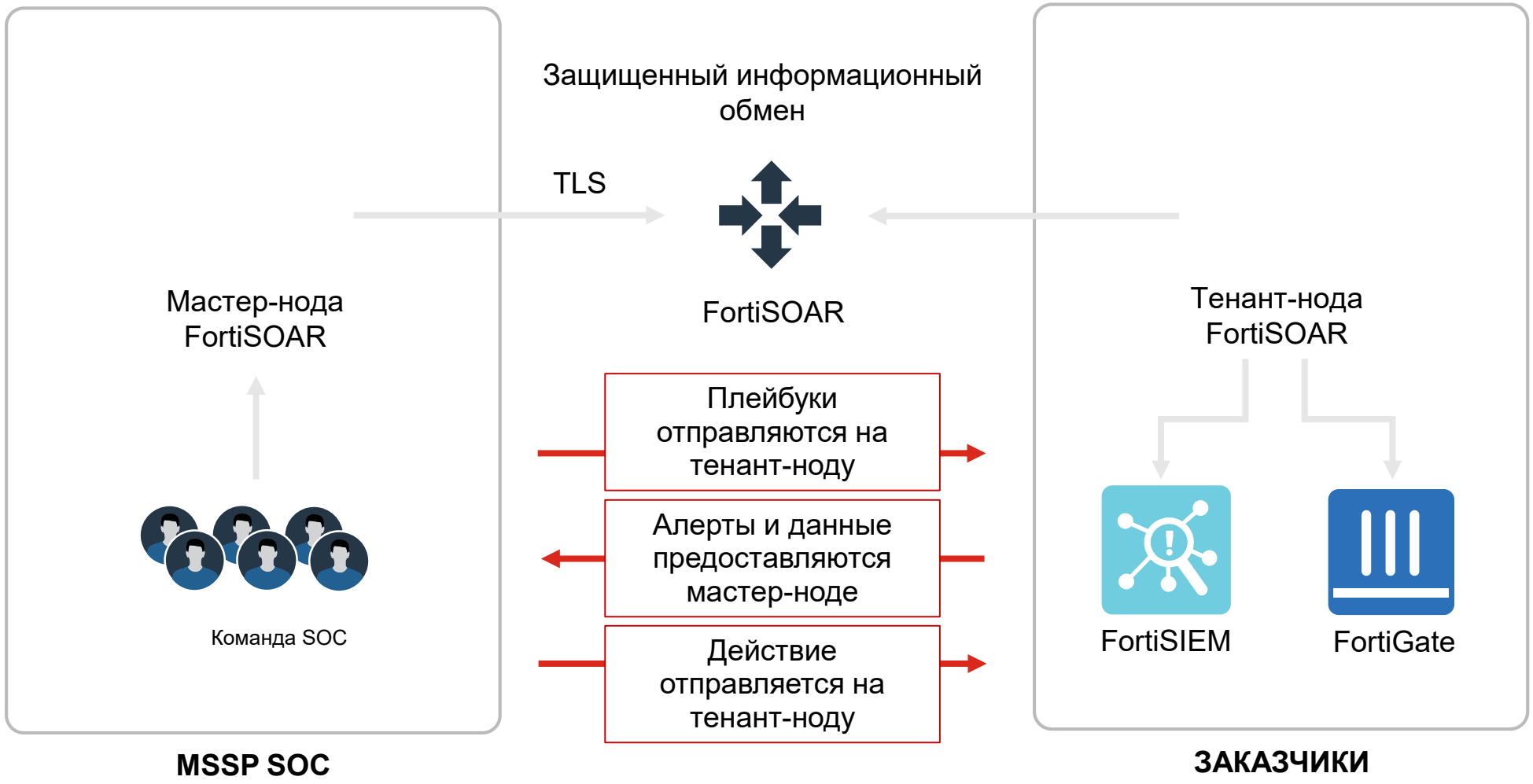
Архитектура

Типовая enterprise архитектура



