servicenow | Microsoft

Accelerate incident response & operational efficiencies

with ServiceNow Security Operations & Microsoft Graph Security API

Challenges facing security teams

Inability to prioritize incidents quickly

No context

76%

of organizations have no common view of assets and applications across security and IT[1]

Few resources

82%

of employers report lack of cybersecurity skills[1]

Manual and delayed response processes

Manual process

56%

of organizations say things slip through the cracks because emails and spreadsheets are used to manage response processes[1]

Silos

62%

of breached organizations were unaware their organizations were vulnerable to a data breach[1]

[1]Source: "COSTS AND CONSEQUENCES OF GAPS IN VULNERABILITY RESPONSE", Ponemon Institute 2019

servicenow | Microsoft

The Threat Landscape

73 Days Average time to contain a breach[1]

667% Days Increase in phishing emails in March and April 2020[2]

$3.92 Million Average total cost of a breach[1]

78% Days Amount of cyber-espionage incidents that included phishing[3]

$6 trillion+
Global cost of cybercrime by 2021[3]

[1]Source: Ponemon Survey, "COSTS AND CONSEQUENCES OF GAPS IN VULNERABILITY RESPONSE", Ponemon Institute 2019
[2]Source: TechRepublic, March 2020
[3]Source: 2019 Verizon Data Breach Investigations Report

servicenow | Microsoft

Why ServiceNow and Microsoft

Incident management

Simplify and scale security monitoring and incident management

Collaborate and automate processes, workflows, and response

Speed up remediation and stay ahead of threats

servicenow | Microsoft

Why How important is automation and collaboration between security and IT teams?

$2.5 Million Average cost of breach savings by companies with fully deployed automated security solutions[1]

[1]Source: Ponemon Survey, "COSTS AND CONSEQUENCES OF GAPS IN VULNERABILITY RESPONSE", Ponemon Institute 2019

servicenow | Microsoft

Capabilities of integration

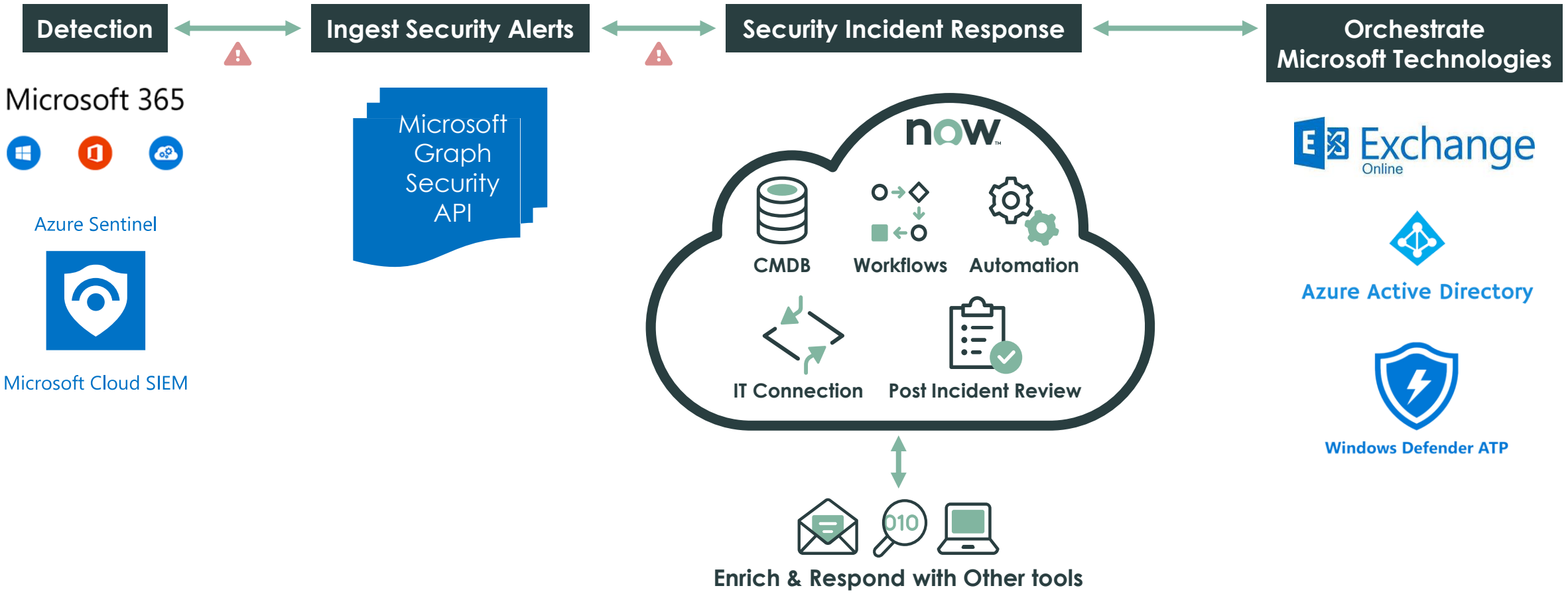
With the ServiceNow + Microsoft integration, security teams can create alert-ingestion profiles that support discovering correlated alerts in Azure Sentinel and other Microsoft security solutions.

