ALCOR
ENABLING CLOUD

White Paper

Accelerate Enterprise Security Response With ServiceNow®

INTRODUCTION

Globally, the estimated cost of malicious cyber activity ranges from US $ 300 Billion to US $ 1 Trillion annually.[1]

The rise in cyber attacks worldwide have caused a severe cause of concern for private organizations as well as the government. The cyber security landscape is changing very rapidly, and companies worldwide need to cope up with these changing dynamics if they want to protect their data and systems from such security threats.

IT teams are under tremendous pressure to ensure that the user data and the IT infrastructure is protected and any security threat does not hamper the continuity of the business.

The average cost of a data breach is US $ 154 per record whereas; the total cost per data breach is US $ 3.79 Million[2]

While security teams are flooded with the information about cyber attacks and security threats, since the vulnerabilities lack business context, IT security teams struggle to know which ones pose the greatest threat to business continuity. For several organizations, the incident response is based upon informal processes which are largely manual – this has a serious impact on the effectiveness and efficiency of the response.

While many organizations worldwide have started investing in security to ensure early detection of cyber threats and quick resolution, the key questions such as “Is the security getting better or worse?”, “Is there any improvement in overall security?”, “What are the benchmarks to compare against?” are still not answered satisfactorily. Without the clear understanding of all such aspects, it is difficult for any organization to have a concrete plan for strengthening their IT infrastructure and improve their incident response time.

In this whitepaper, we will have a look at the key elements of an ideal security response and understand the risks associated with the manual processes in incident response. We will then review how automation can provide a viable solution to those issues and then have a deeper look at the recently launched Security Operations Solution offered by ServiceNow®.

KEY ELEMENTS OF EFFECTIVE SECURITY RESPONSE

In the case of any security breach, the time window available to handle serious vulnerabilities is extremely limited. The security teams need to take quick action to ensure that high-priority alerts are quickly taken care of before any serious damage is caused. However, because of poor coordination between the teams and heavy dependence on manual processes, there could be incorrect decision-making and delays in response times. Issues such as improper categorization of threats, unnoticed alerts, and incorrect prioritization cause loss of precious time. It also has a serious impact on costs, data loss, and staffing budgets.

If the IT teams are able to clearly visualize the complete IT infrastructure, have access to tools for streamlining the activity and are able to automate the response, then it can offer quick and effective incident response. The key elements of an effective security response include –

Complete understanding of the security posture

To be able to provide an appropriate response to a security threat, it is important that the IT and security teams have the accurate information about the threat as well as the infrastructure. They need to get a clear picture of the security posture and need visibility across all the products and their inter-dependencies. A dashboard which can clearly display incidents and vulnerabilities along with the response data can help them assess which assets are under threat or which are not.

Centralized Platform

To be able to effectively collaborate and coordinate, it is important that the security and IT teams have access and view of the same data sets. Having said that, the data access should be controlled as per the roles and responsibilities. The teams should also be able to easily track each item along with the action taken.

There needs to be a strong interoperability across cyber security and ITSM technology components. So, an integration of cyber security and IT operations can facilitate seamless detection and efficient response to security threats.

Strong Team Collaborations

Apart from the technology integration mentioned, there also needs to be a strong collaboration between the incident response and IT operations teams. While the security teams can identify the issue, the IT operations team need to immediately get into action to work with them to prioritize the event, appropriately start or stop the systems, and take actions.

Security Response Automation

With predefined and automated incident response workflows, organizations can be sure of consistent remediation and compliance with security policies. Automation allows staff optimization since the junior staff can easily manage the workflows of the routine incidents and the senior staff can focus on complex issues. Automation of security responses ensure that the systems and resources are appropriately prioritized and automated based on their criticality.

SECURITY RISKS WITH MANUAL PROCESSES

According to a study by Enterprise Strategy Group (ESG) of 180 security executives, 93% of respondents believe that their incident response effectiveness and efficiency is limited by the burden of manual processes.[3]

While the growing number of security attacks are leading to the awareness of the risks associated with delayed threat mitigation, security breaches and threats remain to be a very common occurrence. Organizations are investing heavily in tools and technologies to help them identify security vulnerabilities and threats. However, only identification is not going to be useful unless there is a strong and well-defined incident response workflow. There are several negative issues with manual incident response processes.

Higher Security Threats

In many organizations, security teams rely on emails, phone calls, and hundreds of spreadsheets for information about security products and hand offs. The Ponem on Institute found that, in such organizations, it takes an average of 206 days to spot a breach and an average of 69 days to contain it.

Productivity Loss

The unstructured and repetitive work without any prioritization not only increases security threats but also drains the productivity of the IT and security staff.

