

Security Operations Use Case Guide



Resolve security incidents and vulnerabilities fast with ServiceNow® Security Operations

Responding to security incidents and vulnerabilities is an ongoing process. 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 more efficient and able to respond more quickly.

ServiceNow Security Operations is a security orchestration, automation, and response engine built on the Now Platform®. 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. With ServiceNow Security Operations, you can identify, prioritize, and respond to threats quickly to reduce risk.

As Security Operations is part of the Now Platform, it can leverage the ServiceNow® Configuration Management Database (CMDB) to map threats, security incidents, and vulnerabilities to business services along with IT infrastructure. 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 also makes handing off tasks to IT simple and adds the benefits of visibility, service level agreement tracking, and live collaboration tools.

Workflows, automation, and orchestration speed up analysis, containment, and eradication. Automatically correlate threat intelligence from multiple sources, 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 performance with 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 Security Operations for faster security response.

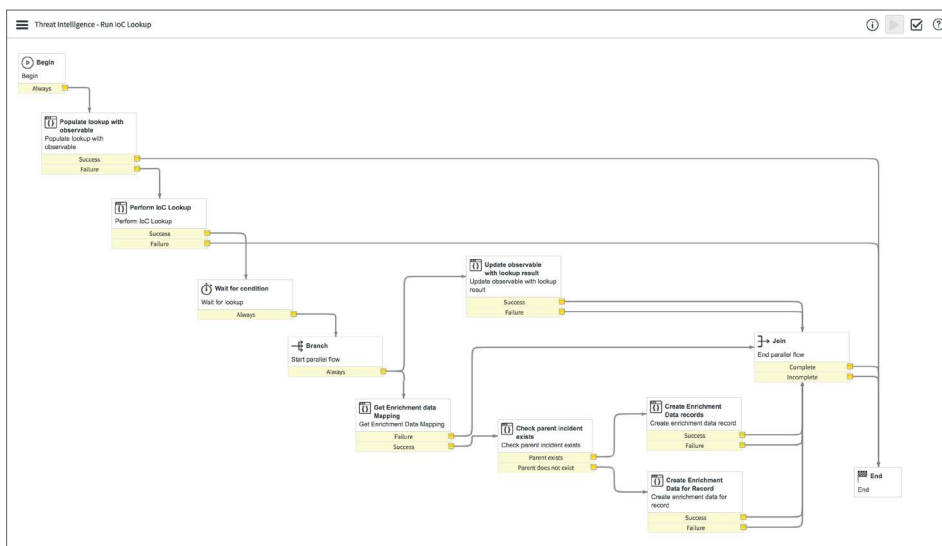
- 1. Automating threat analysis**
- 2. Phishing response and remediation**
- 3. Responding to misconfigured software**
- 4. Addressing a high-profile vulnerability**
- 5. Managing routine vulnerability scan results**
- 6. Improving security visibility**

Automating threat analysis

Security incident triage and analysis is a necessary step in the response process to weed out false positives, and to determine how best to contain and remediate an incident. A 2017 survey from SANS reported the median time from detection to containment was 6 to 24 hours¹.

Most organizations already use threat intelligence feeds as part of their incident response process. Correlating that information automatically and leveraging threat enrichment from other security tools can dramatically reduce the time spent on analysis.

An organization using ServiceNow Security Operations receives an alert about a suspicious file from their Security Information and Event Manager (SIEM), 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.



The first workflow performs IoC lookups against threat intelligence feeds the organization has connected to the Threat Intelligence application. In parallel, the IoCs can also be sent to other security tools for additional reputational data, including VirusTotal, Palo Alto Networks WildFire™, and more.

A second workflow uses Tanium Incident Response™ and Windows Management Instrumentation (WMI) to get the running processes and network statistics from the affected endpoint to see what activity may have been caused by the suspicious file. Another workflow performs a sightings search against the IoCs to see if there is a wider outbreak in the network.