- Map alerts fields to Security Incident Response fields
- Specify filtering conditions
  ex: create security incidents for alerts with severity=high
- Prescribe aggregation conditions
  ex: aggregate alerts on the same CMDB CI and carrying the same malware hash into a single incident
- Schedule the frequency of alert fetch
- Perform updates or closure of security alerts when the security Incident response has been enacted

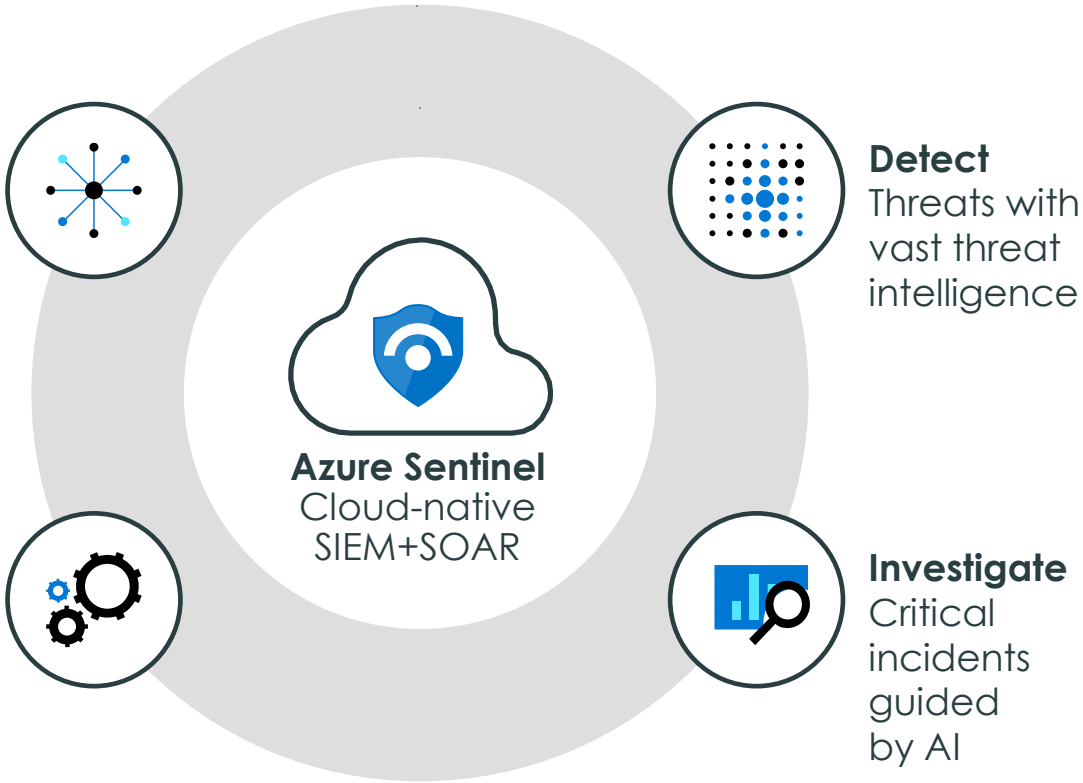
servicenow | Microsoft

Solution Architecture

servicenow + Microsoft



Microsoft Azure Sentinel



Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (**SIEM**) and security orchestration automated response (**SOAR**) solution.

