socautomation™

IBM QRadar

TREND MICRO TippingPoint

Orchestrating and Automating Trend Micro TippingPoint and IBM QRadar

HONEYCOMB

SOCautomation™

Incident Response Automation

SOCAutomation is an information security automation and orchestration platform that transforms incident response. It enables organisations to clearly define what constitutes an incident and then clearly communicates the process to handle it throughout the company and if necessary, across third parties. It uses a methodology based on the SANS 6 steps to incident response.

Orchestration

Instrumentation of existing security investment – auto-detection and generation of out-of-the-box SANS best-practice Run-Book procedures that are superimposed back to the business.

Automation

Fully automate, semi-automate, or control automate some, most or all of the orchestration procedures.

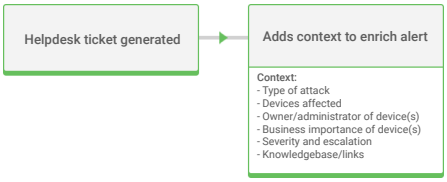
FlowLanes™ Overview

Using the data collected from your infrastructure and security solutions combined with an extensive knowledgebase, SOCAutomation is able to issue relevant 'Run-Books' to all stakeholders when an incident has been detected. These Run-Books are then generated and graphically represented to the relevant stakeholders using our advanced FlowLanes™ engine. With the information provided by these Run-Books, stakeholders know how best to deal with any incident related to them, or assets they own. It also allows security teams to track incident response from start to finish by offering a visualised workflow detailing every step in the remediation process. The following is a simplified outline of how we generate these Run-Books:

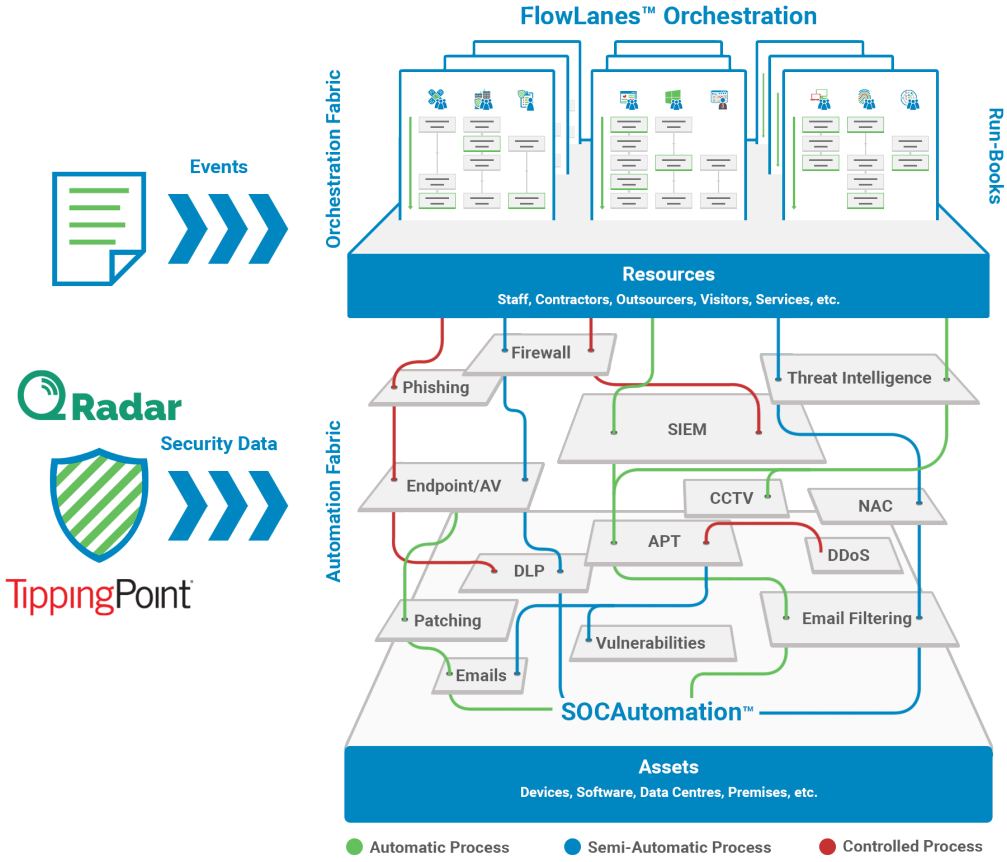
Alert comes in - incident automatically generated in SOCAutomation platform. → In parallel, an incident Run-Book is automatically generated → Incidents are assigned to the necessary stakeholders, based on incident type, asset, department, customer, etc. → Within these automatically assigned Run-Books, each person/department has their own lane → Each cell within FlowLanes™ contain specific tasks, due dates, and knowledgebase articles detailing how to respond to the incident → An email-based alerting system is able to send incident and task updates to all the people involved

