USE CASE GUIDE

# Security Operations Use Case Guide

Improve your cyber resilience and vulnerability management while speeding up response times

servicenow

# Resolve security incidents and vulnerabilities fast with ServiceNow® Security Operations

Responding to security incidents and vulnerabilities is an ongoing process, and you know that reacting too slowly to a critical incident can have drastic consequences. When teams are frequently understaffed, yet overwhelmed by alerts, automation along with orchestration can provide enormous benefit by making these teams able to respond more quickly.

## The power of the platform

ServiceNow Security Operations helps security teams scale faster, smarter and more efficiently, enabling and automating critical collaboration of data and process between IT, security, and risk to effectively respond and remediate threats. It brings in security and vulnerability data from your existing tools and uses intelligent workflows, automation, and a deep connection with IT to streamline security response. ServiceNow Security Operations helps you use the power of the Now Platform® to reduce cybersecurity risk and drive cyber resilience.

## Focusing on what is most critical

As part of the Now Platform, Security Operations can leverage the ServiceNow® Configuration Management Database (CMDB) to map threats, security incidents, and vulnerabilities to business services along with IT infrastructure, like servers, computers, and users. This mapping enables prioritization and risk scoring based on business impact, ensuring your security teams are focused on what is most critical to your business. Working in a single platform enables efficient collaboration with IT for remediation and adds the benefits of visibility and service level agreement tracking to ensure nothing is missed. It also allows you to connect security and risk together by aligning with regulatory compliance and ensuring correct business processes are followed. This provides the context needed for ongoing updates to cyber policy and processes.

## Automation and orchestration

Digital security workflows, automation, and orchestration speed up tasks such as analysis, prioritization, and remediation. Automatically correlate threat intelligence from multiple sources, including MITRE ATT&CK, or take action in other security or IT management tools from a central console. Track your security posture across the organization, as well as team and process performance, with fully-customizable reports and real-time dashboards.

The following use cases will give you a better understanding of how you can benefit from the workflows and automation of ServiceNow Security Operations for faster security response.

| Scale resources with security automation and orchestration | Manage and resolve risks due to high-profile vulnerabilities |
|---|---|
| Use playbooks and integrations to accelerate security response | Find and remediate application vulnerabilities effectively |
| Know an attacker's next move by mapping incidents to MITRE ATT&CK | Get real-time insights on security posture and SOC performance via reporting |
| Leverage workflows to proactively monitor and resolve misconfigurations | Defend against high-profile cyberattacks and reduce your attack surface |

**Digital security workflows, automation, and orchestration speed up tasks such as analysis, prioritization, and remediation. Automatically correlate threat intelligence from multiple sources, including MITRE ATT&CK, or take action in other security or IT management tools from a central console. Track your security posture across the organization, as well as team and process performance, with fully-customizable reports and real-time dashboards.**

# Scale resources with security automation and orchestration

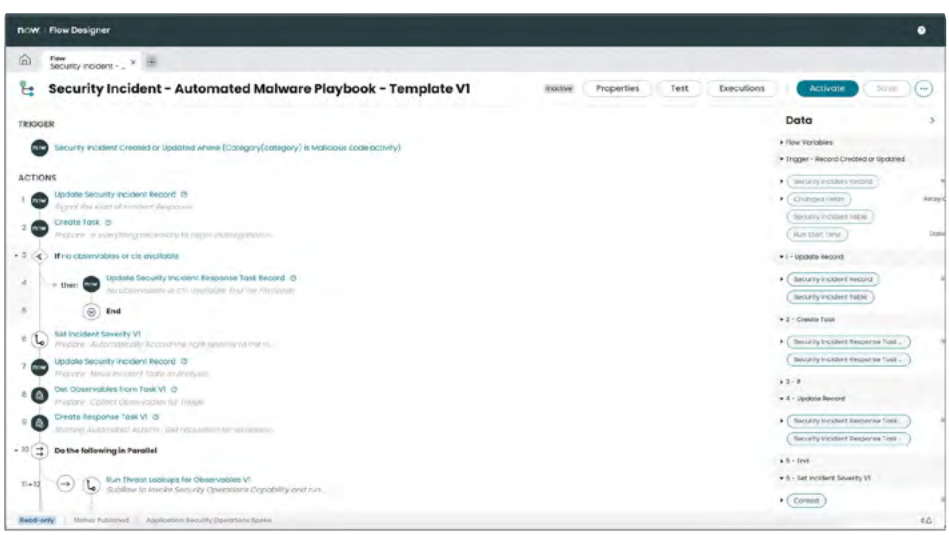
Resourcing is an ongoing issue for security organizations. A 2021 study from the Information Systems Security Association (ISSA) and ESG[1] found that 57% of organizations are impacted by the lack of cybersecurity resources, and 44% said the problem is getting worse. One way to mitigate this is by employing security automation and orchestration wherever possible to ease the burden on skilled personnel.

## Saving time on analysis and prioritization

Some organizations are reticent to relinquish too much control to their security platform, but there are plenty of ways automation can help you scale while still allowing your skilled analysts to handle decision making. A great starting point for this is threat enrichment. Most organizations already use threat intelligence feeds as part of their incident response process. Automatically integrating and correlating threat enrichment sources, as well as threat context from other security tools, can dramatically reduce the time spent on analysis and incident prioritization.

## Parallel workflows to manage threats

An organization using ServiceNow® Security Incident Response receives an alert about a suspicious file from their Security Information and Event Management (SIEM) solution, which creates a new security incident. The creation of this incident kicked off several parallel workflows which extracted Indicator of Compromise (IoC) information, including the hash of this suspicious file and the originating IP address.




These workflows can perform threat lookups, observable enrichment, and malware sandboxing with a number of security vendors, including Cisco, CrowdStrike, Palo Alto Networks, Recorded Future, Virus Total, Zscaler, and more. A threat lookup determines if an IoC is associated with a threat and performs a sightings search to see how widespread it is within the network. Observable enrichment pulls additional information about the IoC from the respective threat intelligence tools via integration. Malware sandboxing can send a file, hash, or URL to the designated sandbox for investigation. You can also get network statistics and running processes through pre-built workflows. All of these actions can be initiated from ServiceNow automatically via workflows or manually by the analyst.

1 Oltsik, John and Lundell, Bill, The Life and Times of Cybersecurity Professionals 2021

All of the resulting data is reported back to ServiceNow Security Incident Response within seconds and is displayed in the security incident record. Now, a security analyst can view a wealth of information from multiple sources in one place without having to perform manual research. With this information in hand, they can determine the next steps to take in the response process.