¹ The Show Must Go On! The 2017 SANS Incident Response Survey, June 2017

All of the resulting data is reported back to ServiceNow Security Operations within seconds and is displayed in the security incident record. Now, a security analyst can view all of the data in one place and determine the next steps to take in the response process.

Running Processes						
<input type="checkbox"/>	Path	Command ...	Owner	PID	Parent PID	Security Tags
<input type="checkbox"/>	C:\Windows\sysste...	C:\Windows\sysste...	SYSTEM	456	368	UNKNOWN
<input type="checkbox"/>	C:\Windows\sysste...	C:\Windows\sysste...	LOCAL SERVICE	856	456	UNKNOWN
<input type="checkbox"/>	C:\Windows\sysste...	!?\C:\Windows\sy...	SYSTEM	1748	320	UNKNOWN
<input type="checkbox"/>	C:\Windows\Syste...	C:\Windows\Syste...	NETWORK SERVICE	3676	456	UNKNOWN
<input type="checkbox"/>	C:\Windows\sysste...	\	Administrator	2400	1056	UNKNOWN
<input type="checkbox"/>	C:\demo\agent\jre...	\	SYSTEM	6932	2540	UNKNOWN
<input type="checkbox"/>	C:\Windows\sysste...	\	SYSTEM	6720	2968	UNKNOWN
<input type="checkbox"/>			SYSTEM	4	0	UNKNOWN
<input type="checkbox"/>	C:\Windows\sysste...	C:\Windows\sysste...	SYSTEM	472	368	UNKNOWN
<input type="checkbox"/>	C:\Windows\sysste...	C:\Windows\sysste...	NETWORK SERVICE	964	456	UNKNOWN

1 to 10 of 50

Phishing response and remediation

Spear phishing is the most common vector in targeted attacks². Email security products can catch many of these attempts, but organizations are dependent on vigilant users reporting those phishing messages that slip through. Making it easy to report possible phishing emails encourages employees to participate, but how do you triage messages to find the real threats?

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 to extract information, including any security observables or Indicators of Compromise, to create a new security incident. These observables are automatically submitted to third-party threat intelligence vendors to determine if the email is malicious.

Observable	Observable Type	Finding	Incident Count
www.bbqdzx.com	Domain name	Malicious	24
10.227.49.115	IP address (V4)	UNKNOWN	25
2bc3f9cfc688d7841c36f0ebe9daa9ec7553784f1be4c09...	SHA256 hash	Malicious	29
182.236.164.11	IP address (V4)	Malicious	23
107.179.62.12	IP address (V4)	Malicious	15
107.170.0.14	IP address (V4)	UNKNOWN	20

In parallel, the security incident is assigned to an analyst for remediation. The record now contains information the analyst needs to determine the right course of action, reducing the need for manual investigation and triage. The actual forwarded email is also available to view in the Security Incident Response application of Security Operations.

View Email X Email Search X

Select Action ▼ Run

Source

Message ID: <MWHPR16MB1389B2A90756945E78F47EFD90860@MWHPR16MB1389.namprd16.prod.outlook.com>
 Username: Suzzane Baker
 Type: received
 State: processed

Address

From: secops@secopsintegration.onmicrosoft.com
 To: secopsmarketing04@secopsmarketing04.service-now.com
 Subject: Change your office 365 password immediately

Body

Hi security team ,
 This email looks suspicious, please take a look

Additionally, the security analyst can run a sightings search 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.

Lastly, the security analyst can search the company's Microsoft Exchange Server from Security Incident Response to see who else received the message and if they opened it. Other instances of the phishing email can be deleted from the server to prevent additional recipients from opening it.

Email Search ↗

▼ Search Criteria 1

Select Action ▼
Run

[Clear all](#)

From

Subject ✕

Bcc

To

Cc

Search Date	Action	Emails Found	Query
○ ▼ May 09 at 03:49pm	Search	32	subject=Change your offic...