FlowLanes™ Automation

SOCAutomation uses a unique state based automation engine that gives users full control over the level of automation in each Run-Book generated. Not only are you able to automate SOCAutomation tasks, you are also able to automate tasks performed by other security products on your network. Each cell can create automation tasks and workflows, all tightly controlled and state mapped. An example of task automation is shown on the right.



Architectural Overview



Automation is utilised throughout the platform in 4 areas:

Incident Response Automation
- Run-Book tracking
- Point automation
- State change tracking
- Audit tracking
- Ticketing integration

Remediation Automation
- Call-out to 3rd party remediation
- Fully customisable
- Building block library
- Status and stream support

Triage Automation
- Incident detection
- Analysis and normalisation
- False positive and filtering
- Severity and escalation

Context Automation
- Asset mapping
- Stakeholders and assignments
- Business context
- Security context
- Run-Book generation

Orchestrating and Automating IBM QRadar and Trend Micro TippingPoint

Product Overview

- Fully featured SIEM solution from IBM
- Rich data correlation – events, flows, packet data, threat intelligence, vulnerability data and patch data
- Extensive threat library powered by IBM XForce
- Unequalled implementation, support and training services
- Multi-tenanted, highly scalable and resilient

Product Overview

- Next generation IPS and ATP solution from Trend Micro
- Monitors malware in a safe, controlled and sandboxed environment
- In the case of malware penetrating and successfully infiltrating the network, the detection technology identifies the suspicious behaviour and informs the user
- Comprehensive threat intelligence
- Protection for current and zero-day vulnerabilities and exploits

IBM QRadar Integration

IBM QRadar is the Gartner leading SIEM solution and enables organisations to monitor sophisticated cyber attacks in real-time. When combined with SOCAutomation, QRadar becomes an automated Security Operation Centre, making SOC operations delivery a reality. SOCAutomation utilises QRadar's API's covering offenses, asset data, vulnerability data and X-Force threat intelligence feeds. QRadar offenses typically give: Severity, IP address(es) of targeted device, short description (e.g. excessive firewall denies) and offense category.

Context we add includes:

- **Mapping Offenses to Assignees:** e.g. level 1 analyst for offense type X, level 2 for offense type Y etc.
- **Stakeholder Mapping:** Who needs to be included 'in the loop', e.g. SOC Manager
- **Security Context:** Add offense-specific knowledgebase content – e.g. links to details about a given type of malware
- **Business Context:** Add business-specific knowledgebase content – e.g. links to regulatory company policy on dealing with malware, DLP, phishing etc.
- **IP Address -> Username Mapping:** Shows who has been logged on to a machine leading up to a breach (uses Lexicon for this)
- **Automated Process Initiation:** e.g. kicks off a set of processes to gather more information, attempt remediation, virtual patching, ticket generation, etc.
- **Normalised Security Process:** Automatically generates the relevant Run-Book for a given offense type (e.g. malware, DDoS, etc.) which allows multiple teams/analysts to know and follow consistent security procedures
- **Audit Tracking:** Tracks incident process for evidential trail
- **Automatic Notifications:** Email notifications automatically sent to assignees/stakeholders