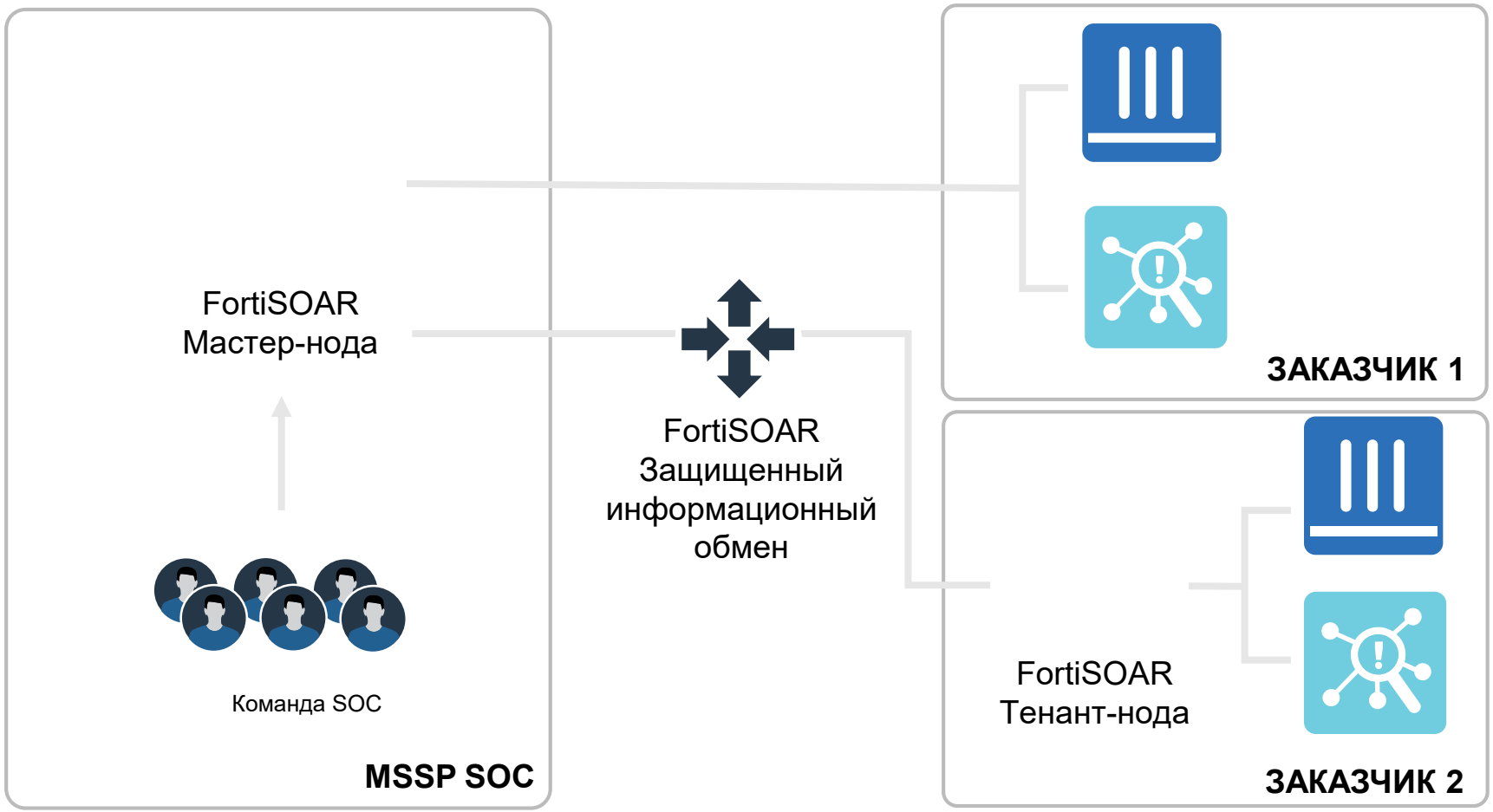
Мультитенантная архитектура с разделяемыми тенантами