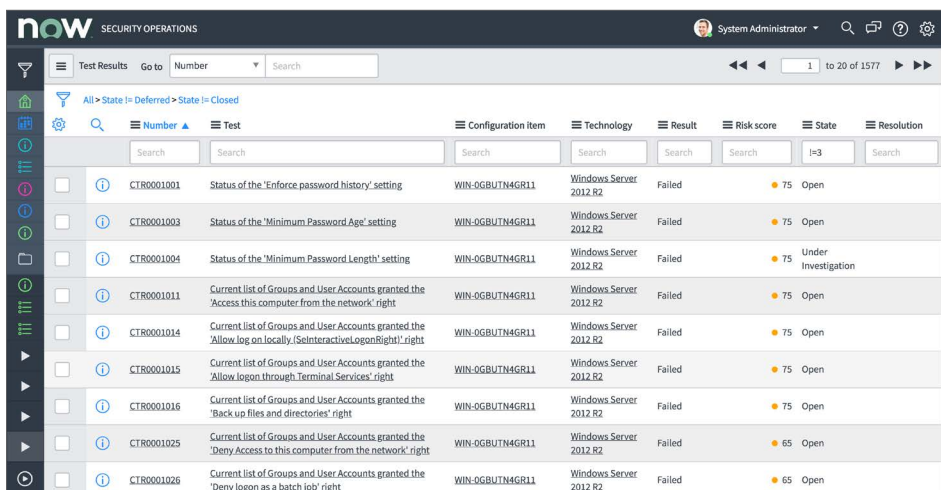
Recipient	Date Received	Email Read	Message ID	Deleted
arlene.watson@se...	Apr 30 at 01:36pm	external recipient/...	438c4d4cc4c0455...	No
ibrahim.jabber@se...	Apr 30 at 01:36pm	external recipient/...	438c4d4cc4c0455...	No
maurice.marin@se...	Apr 30 at 01:36pm	external recipient/...	438c4d4cc4c0455...	No
richard.reybok@se...	Apr 30 at 01:36pm	external recipient/...	438c4d4cc4c0455...	No
cj.desai@secops.c...	Apr 30 at 01:36pm	external recipient/...	438c4d4cc4c0455...	No

When the security incident is resolved and 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.

Responding to misconfigured software

Misconfigured software can leave an organization open to attackers in much the same way as vulnerabilities. These configuration issues include incorrect permissions, weak passwords, access controls, and more. An organization sets policies to define secure configurations (for example, minimum password length requirements), and then runs a scan using a security configuration assessment tool to test assets against these policies to find any misconfigured assets.

Next, an enterprise configures their security configuration assessment tool to integrate with ServiceNow Security Operations. The scan data is then imported into the Configuration Compliance application, where failed configuration test results are matched against assets in the ServiceNow Configuration Management Database (CMDB). Data from the CMDB determines how important each asset is to the business, and that business criticality is one factor in the risk score used to prioritize failed results.



Test	Configuration item	Technology	Result	Risk score	State	Resolution
CTR0001001	Status of the 'Enforce password history' setting	WIN-0GBUTN4GR11	Windows Server 2012 R2	Failed	75	Open
CTR0001003	Status of the 'Minimum Password Age' setting	WIN-0GBUTN4GR11	Windows Server 2012 R2	Failed	75	Open
CTR0001004	Status of the 'Minimum Password Length' setting	WIN-0GBUTN4GR11	Windows Server 2012 R2	Failed	75	Under Investigation
CTR0001011	Current list of Groups and User Accounts granted the 'Access this computer from the network' right	WIN-0GBUTN4GR11	Windows Server 2012 R2	Failed	75	Open
CTR0001014	Current list of Groups and User Accounts granted the 'Allow log on locally (SInteractiveLogonRight)' right	WIN-0GBUTN4GR11	Windows Server 2012 R2	Failed	75	Open
CTR0001015	Current list of Groups and User Accounts granted the 'Allow logon through Terminal Services' right	WIN-0GBUTN4GR11	Windows Server 2012 R2	Failed	75	Open
CTR0001016	Current list of Groups and User Accounts granted the 'Back up files and directories' right	WIN-0GBUTN4GR11	Windows Server 2012 R2	Failed	75	Open
CTR0001025	Current list of Groups and User Accounts granted the 'Deny Access to this computer from the network' right	WIN-0GBUTN4GR11	Windows Server 2012 R2	Failed	65	Open
CTR0001026	Current list of Groups and User Accounts granted the 'Deny logon as a batch job' right	WIN-0GBUTN4GR11	Windows Server 2012 R2	Failed	65	Open

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.