Observables

| | | Observable | Observable Type | Finding | Incident Count |
|---|---|---|---|---|---|
| | 0 | https://www.totallylegitwebsite.com/notm... | URL | Malicious | 3 |
| | 0 | fe80::699e:e0c4:f04:9bdd%6 | IP address (V6) | Unknown | 3 |
| | 0 | drf@totallylegitwebsite.com | Email address | Unknown | 3 |
| | 0 | fe80::699e:e0c4:f04:9bdd | IP address (V6) | Unknown | 3 |

Perhaps in this case, the next step is to create a firewall block request to prevent malware from exfiltrating data. Again, orchestration can be used by the analyst to create the block request in a couple of clicks without leaving ServiceNow. This saves time and also creates a traceable record as to why the block request was created. You can even choose to fully automate workflows within a response if desired. Security Operations can notify analysts of the steps taken in case they wish to make changes.

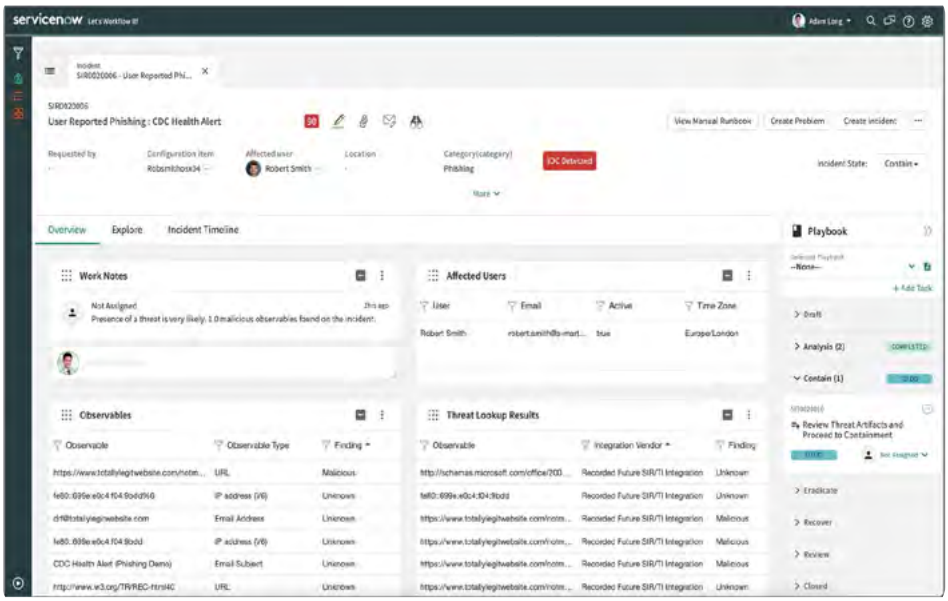
# Use playbooks and integrations to accelerate security incident response

Speed is critical when it comes to security incidents. We've covered how automation can help reduce the amount of work security analysts need to do while also driving efficiencies and helping them respond faster. Security Incident Playbooks are another tool to help increase the effectiveness of your security analysts, especially those who are newer to the organization or early in their career. Playbooks provide step-by-step guidance to remediate common security threats.

## A phishing example

A number of playbooks, subflows, and actions are included with ServiceNow Security Incident Response. You can configure these or create new playbooks quickly and easily without code using Flow Designer, a Now Platform feature for automating processes using natural language. Here's a phishing example to show how playbooks and integrations accelerate security response.

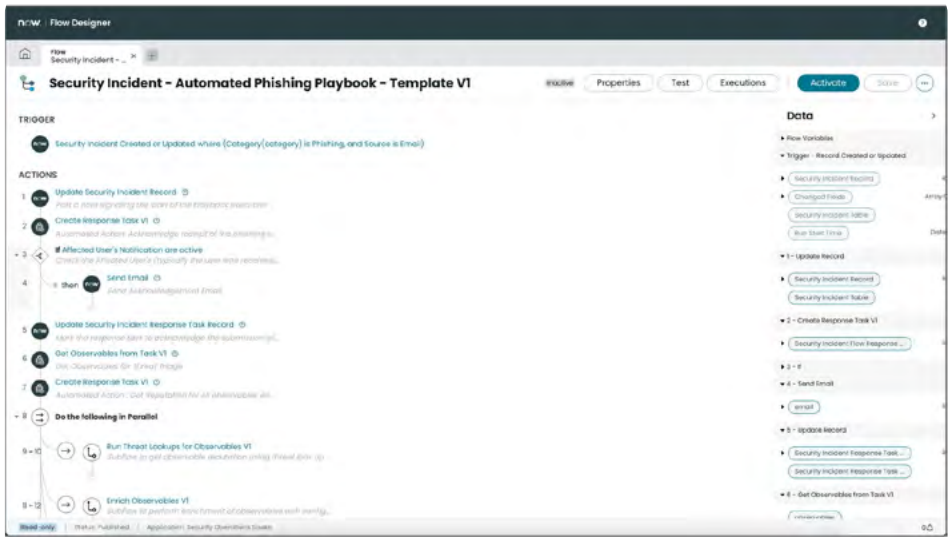
An employee forwards a suspicious email to phishing@example.com, a specific mailbox set up by their organization's security team to direct the email to their ServiceNow instance. The instance then parses the attached .eml file and compares it against email matching rules that have been created in advance to determine if it's a potential phish. If so, a security incident is created that includes an attached copy of the email. Any security observables or Indicators of Compromise (IoCs) are automatically submitted to third-party threat intelligence vendors to determine if the email is malicious. The observables and threat lookup results are then visualized in the security incident overview.




**A number of playbooks, subflows, and actions are included with ServiceNow Security Incident Response. You can configure these or create new playbooks quickly and easily without code using Flow Designer, a Now Platform feature for automating processes using natural language. Here's a phishing example to show how playbooks and integrations accelerate security response.**

In parallel, the security incident is assigned to an analyst for remediation. Because this has been identified as a potential phishing email, the phishing playbook is associated with the incident. This playbook contains tasks to help analyze, contain, and eradicate a phishing threat. The tasks are organized into phases, and when all tasks for a phase have been completed, the playbook guides the analyst to the next phase.

In the analysis phase, the analyst will be guided through determining the validity and impact of the threat from the threat lookup results pulled via threat intelligence integrations. They can also view related knowledge articles and investigate the email attachment.




In the contain phase, the analyst is given tasks to further assess the phishing threat and limit potential spread. They can use sightings searches to see how often the observables were seen in the environment in a specific timeframe to determine how many other assets may have been impacted by the phishing attack. They can also search the company's Microsoft Exchange Server or Exchange Online from Security Incident Response to see who else received the message and if they opened it.