Мультиненантная архитектура с распределенными тенантами



Мультитенантная архитектура с гибридной мультитенантностью

Совмещение и использование разделяемой или распределенной архитектуры в зависимости от требований



Заказчик 1

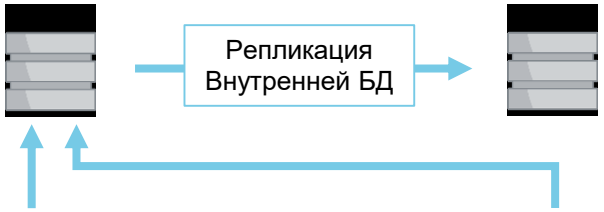
Центральное управление

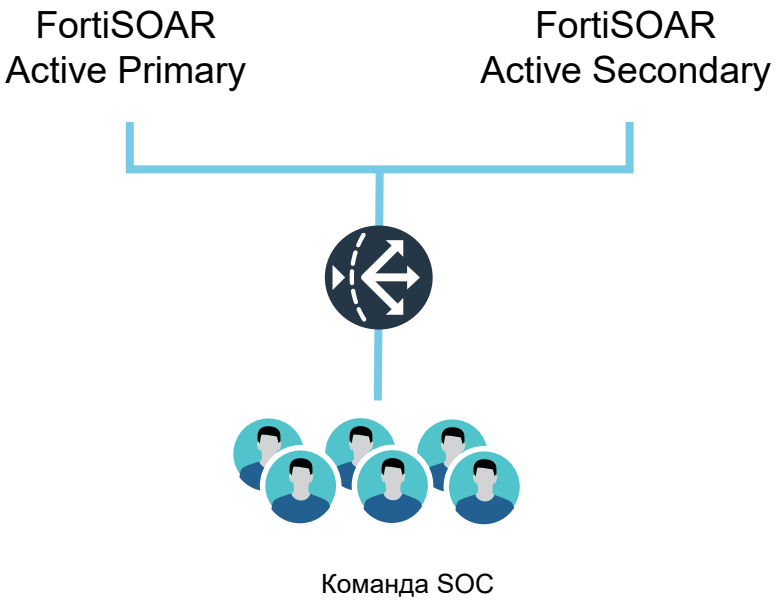
Заказчик 2

Распределенные ноды

Обеспечение высокой доступности и кластеризация