Now that responders have a prioritized list of configuration test failures, they know which ones to address first. They can group together failures based on the teams that will address them. For example, failures on the supply chain and manufacturing application servers can begin remediation using the workflows and automation built into ServiceNow. If remediation requires action from IT, the security analyst can easily create IT change tickets associated with the configuration items. Alternately, non-critical failures can be deferred to the next standard change window. 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, which then creates Key Control Indicators to automatically determine the compliance state of controls.

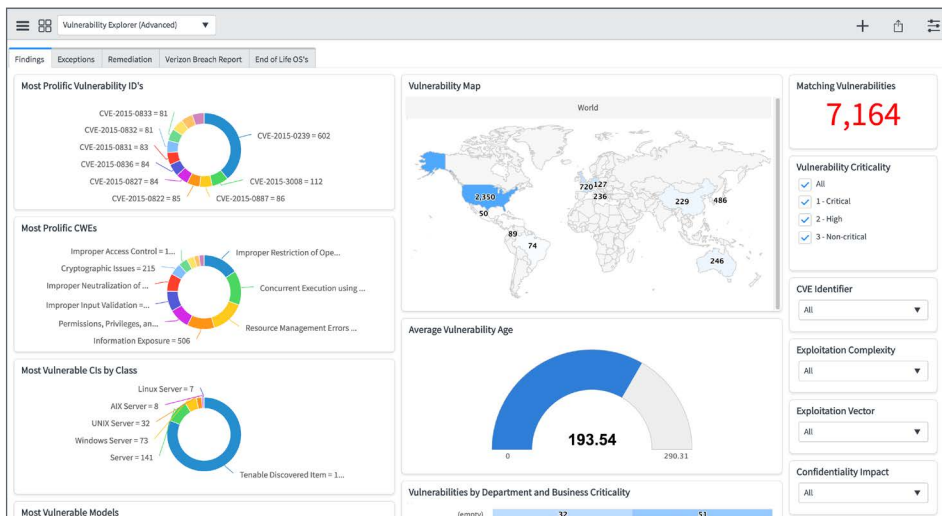
Learn more about ServiceNow GRC at servicenow.com/products/governance-risk-and-compliance.html

Addressing a high-profile vulnerability

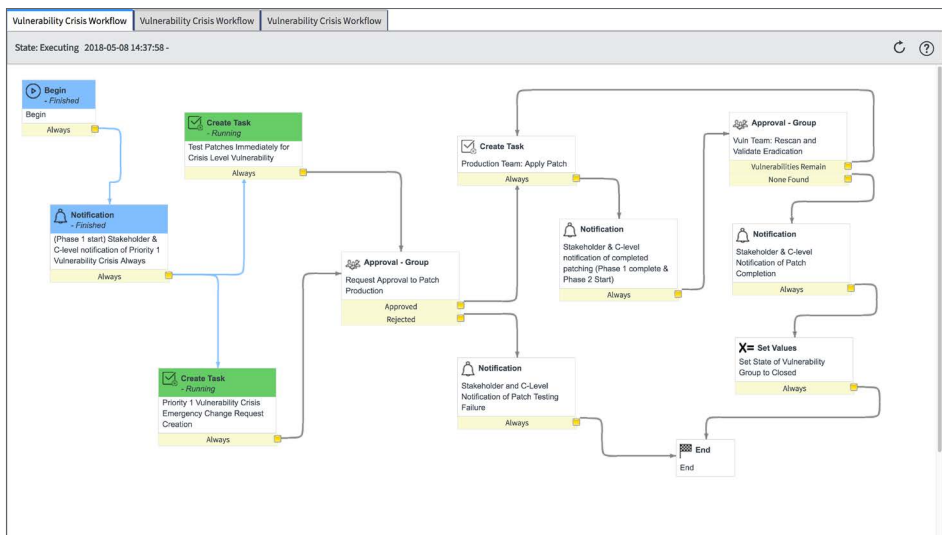
When news broke about two separate, but equally critical, vulnerabilities in early 2018: Meltdown and Spectre, the breadth and scope of their impact was difficult to imagine. Nearly three billion systems globally were potentially affected by the vulnerabilities, as both hardware and software providers scrambled to get patches into the hands of their customers. The question in many minds was, "how do we determine what our risk exposure is and, more importantly, how do we determine which systems to address first?"