## Preventing phishes and eradicating malware

Other instances of the phishing email can then be deleted from the server to prevent additional recipients from opening it. Analysts can also take actions such as updating network defenses and isolating impacted systems using integrations with endpoint detection and response tools. Using orchestration, these actions can be taken directly from within ServiceNow.

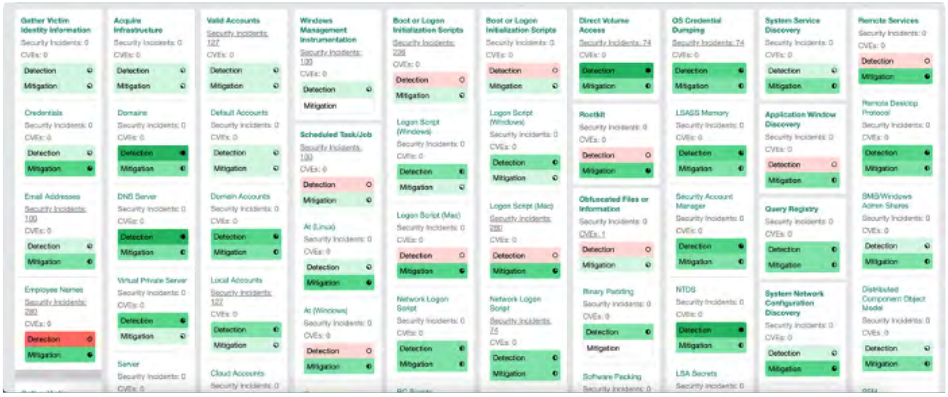
The eradicate phase of the playbook includes guidance to find and remove any malware caused by the phishing email. It includes tasks such as scanning endpoints that may have been affected, removing malware, and wiping and reimaging host devices, if necessary. Once the eradication tasks are complete, the security incident is automatically closed. Security Incident Response automatically generates a post-incident review containing a time-stamped record of all actions taken within the incident and any related sub-tasks.

# Know an attacker's next move by mapping incidents to MITRE ATT&CK®

Security teams have historically found internalizing an adversary's intent a challenge when dealing with security incidents and may incorrectly prioritize security incidents without this insight. MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) documents and tracks various adversarial techniques that are used during different stages of a cyberattack. By integrating the MITRE ATT&CK knowledge base with ServiceNow Security Incident Response, organizations can more quickly identify threats and anticipate cyberattack responses. This framework helps security analysts align events and IoCs with the tactics and techniques used by adversaries and attack campaigns.

## Operationalizing security response

ServiceNow Security Operations allows you to combine SOAR and MITRE ATT&CK to add business, asset, risk, and threat context to your security automation and orchestration. The combination delivers an incident response platform and threat intelligence to help you respond fast and efficiently, enabling you to move beyond point tools to operationalize security response.



Whenever a security incident is created from an alert, details from all data sources, including third-party products like SIEM, sandbox, and TIPs, are forwarded to ServiceNow Security Operations, which also gathers all information related to MITRE ATT&CK tactics and techniques. These tactics and techniques are then mapped to a MITRE ATT&CK card. This allows analysts to better understand where individual security events fit into an overall attack. ServiceNow also can ingest MITRE ATT&CK data from third-party products like SIEM or threat intelligence feeds.

## Similar to GPS tracking

Beyond associating specific security incidents with MITRE tactics and techniques, security analysts can use the ServiceNow ATT&CK Navigator to pivot across the MITRE ATT&CK Matrix and understand what likely happened before an individual security event and what's likely to happen next. ServiceNow has enhanced the MITRE ATT&CK navigator with additional visualization features to help organizations understand the scope and relationships of different types of attacks and what to do next for response and containment. This is analogous to navigation using GPS tracking rather than depending upon a compass and celestial constellation. This sequencing alone can help accelerate security operations processes.

**ServiceNow Security Operations allows you to combine SOAR and MITRE ATT&CK to add business, asset, risk, and threat context to your security automation and orchestration. The combination delivers an incident response platform and threat intelligence to help you respond fast and efficiently, enabling you to move beyond point tools to operationalize security response.**

## Using heatmaps for prevention

With the included heat maps, your SOC teams can visualize their security effectiveness and adjust detection rules and controls coverage across techniques, campaigns, and specific adversaries. Once security teams can determine the tactics and techniques used in cyberattack campaigns, they can better understand the attack surface and how well prepared they are in terms of threat prevention and detection. This clarity can help them answer key questions like: Do we have the right controls in place to block tactics and techniques? What can and can't we detect using current controls and data sources? Are security controls and data sources adequate or are there gaps in coverage?

The analyst can use filters to quickly see relevant information to their investigation and change the view of the heatmap. Many filter choices are available out of the box to help analysts focus on the right information and configure the best view for them. For example, toggling a filter will display CVEs associated with various techniques.

Clicking on a technique in the heatmap opens up the full record, including the description and detection information. Adversary groups known to use the technique are linked and can be viewed, which in turn connect to attack patterns and tools. This data can also be viewed using the STIX Visualizer, which provides an easy way to see relationships between an adversary group and malware.


## Roadmaps to resolutions

Security analysts can also use MITRE ATT&CK when investigating a security incident. The analyst can immediately view the MITRE ATT&CK tactics and techniques data that was automatically mapped based on the incident category. Automatic mapping makes it easier for the analyst to find the right information quickly.

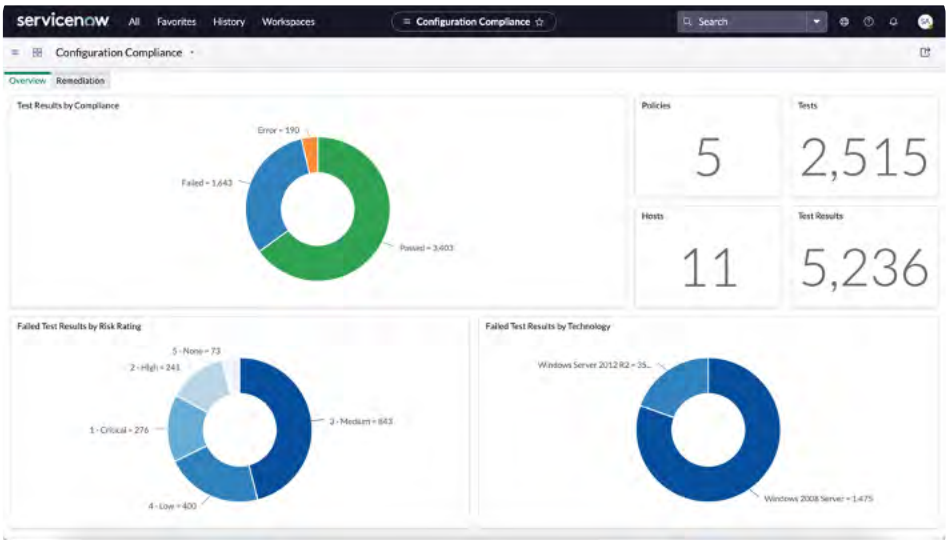
They can look into the IoCs for this incident, which include the threat lookup and observable enrichment results that were run via orchestration. In addition, they can see MITRE ATT&CK information that has been mapped to individual observables. The analyst can then use the ServiceNow ATT&CK Navigator to visualize how an individual tactic or technique is used by the numerous adversaries tracked by MITRE. The security analyst can now get an adversary perspective and a roadmap for investigations and resolution.