Высокая доступность и кластеризация для надежности и масштабируемости

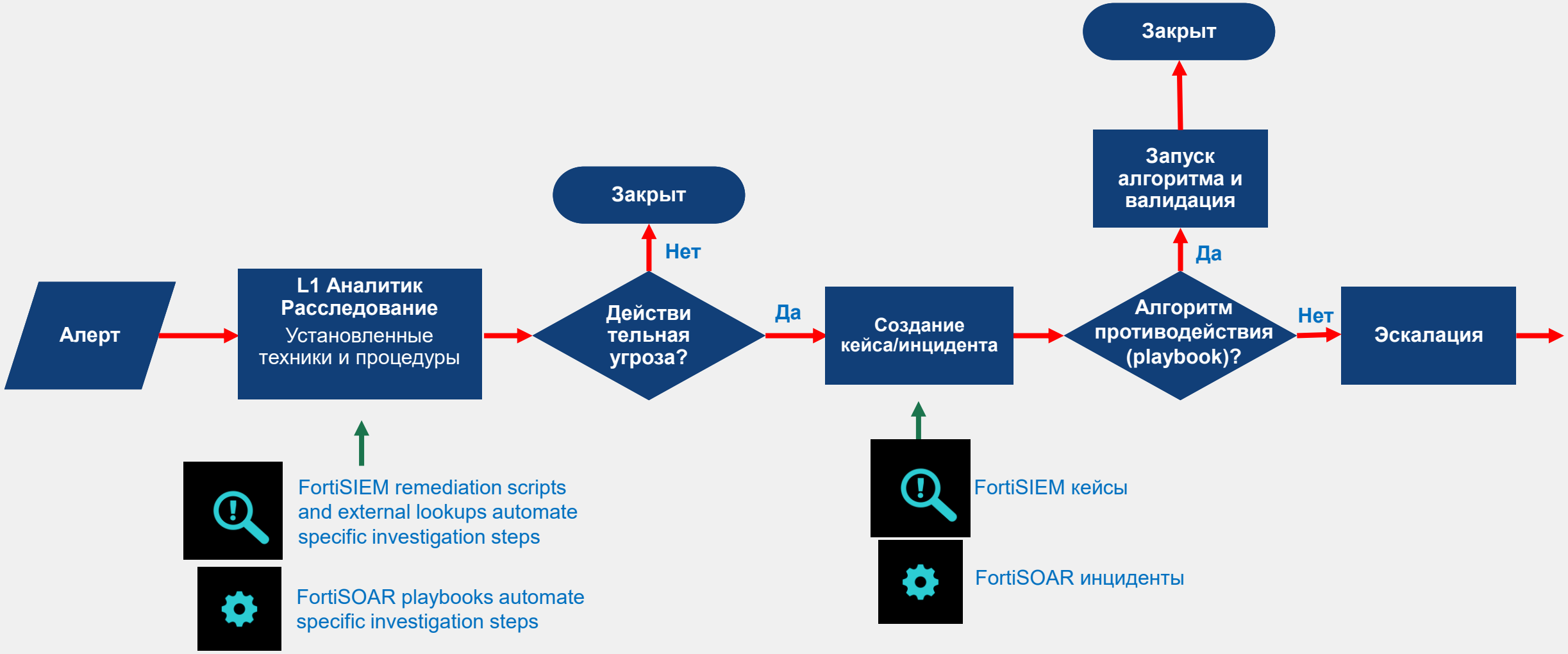




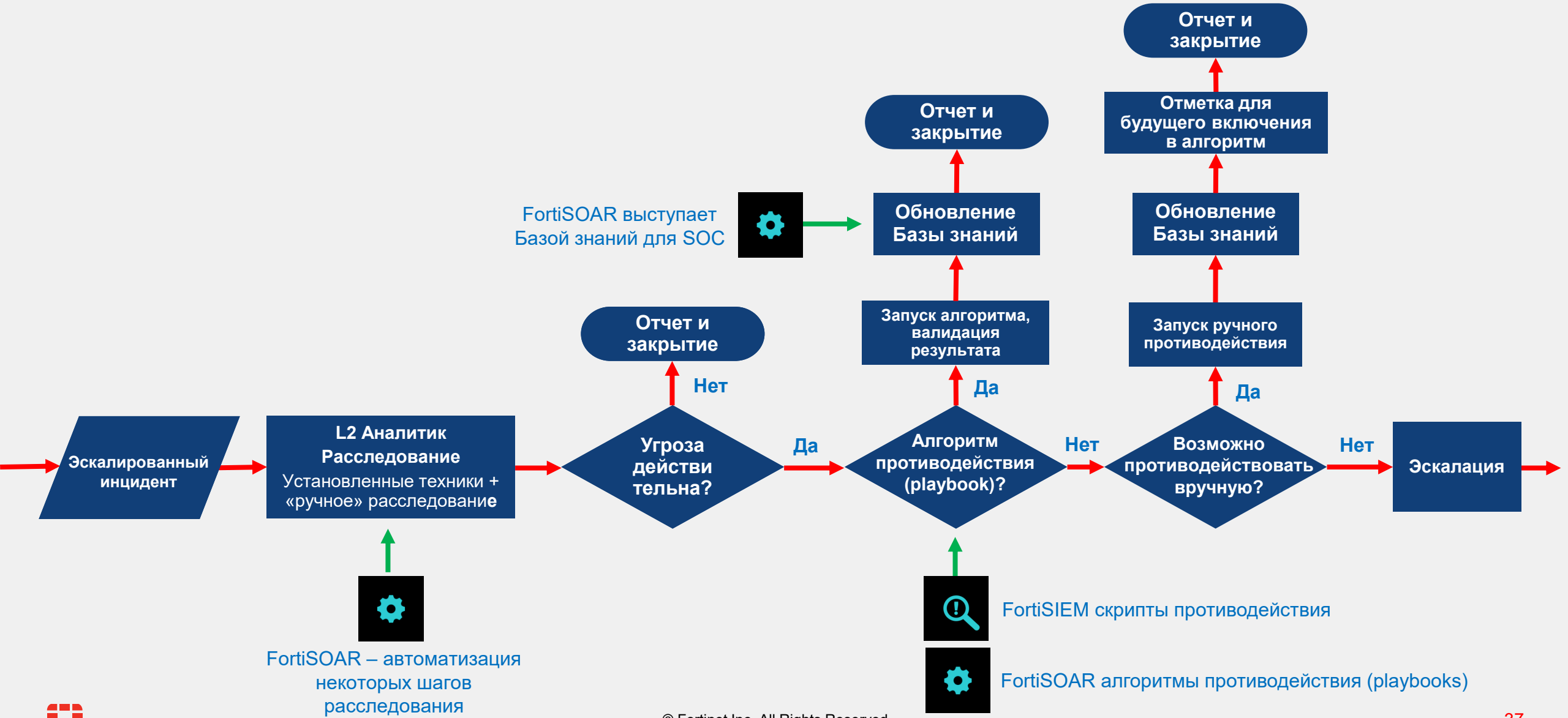
- Active – Passive для надежности
- Active – Active для надежности и масштабируемости
  - Требуется использование балансировщика
- Поддержка внутренней и внешней базы данных
- Поддержка нескольких Secondary узлов
  - Требуется лицензия (HA license)