Trend TippingPoint Integration

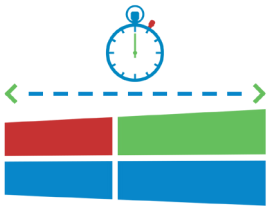
Trend Micro TippingPoint offers a wide range of network security solutions with real-time network protection, visibility, and centralised management and analytics that are easy to use, configure, and install. SOCAutomation utilises TippingPoint's API's covering IOC, digital vaccine, virtual patch, threat intelligence, vulnerability, policy, configuration and data automation.

SOCAutomation orchestrates the TippingPoint malware detection framework IPS and TippingPoint Advanced Threat Protection (ATP) working together to;

- Analyse suspected new malware in over 100 network protocols
- Once malware is detected, it's spread is qualified using TippingPoint ATP Endpoint Sensor
- TippingPoint then remediates by quarantining the affected devices or creating a reputation filter to block any rogue communication

Risk Reduction and Patch Management Window Lengthening

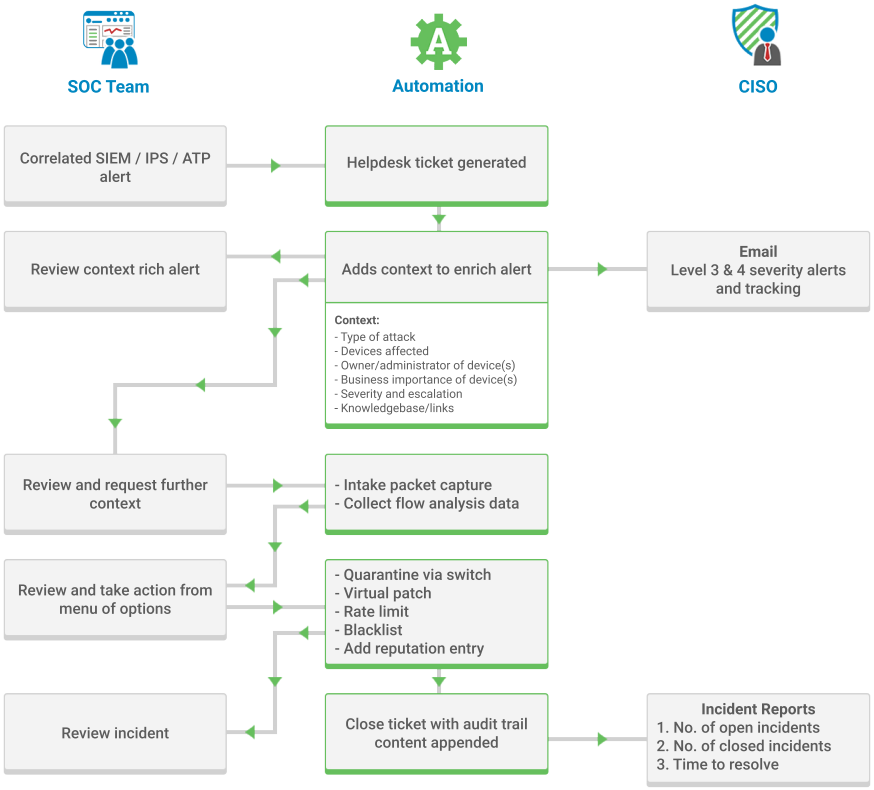
For vulnerability management, SOCAutomation collates all vulnerability & patch information then reports which security gaps can be automatically fixed using TippingPoint's Virtual Patching capability. Patch Tuesday now becomes – Patch when we are ready!