# Leverage workflows to proactively monitor and resolve misconfigurations

Misconfigured software leaves an organization open to attackers and was responsible for 10% of breaches in 2020[2]. Configuration issues include incorrect permissions, weak passwords, access controls, and more. These are preventable issues that must be found and remediated to reduce your attack surface. The process starts with setting policies to define secure configurations (for example, minimum password length requirements), and integrating a security configuration assessment (SCA) tool with ServiceNow Security Operations.

## Finding misconfigured assets

The SCA tool scans your network to test assets against these policies to find any misconfigurations. The scan data is then imported into the Configuration Compliance application in ServiceNow, where failed configuration test results are matched against assets in the ServiceNow CMDB. Data from the CMDB determines how important each asset is to the business, and that business criticality is a key factor in the risk score used to prioritize failed results.




This risk score is based on a scale of 0–100 and is used across applications in Security Operations for consistent prioritization. The risk score calculator can be customized to include additional criteria, or to give greater weight to specific factors impacting your organization's applications.

## Collaborating on remediation

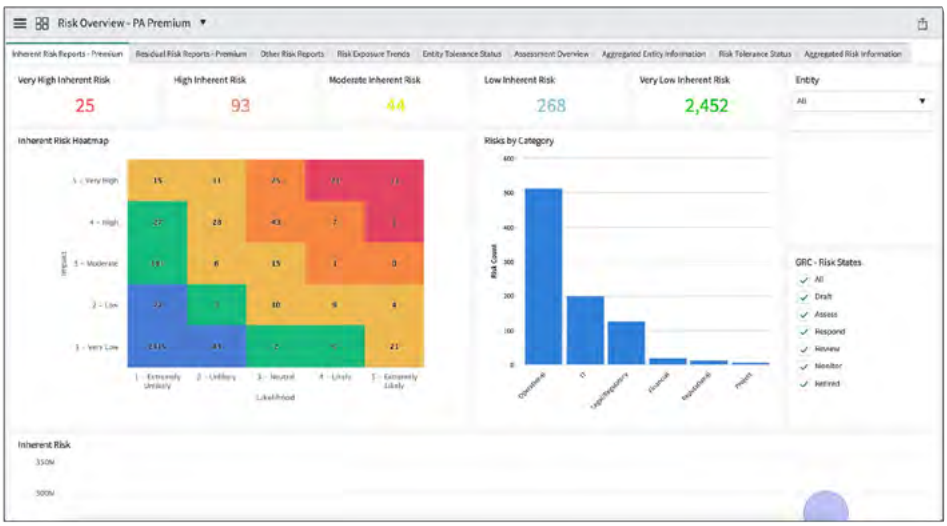
Now that responders have a prioritized list of configuration test failures, they know which ones to address first. Machine learning can automatically group together similar failures and then automatically assign them to the teams that will address them. For example, failures on the supply chain and manufacturing application servers will be grouped and assigned to those asset owners for remediation. If remediation requires action from IT, the security analyst can easily create IT change tickets associated with the configuration items directly from the test result group. This allows IT to use change management in ServiceNow® IT Service Management to track and implement changes. Remediation target rules define the expected time frame for remediation to ensure all failures are addressed. Both security and IT teams can see when target dates are approaching or past due.

2 Verizon Data Breach Investigations Report, 2021

**The SCA tool scans your network to test assets against these policies to find any misconfigurations. The scan data is then imported into the Configuration Compliance application in ServiceNow, where failed configuration test results are matched against assets in the ServiceNow CMDB. Data from the CMDB determines how important each asset is to the business, and that business criticality is a key factor in the risk score used to prioritize failed results.**

Alternately, non-critical failures can be deferred to the next standard change window using the exception management approval process. Once the failures are addressed, a follow-up scan confirms the fix, and the group is closed.

Test results from Configuration Compliance can also feed into ServiceNow® Governance, Risk, and Compliance. Configuration Compliance tests can be associated with a GRC policy to generate controls, profiles, and indicators. A test failure means the control is non-compliant, generating a risk issue. When the misconfiguration is remediated, the risk issue is closed automatically.



# Manage and resolve risks due to high-profile vulnerabilities

Many organizations find they're overwhelmed with the number of vulnerabilities they need to deal with. A recent survey from ESG found 61% of organizations understand the importance of security hygiene but find it difficult to prioritize the right actions that can have the biggest impact on risk reduction.[3] That means when a critical vulnerability hits, it can be hard to tell what's important.

## Prioritizing and tracking vulnerabilities

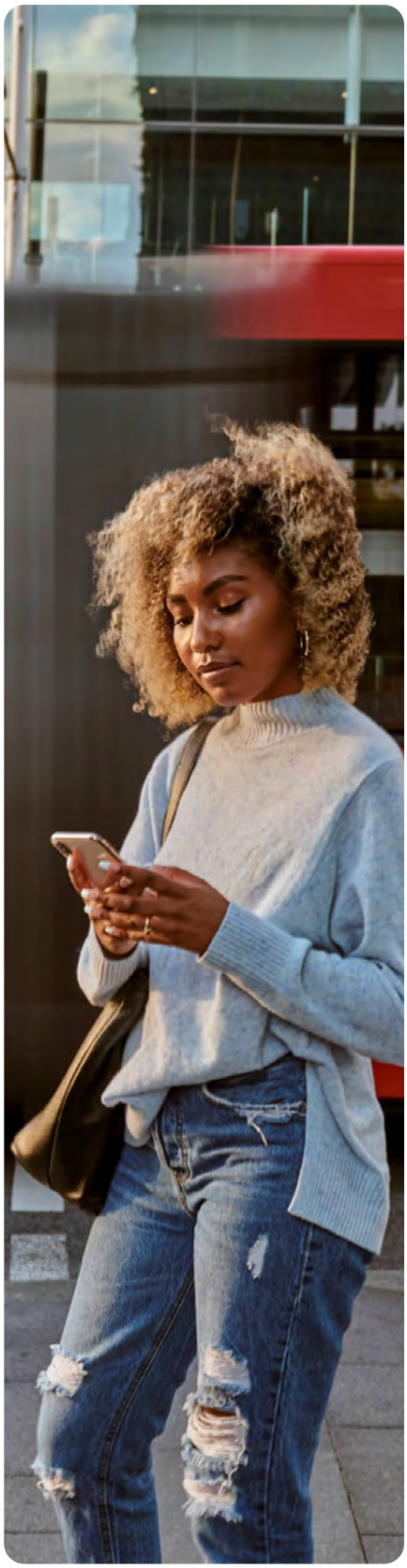
ServiceNow® Vulnerability Response helps organizations respond faster and more efficiently to vulnerabilities, connect security and IT teams, and provide real-time visibility into all vulnerabilities affecting a given asset or service. When used with the ServiceNow CMDB, Vulnerability Response can prioritize vulnerable assets by business impact using a calculated risk score so teams can focus on what is most critical to their organization.