Логика работы с событиями/алертами

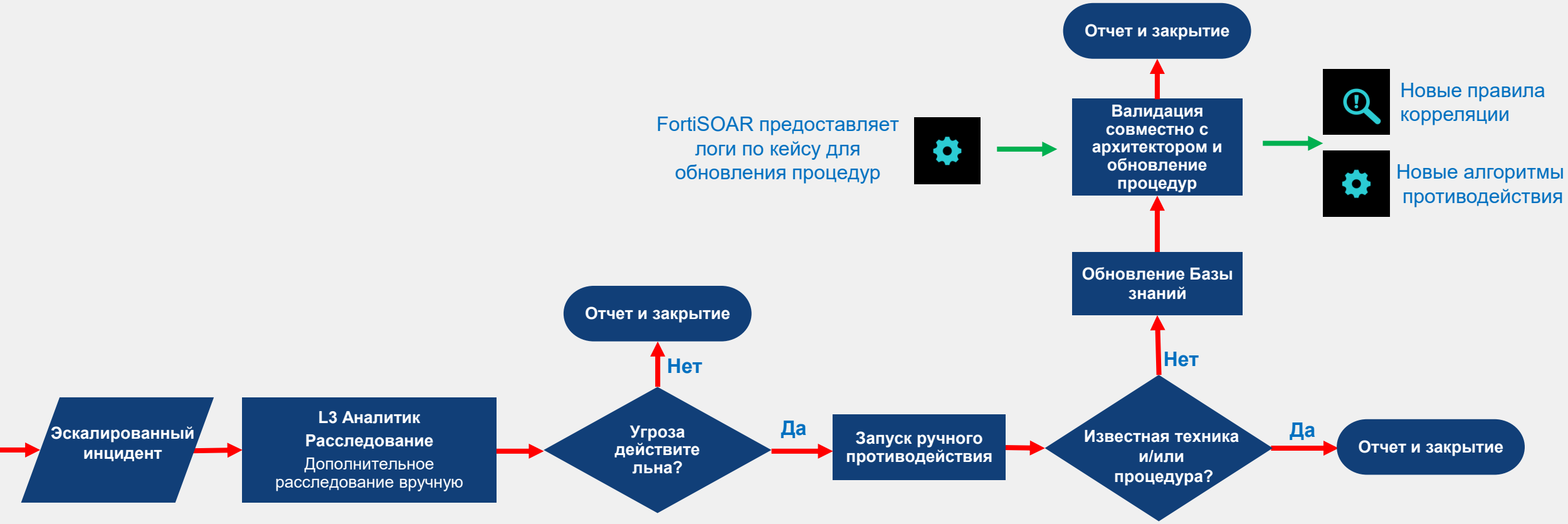
SOC: обработка событий и реагирование – L1