servicenow | Microsoft

Microsoft Graph Security API

The Microsoft Graph Security API is an intermediary service (or broker) that provides a single programmatic interface to connect multiple security providers (native to Microsoft as well as partners)

- Unify and standardize alert tracking
- Correlate security alerts to improve threat protection and response
- Unlock security context to drive investigation
- Automate security workflows and reporting
- Utilize your threat intelligence in Microsoft security solutions
- Act quickly in response to new threats
- Proactively manage security risks using Microsoft Secure Score

servicenow | Microsoft

Automate Incident Response

Visibility into your critical incidents
Identify high-impact threats in real time, at scale

Quickly prioritize security incidents
Know your security posture with business context

Accelerate response time with security and IT collaboration
Orchestrate and automate actions and insights across teams

servicenow | Microsoft

Know when threats change, and new threats occur

Visibility into your critical incidents

Continuously monitor security incidents across your enterprise, at scale

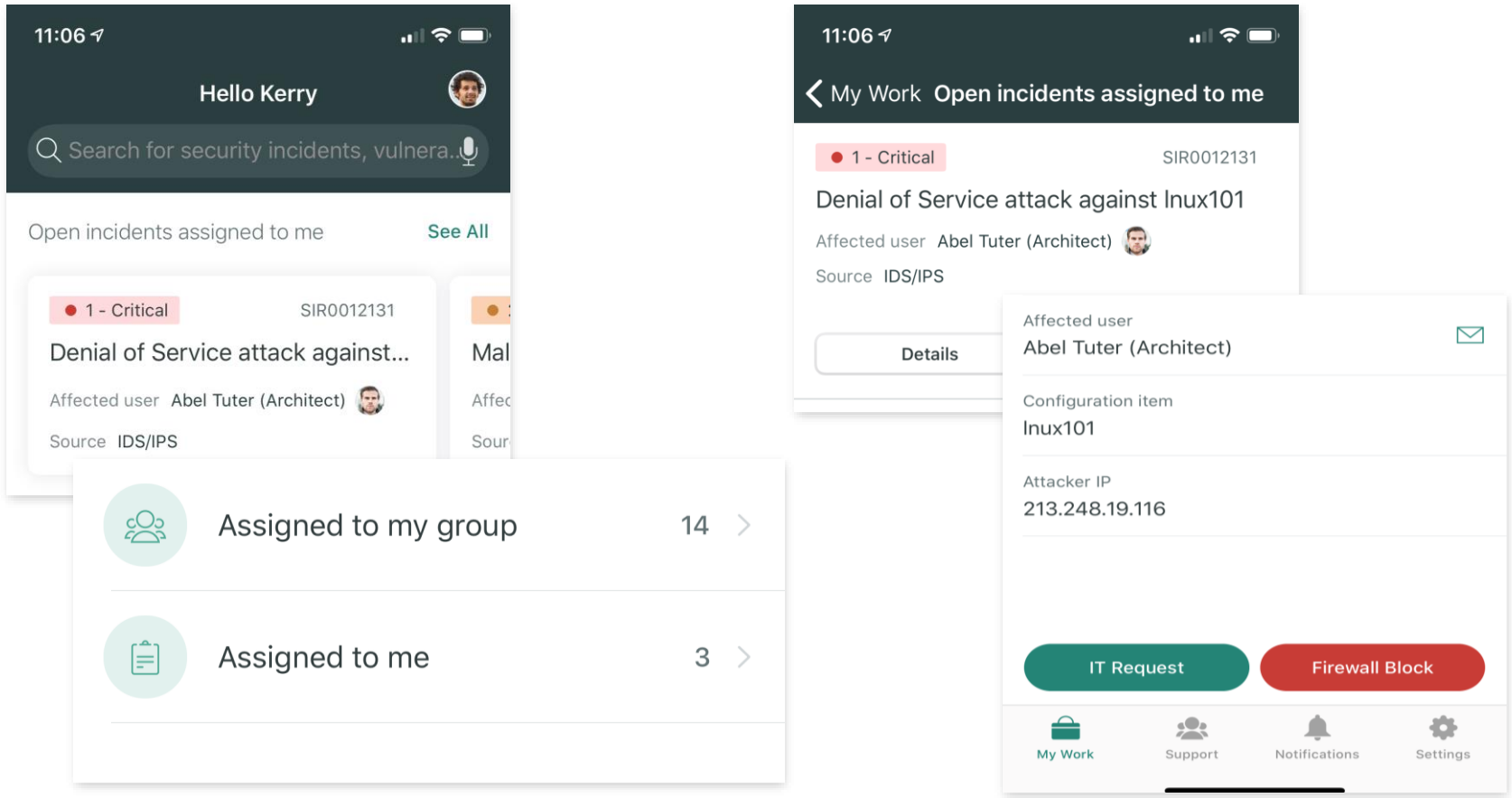
- Visibility into your threat exposure
- Identify security changes in real time
- Accurately assess business impact to best prioritize incidents and response workflow