With ServiceNow Vulnerability Response, a vulnerability manager may choose to create a watch topic for a specific vulnerability when a new critical weakness is discovered. This will allow them to easily track all occurrences of the vulnerability within the organization. This happens when vulnerability scan data is automatically imported into the Vulnerability Response application using APIs and is matched against the ServiceNow CMDB. These resulting vulnerable items are assigned a risk score based on multiple factors, including the severity of the vulnerability, the importance of the affected asset, and whether an exploit exists. The risk score is configurable and provides quick prioritization.


## No manual research needed

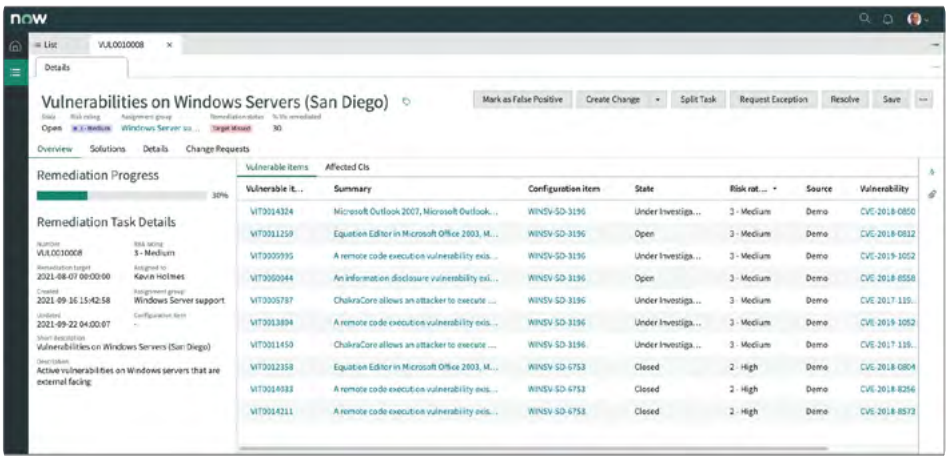
Information about the vulnerability (e.g., what it is, how it's exploited, and how to remediate the threat) is automatically pulled into Vulnerability Response from the National Vulnerability Database (NVD) and other third-party sources, eliminating the need for manual research. If a known solution exists from Microsoft or Red Hat's databases, that will also be included with the remediation information. Configurable dashboards quickly show the organization's overall vulnerability exposure.

Grouping and prioritization work together to make the volume of vulnerabilities manageable. Instead of dealing with thousands of individual vulnerable items, you can work with a much smaller number of groups and handle prioritization and remediation at the group level.



3 ESG Research Study, Security Hygiene and Posture Management, 2021

When a vulnerability manager sees new entries on the high-profile CVE watch list, they can quickly take action by creating a remediation effort. This will create patching tasks for IT based on the vulnerability, asset, or assignment group. Remediation tasks will be prioritized for the assignees in IT so they can focus on the most critical tasks first.




Alternately, you can use orchestration to patch automatically. Requests to approve automatic patching are sent and the appropriate owners are notified. There is no need to search for who's on call or manually decide which items count as "critical." Upon approval and completion of the patch, a second scan is automatically run to verify the fix. Using prioritization, workflows, and automation, the most critical items are addressed first.

## Deferring non-critical vulnerabilities

For non-critical vulnerabilities, you might choose to defer remediation to align with standard change windows. Vulnerability Response includes exception handling workflows to defer a single vulnerable item (asset with a vulnerability) or a group of items. Deferral includes approval flows as well as an expiration date so the vulnerability can become active again when the exception expires.

Vulnerability Response also ties into ServiceNow Governance, Risk, and Compliance via Continuous Monitoring. In the case of the high-profile vulnerability, you can choose to also track it as a business risk due to the potential for exploit. When the vulnerability is fixed and closed, the corresponding risk issue will also be closed.

**Vulnerability Response also ties into ServiceNow Governance, Risk, and Compliance via Continuous Monitoring. In the case of the high-profile vulnerability, you can choose to also track it as a business risk due to the potential for exploit. When the vulnerability is fixed and closed, the corresponding risk issue will also be closed.**

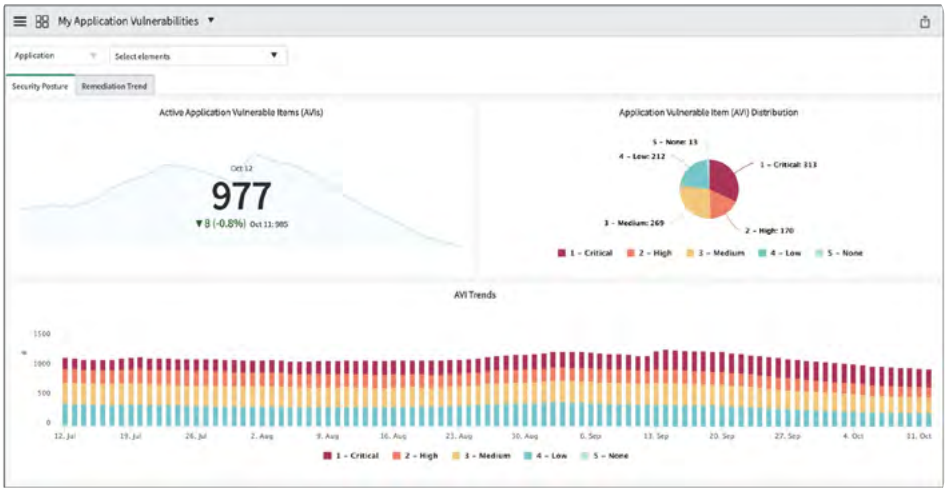
# Find and remediate application vulnerabilities effectively

Organizations are increasingly developing their own custom software applications, but these can unfortunately lead to new security risks. 39% of data breaches in 2020 stemmed from web application compromise, according to the Verizon Data Breach Investigations Report. One cause is using open-source code for faster application development, as this code is also readily available for cyber criminals to study and exploit.