With ServiceNow, a vulnerability scan data is automatically imported into the Security Operations Vulnerability Response application using APIs and is matched against both the ServiceNow Configuration Management Database. These resulting vulnerable items are assigned a risk score based on multiple factor, including the severity of the vulnerability, and the importance of the affected asset. The risk score is configurable and provides quick prioritization.

All of the 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), eliminating the need for manual research. The solution's configurable dashboards quickly show the organization's overall vulnerability exposure.



Security Operations workflows automate several of the next steps. For business-critical vulnerable items, 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.

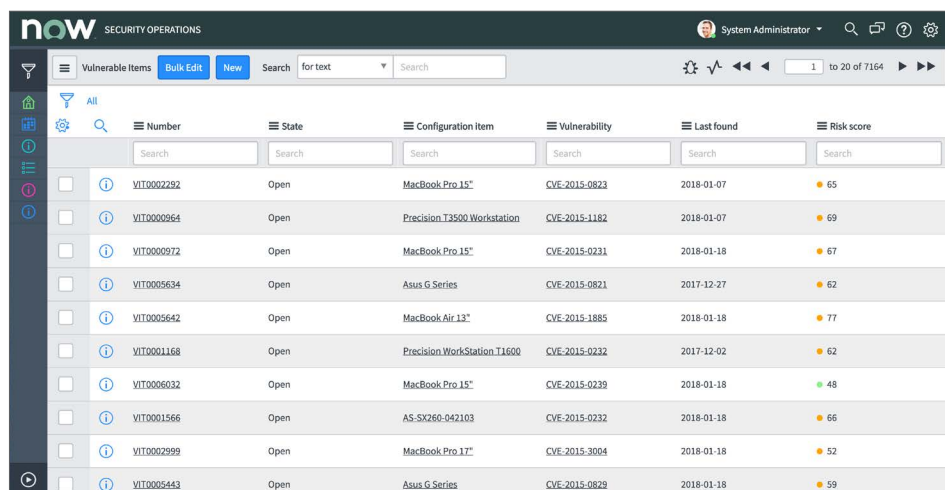


Managing routine vulnerability scan results

Coordinating vulnerability response across teams is time consuming with up to 12 days lost in the effort, according to a study by the Ponemon Institute.³ The same study also found that the lack of visibility into affected assets and patching status allowed things to fall through the cracks. Improving visibility and coordination is essential to effective vulnerability response.

As part of the standard security practice, vulnerability scans are routinely done to determine the company's risk exposure. The CISO wants to ensure that vulnerabilities that could have a dramatic impact to the business are quickly identified and resolved.

Vulnerability scan data is automatically imported from a vulnerability scanner into the Security Operations Vulnerability Response application. Next, the vulnerability scan results are matched to the assets in the ServiceNow configuration management database (CMDB). These vulnerable items (a combination of a single vulnerability and a single asset) can be prioritized by risk score. The risk score is a calculation based on the danger of the vulnerability and criticality of the affected asset.