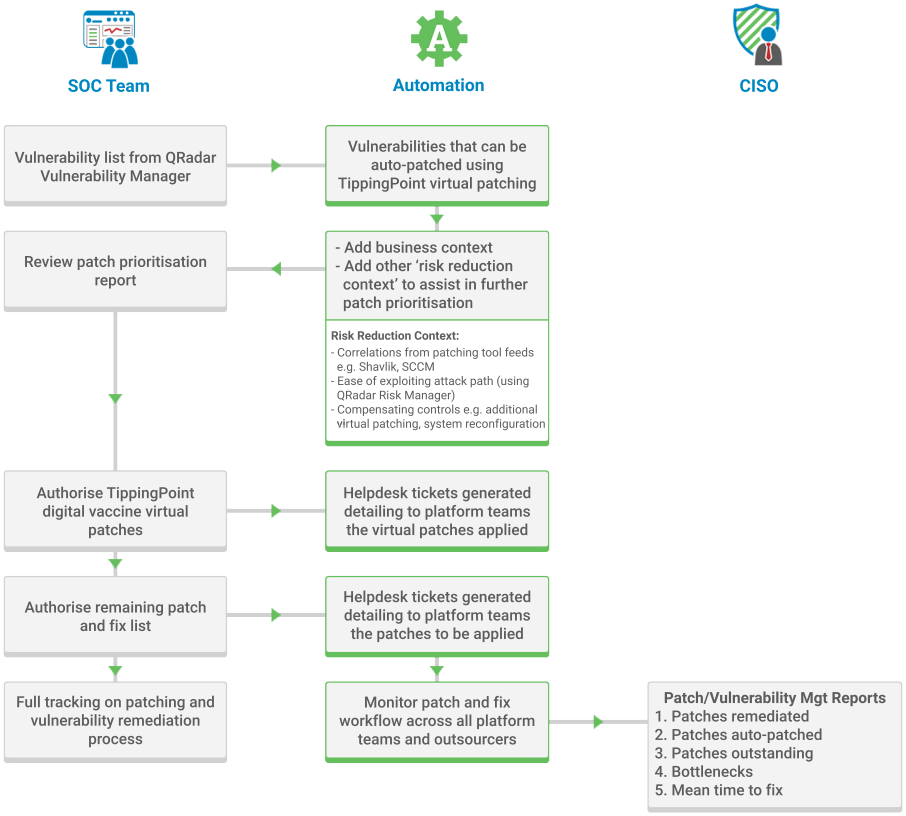
Example Run-Books

SOCAutomation enables powerful orchestration and automation of these platforms as illustrated in the following sample Run-Books

Run-Book 1: TippingPoint IPS/ATP (Zero Day), QRadar with Automated TippingPoint Remediation



Run-Book 2: Vulnerability/Patch Management Using QRadar and Trend Micro TippingPoint with Remediation Tracking



Run-Book 3: Botnet Activity Alert from Threat Intelligence with Automated TippingPoint ATP Remediation and Forensics - Using BitSight CyberRating Threat Intelligence

This Run-Book utilises data gathered from BitSight CyberRating Threat Intelligence, the following images outline the data collected