SOC: обработка событий и реагирование – L2

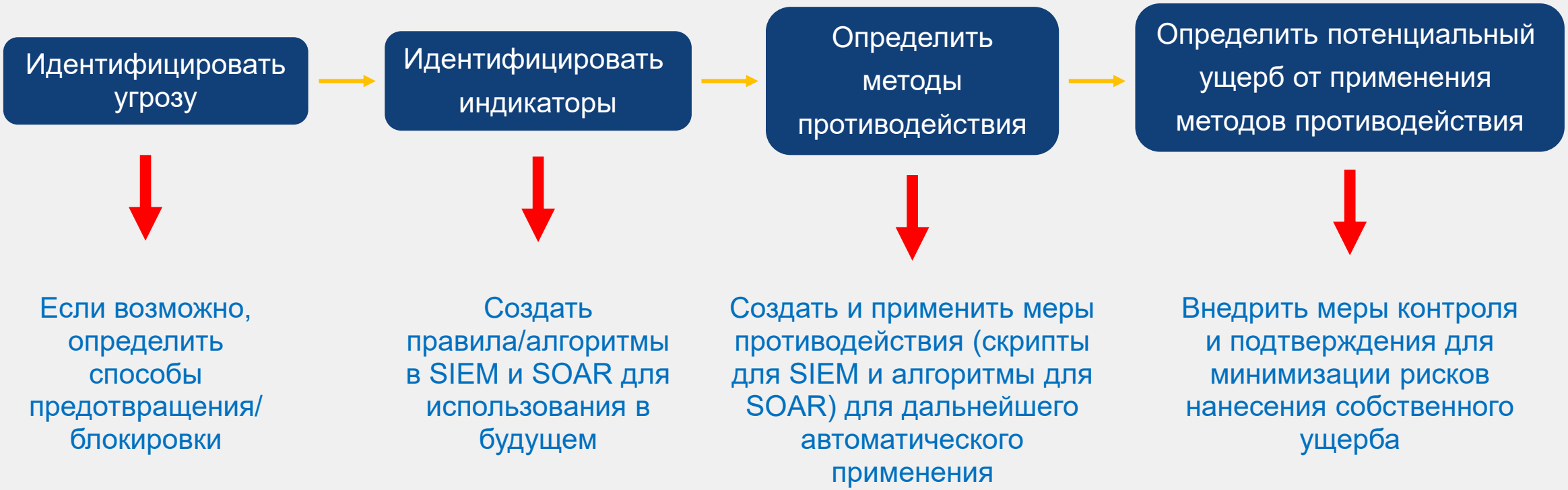


SOC: обработка событий и реагирование – L3



Замечание: могут потребоваться дополнительные действия, такие как обновление правил корреляции, политик МСЭ, патчинг конечных узлов и т.п.

FortiSOAR: новая техника или процедура



Особенности

Основные особенности FortiSOAR

Продвинутое управление кейсами
SOAR + IR + VM + Legal + Custom Modules + Dashboards and Reporting

Поддержка сложных сценариев ролевого доступа
Data Partitioning (Horizontal and Vertical), Playbook, Dashboard

Упрощенный редактор плейбуков
250+ Connectors, Simulation, Debugger

Масштабируемая архитектура
Active/Active HA, Distributed Multi-Tenancy

Упрощенное лицензирование
Предсказуемое лицензирование на базе пользователей

Преимущества FortiSOAR

Q&A


FORTINET