The screenshot shows the ServiceNow Security Operations interface. At the top, there's a navigation bar with 'now SECURITY OPERATIONS' and a user profile for 'System Administrator'. Below that, there's a search bar and a table of vulnerable items. The table has columns for Number, State, Configuration Item, Vulnerability, Last found, and Risk score. The items listed are:

Number	State	Configuration Item	Vulnerability	Last found	Risk score
VIT0002292	Open	MacBook Pro 15"	CVE-2015-0823	2018-01-07	65
VIT0000964	Open	Precision T3500 Workstation	CVE-2015-1182	2018-01-07	69
VIT0000972	Open	MacBook Pro 15"	CVE-2015-0231	2018-01-18	67
VIT0005634	Open	Asus G Series	CVE-2015-0821	2017-12-27	62
VIT0005642	Open	MacBook Air 13"	CVE-2015-1885	2018-01-18	77
VIT0001168	Open	Precision WorkStation T1600	CVE-2015-0232	2017-12-02	62
VIT0006032	Open	MacBook Pro 15"	CVE-2015-0239	2018-01-18	48
VIT0001566	Open	AS_SX260-042103	CVE-2015-0232	2018-01-18	66
VIT0002999	Open	MacBook Pro 17"	CVE-2015-3004	2018-01-18	52
VIT0005443	Open	Asus G Series	CVE-2015-0829	2018-01-18	59

In addition to prioritization, matching vulnerability scan data against the CMDB can also help IT Operations personnel to determine which configuration items can be added or pruned from the CMDB, as the vulnerability scanner offers a near-real-time snapshot of the organization, improving overall accuracy.

Additional information is added to the record, including details about the specific vulnerability and the National Vulnerability Database (NVD) Common Vulnerability and Exposure (CVE) number.

³ Ponemon Institute, "Today's State of Vulnerability Response: Patch Work Requires Attention," 2018

< ☰ National Vulnerability Database Entry
CVE-2015-2736

☰ ☰ ☰ ↑ ↓

ID	CVE-2015-2736	Date published	2015-07-05
CWE entry	Code ⓘ	Last modified	2016-12-27
Summary	The nsZipArchive::BuildFileList function in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 accesses unintended memory locations, which allows remote attackers to have an unspecified impact via a crafted ZIP archive.		

Common Vulnerability Scoring System ▼

Vulnerability score	9.3	Score generated	2016-10-19
Access vector	Network	Source	http://nvd.nist.gov
Access complexity	2 - Medium		
Confidentiality impact	Complete		
Integrity impact	Complete		
Availability impact	Complete		
Authentication			

With this information, the vulnerability manager can now determine which items to address first and can assign tasks to IT staff directly from Vulnerability Response, either manually or automatically. Change requests are associated with the vulnerabilities so security has visibility into the IT tasks. Groups of vulnerabilities can also be deferred to a later date, at which time the state will return to open.

Once the IT change request is completed, IT personnel updates the record, which notifies the vulnerability manager. A follow-up vulnerability scan is initiated manually or automatically to ensure the patch has been successfully applied.

Improving security visibility

"Forget detection," a headline in CSO Magazine declares, "visibility is the key to long-term protection." With the vast number of security tools used in modern enterprises, understanding the big picture when it comes to security has become increasingly difficult.

An organization's CISO needs to provide an update to the board of directors on the status of the security program. He needs quantitative metrics to back up his assessment of the organization's current risk exposure and security team performance. ServiceNow® Performance Analytics dashboards built into ServiceNow Security Operations are the easiest way to demonstrate key performance indicators for security like 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.



Risk exposure covers 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 Configuration Management Database (CMDB), the dashboard can show the current number of critical versus non-critical open issues. 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 same latest data.

If more granular data is needed on a particular security incident, a post-incident review is automatically created at the close of security incident. It 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.

Armed with this wealth of data, the CISO is prepared to present to the board and has improved visibility across his organization.

Learn more at servicenow.com/sec-ops

servicenow