To determine security flaws in deployment-stage applications, most organizations use testing tools such as Dynamic Application Security Testing (DAST), Static Application Security Testing (SAST), and Software Composition Analysis (SCA). These provide different ways to find weaknesses, whether in a running application or by examining source code. Using multiple testing tools creates a new layer of complexity for security teams to collect data points, identify relevant development teams, and determine next steps.

## Identifying and coordinating fixes

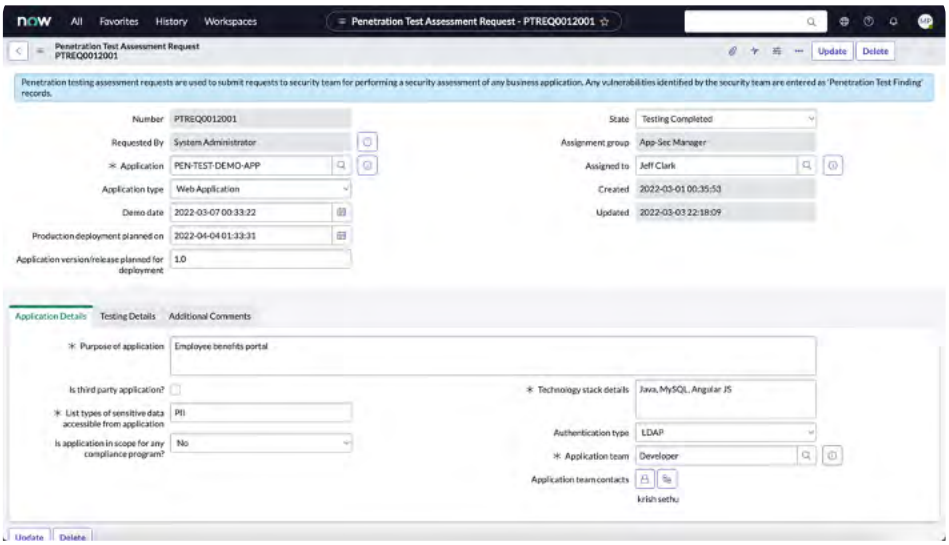
ServiceNow® Application Vulnerability Response works with application vulnerability scanners and the Common Weakness Enumeration (CWE) to assesses DAST and SAST results to identify vulnerable items and coordinate fixes. It starts with scanning. Dynamic (DAST) scans assess a running service, and results come with a URL location of the discovered vulnerability. Static (SAST) scans use the source code of the application and return a file and line number location of the vulnerability. The scan data is pulled into ServiceNow to see which applications and releases thereof are impacted.




For this example, let's examine a case involving penetration testing instead of a scanner. An application developer wants to make sure there are no potential weaknesses in their application, so they make a request to their organization's ethical hacking team via the service catalog.

## Determining risk scores

The ethical hacking team receives the request, scopes it, and creates a test environment. They perform their testing and create new application vulnerable items for the issues they find. The new entries are assigned a risk score determined automatically by a configurable calculator that includes the severity of the vulnerability and the business criticality of the affected services or other dependencies. With Service Mapping from ServiceNow IT Operations Management, the security team can see how an application is related to other parts of the network, including the supported services. Risk scores are used consistently across the broader ServiceNow Security Operations solution to help you understand your overall security posture.




## Setting remediation target dates

The new application vulnerable items also get remediation target dates determined by previously-configured remediation target rules. These rules can apply different timelines based on factors such as criticality or asset. Automated assignment rules mean the correct development team has already been associated with the application, allowing the application vulnerability to be assigned to the right team for remediation automatically. The application team will see the results of the pen testing, and the security team maintains visibility into remediation progress. This centralized view of application vulnerabilities provides a better understanding of risk and can be rolled up to broader vulnerability reporting across your organization.

**The new application vulnerable items also get remediation target dates determined by previously-configured remediation target rules. These rules can apply different timelines based on factors such as criticality or asset. Automated assignment rules mean the correct development team has already been associated with the application, allowing the application vulnerability to be assigned to the right team for remediation automatically.**

# Get real-time insights on security posture and SOC performance via reporting

Visibility can be an elusive topic in security. You know you need it, but what exactly do you need to see to be successful? With the vast number of security tools used in modern enterprises—over 75 on average—understanding the big picture when it comes to security has become increasingly difficult. But it's more than just the big picture—you also need to tailor visibility to the viewer and their goals.

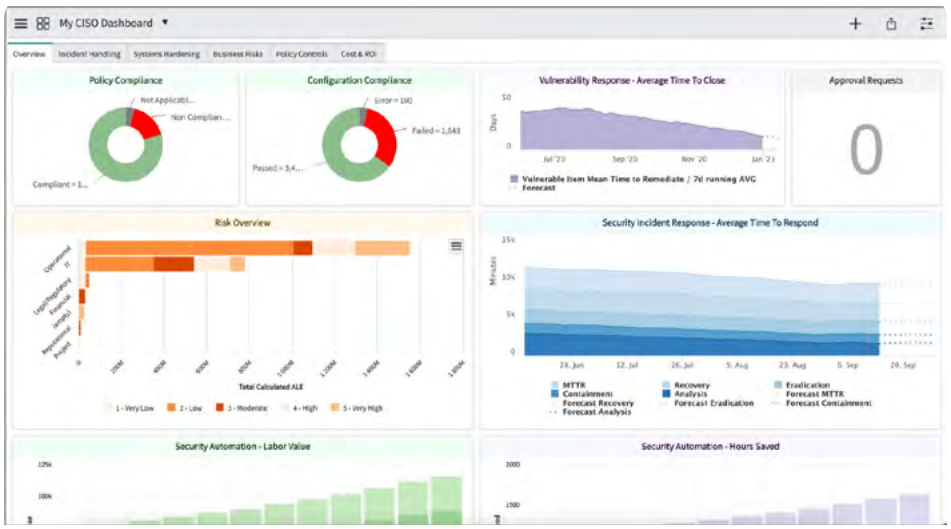
A 2021 report from the SANS Institute[4] looked at three key stakeholders and their expectations. Here are some of the needs by role:

- **Senior management:** industry security risk trends, security preparedness, organizational risk, and performance over time
- **Operational security teams:** near real-time view of vulnerabilities, events, and threats, plus signs of malware, misuse, or compliance failures
- **Analysts:** baseline behavior, device communication, and indications of the latest threat

Let's look at how ServiceNow provides the right level of visibility to these different roles.