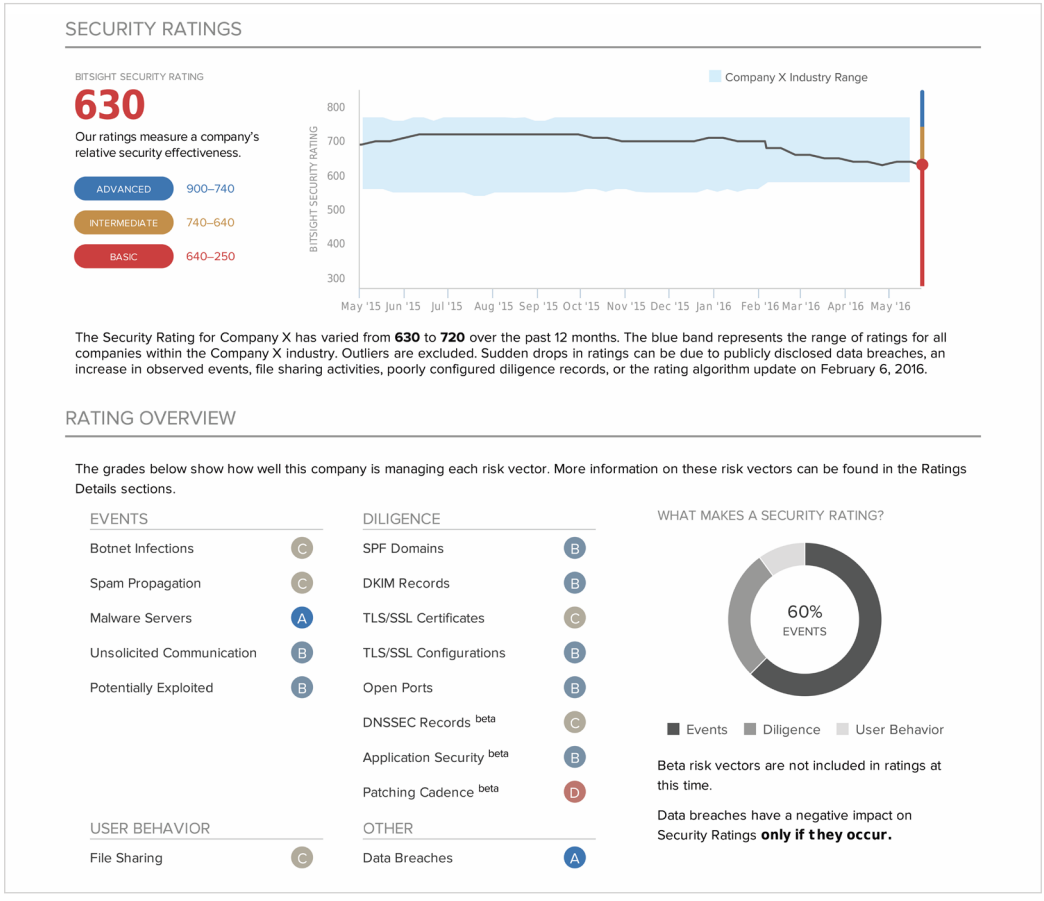


Fig 1: Overall BitSight security rating for 'Company X'