servicenow | Microsoft

View your security incidents anytime, anywhere

Visibility into your critical incidents

- Security analysts can review incidents from their mobile device
- Quickly coordinate and support response efforts



servicenow | Microsoft

Know which incidents are critical

Quickly prioritize security incidents

Insights and business context into incident severity accelerate prioritization.

Focus on the incidents that matter most

- Prioritize by business criticality
- Inform decision-making
- Align the right data

50%
Reduction in incident triage time[1]

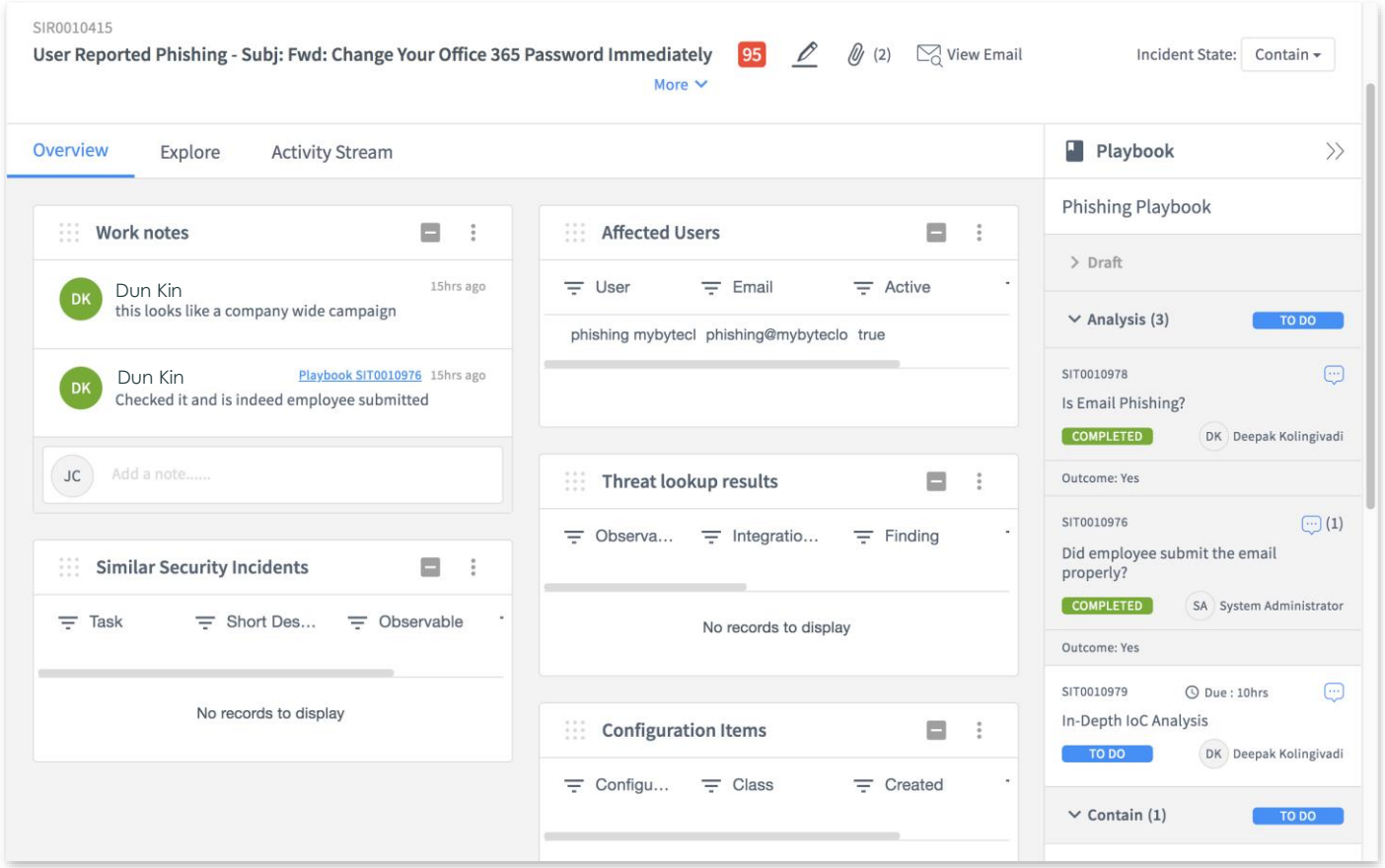
40%
Reduction in investigation times[2]