## Senior management

An organization's CISO needs to provide an update to the board of directors on the status of the security program. They need quantitative metrics to back up the assessment of the organizations current risk exposure and security team performance. ServiceNow® Performance Analytics dashboards, built into ServiceNow Security Operations, simply and quickly deliver key performance indicators for security—such as the time to identify, contain, and eradicate security incidents. The data in these dashboards is tracked from the actual incident records, meaning it's accurate and up-to-date. Dashboards can also track security status via any number of statistics, including open incidents by priority, or open critical vulnerabilities.

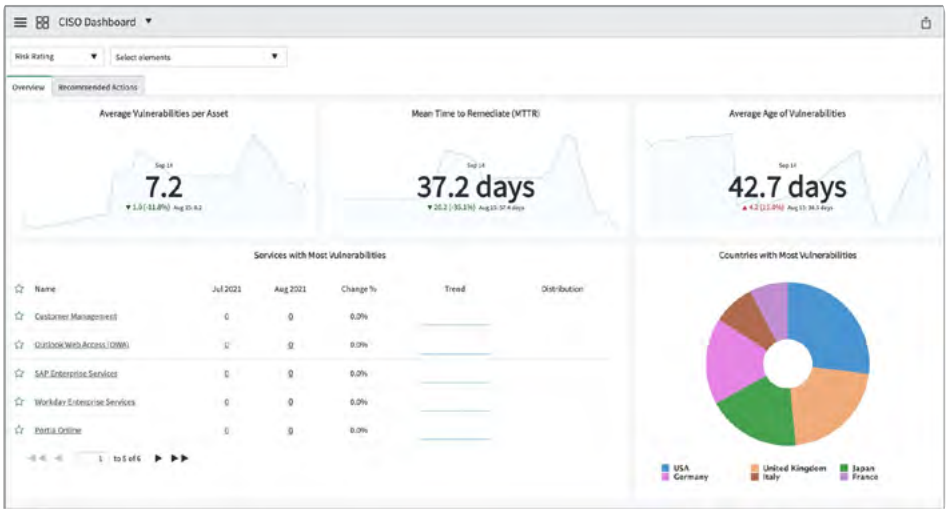



4 Filkins, Barbara and Pescatore, John, A SANS 2021 Report: Making Visibility Definable and Measurable

Risk exposure consists of multiple factors, including security incidents, vulnerabilities, and software configurations. Because all of these issues are prioritized by how critical they are to the business in the ServiceNow CMDB, the dashboard can show the current number of critical versus non-critical open issues across the organization. This data can also be used in ServiceNow Governance, Risk, and Compliance to track overall business risk. The CISO can also go one level deeper with reports, which can be created using any data tracked by ServiceNow. Reports can be scheduled to run automatically and be sent by email, so all stakeholders have the most recent data.

## Operational teams

A vulnerability manager needs to understand the current status of vulnerabilities and remediation. With ServiceNow Vulnerability Response, they can get real-time updates on remediation efforts, open vulnerabilities, and high-risk items. They can also understand what types of assets are impacted, see where they reside in the organization, and dig deeper to get details on each vulnerable item from the dashboard. Tracking of remediation targets allows them to see if there may be compliance issues from unpatched vulnerabilities.




## Analyst

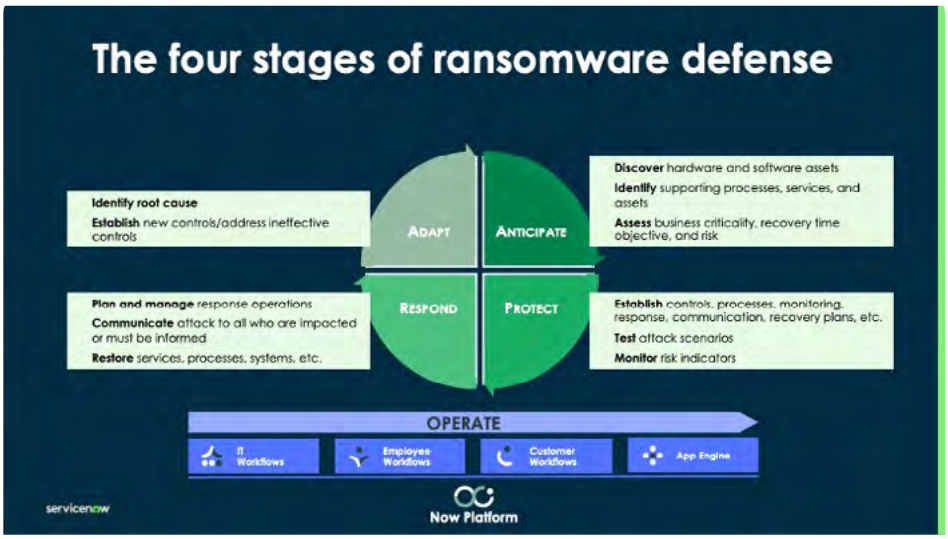
Security analysts need the greatest level of detail. If they're working on a security incident and want information on how a similar incident was resolved, they can leverage the Security Operations post-incident review. This review is automatically created at the close of each security incident and contains a time-stamped record of every action related to the security incident taken within ServiceNow, whether in security or IT. Assessments from incident responders can also be included as part of the post-incident review.

Analysts can also build their own custom reports and dashboards based on any information they have access to in ServiceNow with Performance Analytics. These can help identify patterns or potential issues

# Defend against high-profile cyberattacks and reduce your attack surface

High-profile cyberattacks such as ransomware have become big news, causing major disruption to business, government, and the general public. The total cost of ransomware was over $20 billion USD in 2021 and as much as $265 billion annually by 2031. Between expanding attack surfaces and the rise of ransomware-as-a-service, the risk will only continue to grow.

Adequately defending against these high-profile attacks requires organizational resilience, defined as "the ability of an organization to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper." This final use case requires all of the techniques we've covered, plus a few new ones. Let's look at how ServiceNow can help your organization successfully achieve resilience.