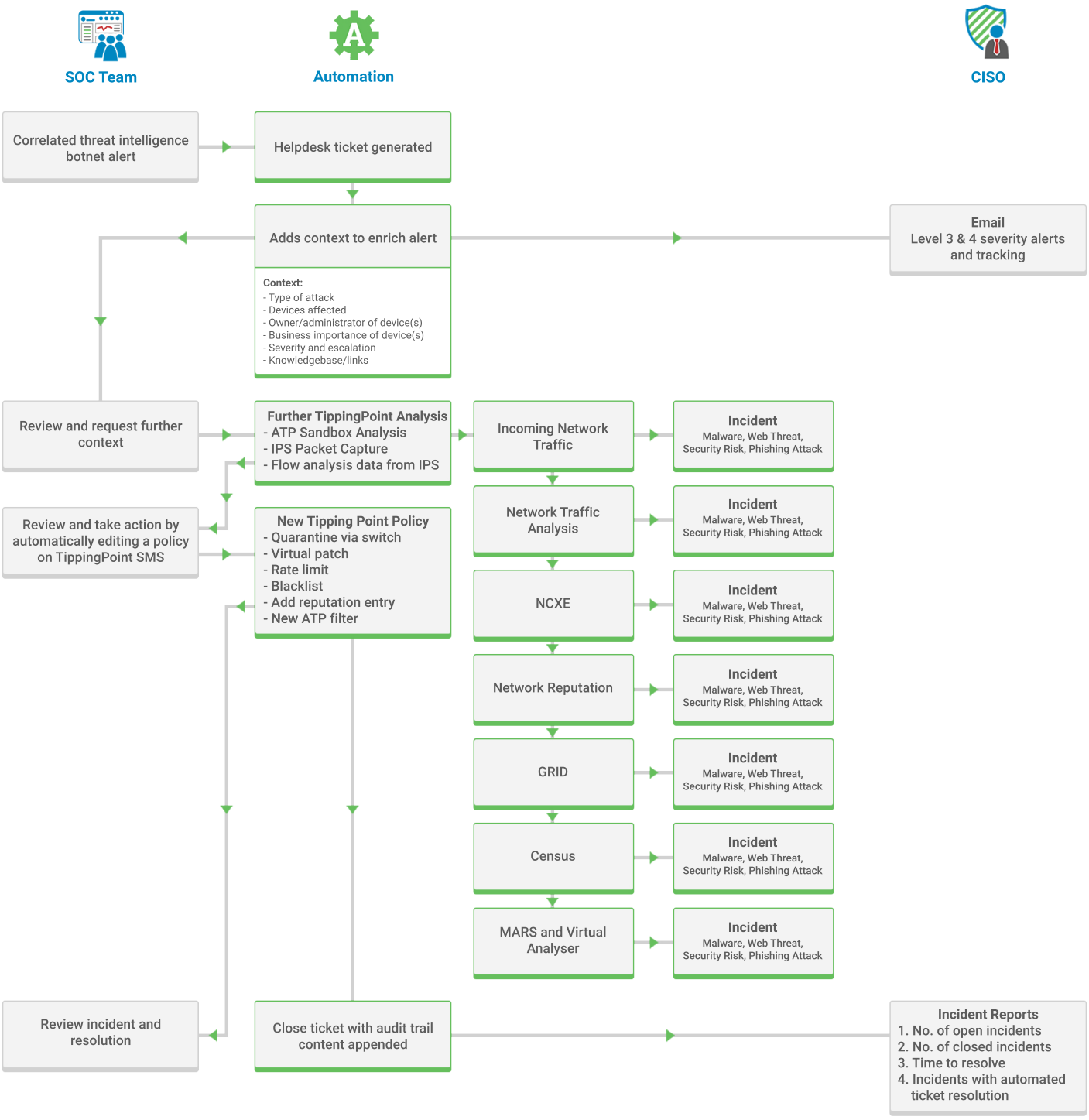
BOTNET INFECTIONS

C GRADE	2 THIS WEEK	127 PAST YEAR	1.9 days AVERAGE DURATION	COMPANY X
In the bottom 50% of all companies	1 THIS WEEK	14 PAST YEAR	3.2 days AVERAGE DURATION	COMPANY X INDUSTRY

40.6% faster to resolve events than the Company X industry average.

Botnet Infection events indicate that devices on a company's network were observed participating in botnets as either bots or Command and Control servers. Botnets can be used to exfiltrate corporate secrets and sensitive customer information, repurpose company resources for illegal activities, and serve as conduits for other infections.

Fig 2: Overview of botnet infections at 'Company X' compared to the industry



Dashboards and Reporting

SOCAutomation offers fully customisable dashboards, giving each user a personalised graphical representation of the data, as well as incidents and alerts relevant to them. Using a fully distributed and automated reporting engine, SOCAutomation is able to generate and deliver reports, graphs, tables, summaries and statistics to any number of stakeholders. Personnel from different areas of your organisation can receive specific reports relevant to their role via email. Reports are able to be automatically distributed to all stakeholders involved in an incident as soon as it is resolved. Some of the reports that can be generated are listed below:

- Incidents Handled by Severity
- Incident Response Timeliness
- Open Incidents
- Closed Incidents
- Incidents Utilising Most Resources
- Incidents Requiring Further Investigation
- Incident Handling Satisfaction
- Damage From an Incident
- Process Workflow
- General Mission Success
- Fire Drill Results
- Lessons Learned
- Incident Response Performance
- Incident Costs