[1]Source: DXC Technology
[2]Source: Freedom Security Alliance

servicenow | Microsoft

Comprehensive incident record shared across teams

Quickly prioritize security incidents



Single system of record to drive prioritization and cyber resilience:

- Response process and actions
- Analysts' work notes
- Post-incident reviews

Enables repeatable and collaborative workflows.

servicenow | Microsoft

Automate and orchestrate processes and assign owners

Accelerate response time with security and IT collaboration

Route work seamlessly between security and IT teams, so they can:

- **Accelerate** resolution with automated workflows
- **Automate** incident assignment
- **View** real-time incident status and track remediation processes
- **Centralize** data and reporting

80%

Of organizations that use automation say they can respond to vulnerabilities faster[1]

[1]Source: *2019 Ponemon Survey sponsored by ServiceNow, "COSTS AND CONSEQUENCES OF GAPS IN VULNERABILITY RESPONSE"*

servicenow | Microsoft

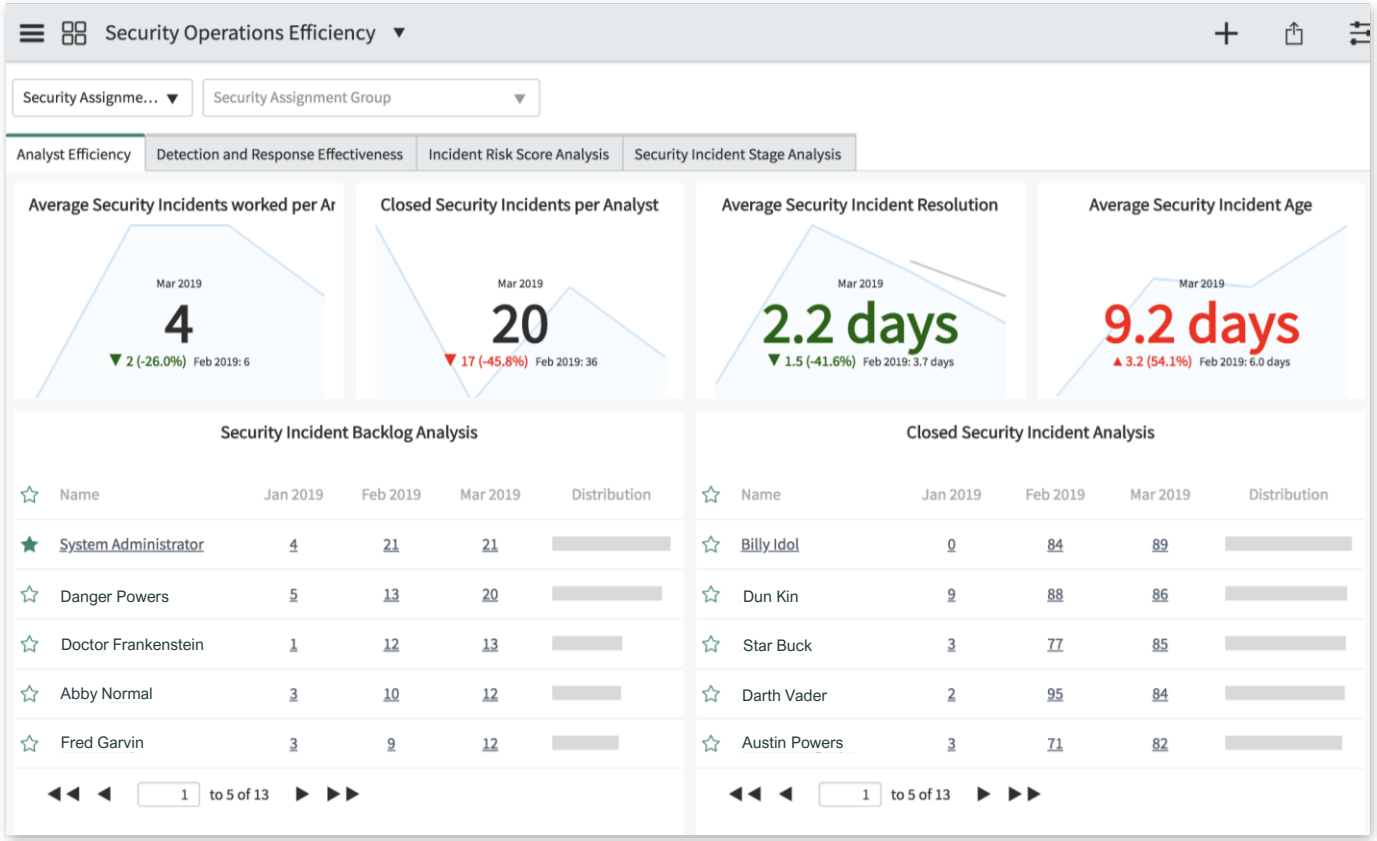
Report, review and plan for success

Security operations center efficiency dashboards

Accelerate response time with security and IT collaboration

Know how your SOC is performing

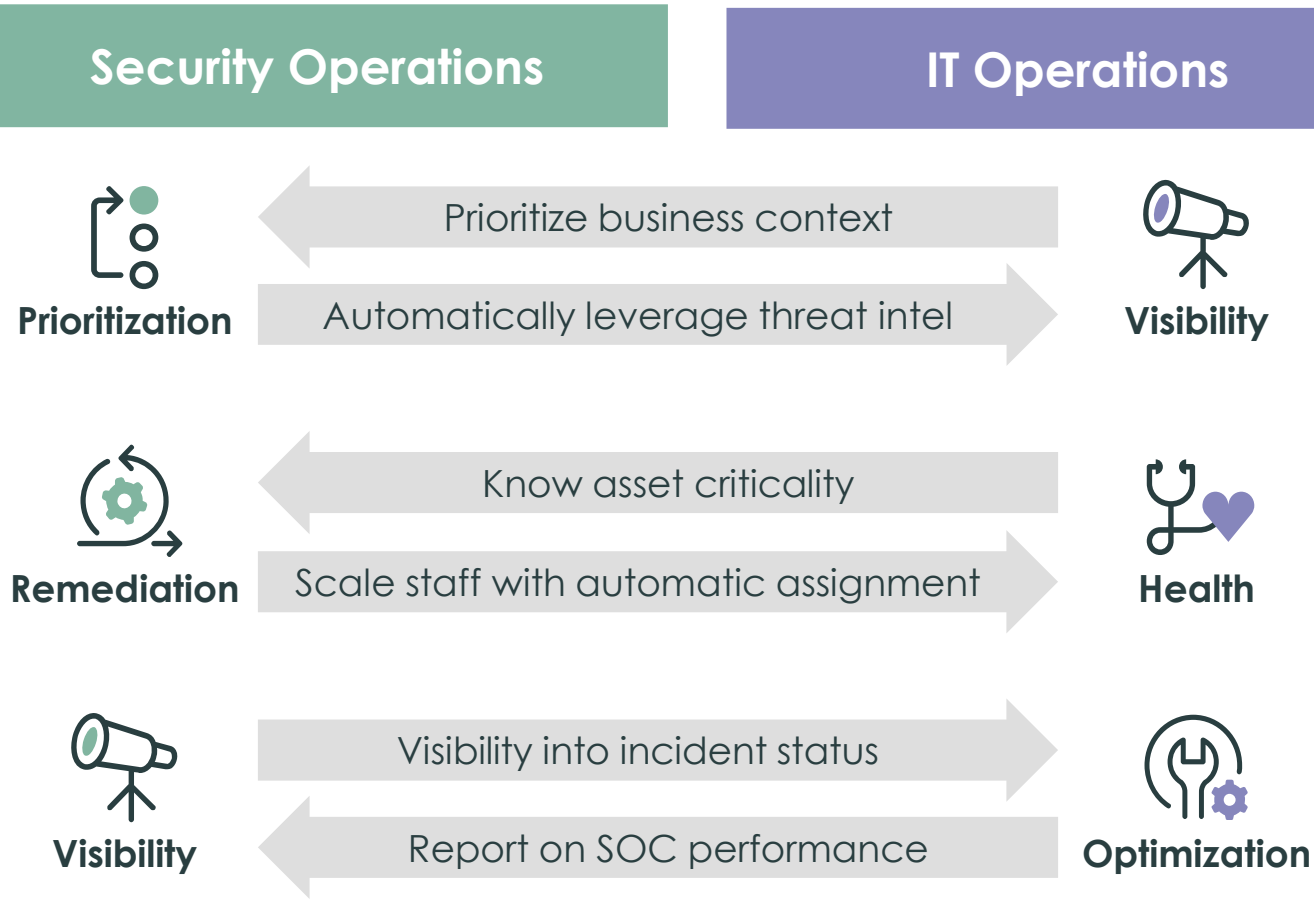
- Analyst efficiency metrics
- Measurement of response workflow effectiveness
- Incident risk analysis
- Security Incident trends



servicenow | Microsoft

Collaborative data sharing and orchestrated actions

Accelerate response time with security and IT collaboration



servicenow | Microsoft

Automate Incident Response

ServiceNow Security Incident Response helps you effectively manage the evolving threats to your business

Proactively manage exposure with visibility into high-impact threats

Ensure cyber resilience with real-time view into your security posture to quickly prioritize security incidents

Drive efficiencies and accelerate reaction time with insights across teams to effectively orchestrate and automate actions

servicenow | Microsoft

ServiceNow Security Operations' value to the IT organization

Tools and intelligence, **all in one collaborative platform**

Open lines of communication

Elimination of error-prone, manual tasks

servicenow | Microsoft

Drive operational excellence across your security operations and IT teams with shared data and workflows

- Cut through the noise
- Simplify management and response
- Connect security and IT teams
- Reduce the burden
- Easily customize
- Gain greater confidence
- Get deeper knowledge

servicenow | Microsoft

servicenow | Microsoft

Thank you