## Anticipate

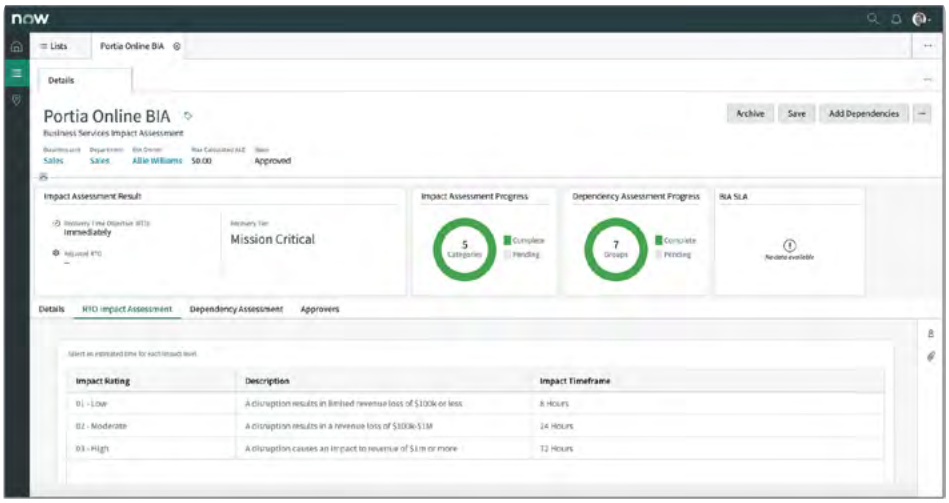
This first phase is around discovery and planning. It starts with understanding your attack surface by cataloguing all of your assets, whether on-premises or in the cloud, and understanding their relationship to each other and your business services. You can use ServiceNow® ITOM Visibility to discover end-to-end IT infrastructure and automatically map it to your digital services, creating a complete, accurate, up-to-date, and consistent record in the CMDB. ServiceNow IT Asset Management and Vulnerability Response can also keep records updated for an accurate hardware and software inventory, and they can help you find end-of-life assets that should be retired or replaced.

Knowing what you have and what needs to be protected allows you to perform a business impact analysis and create a business continuity plan with ServiceNow® Business Continuity Management. This may include running tabletop exercises and attack simulations to find weaknesses.

5 Cybersecurity Ventures, Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031, 2021

6 British Standards Institution, BS 6500

**You can use ServiceNow® ITOM Visibility to discover end-to-end IT infrastructure and automatically map it to your digital services, creating a complete, accurate, up-todate, and consistent record in the CMDB. ServiceNow IT Asset Management and Vulnerability Response can also keep records updated for an accurate hardware and software inventory, and they can help you find end-of-life assets that should be retired or replaced.**




## Prepare

The next phase helps you proactively reduce the risk of an attack. Harden your attack surface by reducing weaknesses due to vulnerabilities or misconfigurations. Use ServiceNow Vulnerability Response to prioritize vulnerabilities using severity, business criticality from your CMDB, and exploitability. Assign remediation tasks to IT owners automatically using machine learning and use orchestration to apply patches efficiently.

Use MITRE ATT&CK to find vulnerabilities related to ransomware or other high-profile attacks. Don't forget application vulnerabilities and weaknesses found through penetration testing.

You'll also need strong security controls and policies. With Continuous Monitoring, you can harvest key risk indicators from vulnerabilities to track additional business risk, whether due to a critical vulnerability or a missed remediation target. Vendors should also be assessed, as they may have sensitive information or privileged access to your systems. Collect vendor assessments via a self-service portal to ensure vendors are compliant with ServiceNow Vendor Risk Management. Assessments are scored automatically based on a weighted scoring framework backed by a configurable scoring methodology and risk engine. You can associate issues to risks, controls, and risk ratings at a questionnaire and assessment level to track vendor risk alongside internal risks.

## Respond

Reducing your attack surface consequently reduces your risk of attack, but you must be prepared to respond to anything that makes it through your defenses. Security playbooks allow you to build a response plan. When an incident is discovered, Security Incident Response can use automation to prioritize the incident using a risk score calculator and orchestration for quick enrichment with threat intelligence. Then your security analyst can follow the correct playbook to review and select response options to take quick action to contain or remediate the ransomware attack. They can also use the MITRE ATT&CK Navigator to understand tactics and techniques related to ransomware to help with with aligning the appropriate response to each threat as well as defense.

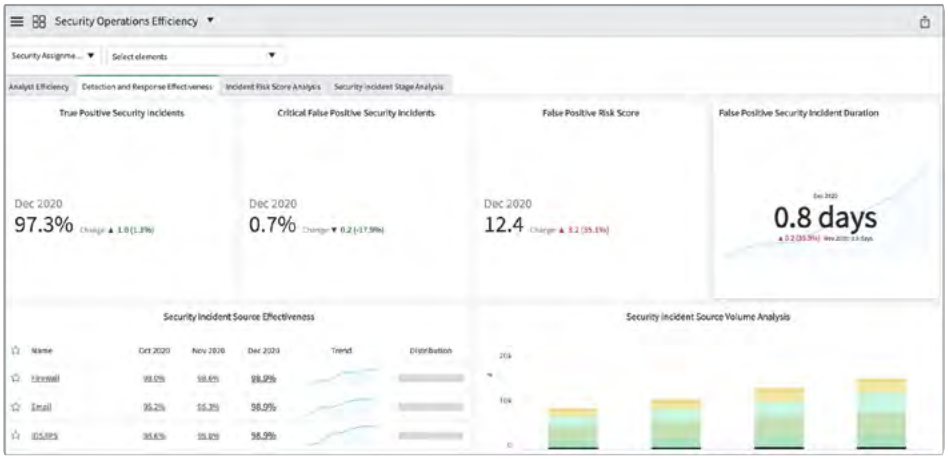
In parallel, activate the business continuity and disaster recovery plans you created in the anticipate phase. Whether you need to implement emergency changes with IT using IT Service Management or restart operations with IT Operations Management, working from a single platform lets you centrally manage your recovery efforts. ServiceNow also handles communication to business stakeholders to ensure all necessary parties stay informed, whether it's through Slack, Microsoft Teams, text messages, email, or mobile apps.

**When an incident is discovered, Security Incident Response can use automation to prioritize the incident using a risk score calculator and orchestration for quick enrichment with threat intelligence. Then your security analyst can follow the correct playbook to review and select response options to take quick action to contain or remediate the ransomware attack.**

## Adapt

Finally, you need to analyze a major event to help ensure it doesn't happen again. You can use Predictive Intelligence and machine learning to help the system better recognize threats to improve automated triage in the future and eliminate false positives.

With ServiceNow Performance Analytics, you can uncover areas for improvement and be even better prepared for the next high-profile attack. View dashboards and reports to understand how the SOC is performing. Were teams able to respond quickly? Were there process bottlenecks that can be addressed? Reports and dashboards can assist with both a post-event analysis as well as with reporting to executives or the board of directors for current and future resource and tools planning.




## Mature your security posture with ServiceNow

Good security hygiene requires ongoing effort, but workflows, automation, and a single platform for managing assets, vulnerabilities, security incidents, and risk can make the process easier. By integrating the tools and teams involved, you can better understand your risks and work efficiently to prioritize and remediate issues before they become a breach.

The Now Platform lets you bring together security, IT, and risk for a holistic approach to keeping your organization safe. From asset discovery to vulnerability management to integrated risk management, ServiceNow can make your people and processes more efficient.

To learn more, visit: www.servicenow.com/sec-ops

servicenow