Coordination Issues

In the case of manual processes, the cybersecurity and IT teams have to spend a humongous amount of time in inter-team coordination, which causes a huge loss of time and efforts.

Monitoring Issues

Right from threat detection, investigation and remediation, all stages need to be closely monitored and statuses need to be reported appropriately. However, in the case of manual processes, it can become challenging for the stakeholders to get a clear picture of the current state as a lot of individuals work in silos.

Shortage of Skills and Talent

With growing security threats and new cyber attacks, it is important for organizations to ensure that they have the right talent on board who can help them prevent and mitigate the sophisticated attacks. However, such skills are in short supply and organizations often struggle to maintain the right mix of skills in a team. The hiring and training of the right staff is a time consuming and costly activity.

SECURITY INCIDENT RESPONSE AUTOMATION

As we saw in this paper, manual processes, lack of technology integration, and lack of coordination between the security and IT operations teams hamper the incident response efficiency and effectiveness. Acknowledging these problems, organizations are looking for ways to not only improve the productivity of their staff but also improve the incident response efficiency.

Considering the speed at which new attacks are surfacing and the shortage of cyber security skills, CIOs have realized that the best ways to tackle these issues are formalization, automation, and orchestration of incident response processes.

> By 2019, 40% of large enterprises will require specialized, automated tools to meet regulatory obligations in the event of a serious information security incident. – Gartner[5]

Implementation of automated workflows and system management capabilities allows organizations to map threats and security incidents to business services and IT infrastructure. Through such mapping, threat prioritization can be done in a more effective way and also ensures that security teams are focused on what has the most impact to the business.

Automation can help IT security teams in a variety of ways –

- It helps them be better prepared for attacks since it helps the teams simulate and test multiple scenarios and validate play books.

- It facilitates faster collection and analysis of data and then helps the teams quickly identify threats and measure the associated risks.
- It frees them up to prioritize a response that mitigates the damages.
- Automation enables 24X7 coverage because irrespective of who is on duty, automation enables fast and best practice response.
- It helps them achieve a better balance between detection and prevention.
- Through transparent and streamlined reporting, the key stakeholders are always aware of the exact situation with accurate information.
- Data analytics helps in getting clear visibility into the operational status and effectiveness of security controls across the environment.

To get automation right, security leaders must ensure a few things -

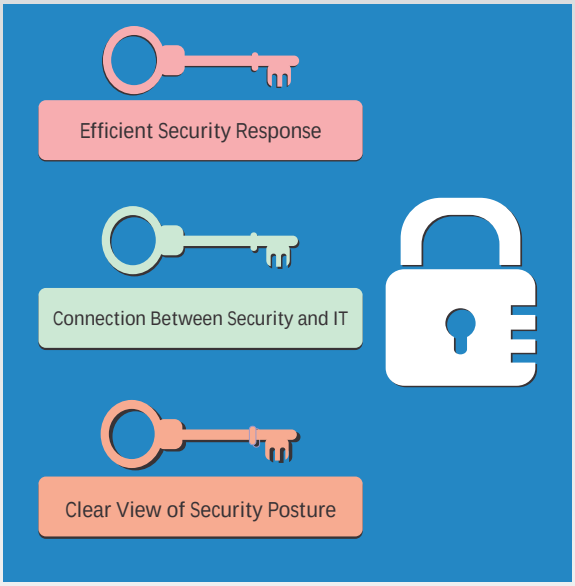
- The automation response workflow is customized as per the exact specifications of the security response run-book
- The platform tracks all activities in the complete lifecycle of the incident response right from analysis, investigation, containment, and re-dedication of the incident.
- The platform automatically documents the Post Incident Review (PIR) document mentioning all the incident related activities.

INTRODUCING SERVICENOW® SECURITY OPERATIONS

Manual processes to incident response are not only time consuming but also limit the organization's ability to effectively and efficiently respond to security incidents and threats.

ServiceNow® Security Operations help organizations in accelerating response to security vulnerabilities.

- It connects the workflow and systems management capabilities of the ServiceNow® platform with security data from leading vendors.



- It offers a single platform that can be shared between security and IT making the collaboration between the two teams easy and effective.
- It helps in increasing the team productivity because everyone involved has a better visibility, the workflows are well-defined, and there is an automated threat intelligence. The teams can spend their time in preventing the advanced attacks rather than spending time in managing simple tasks.
- Customizable reports and dashboards offered by ServiceNow® Security Operations clearly display the current security status, including critical versus non-critical issues. Using these dashboards, security teams can quickly prioritize incidents and vulnerabilities based on their potential business impact and speed up the remediation tasks to resolve the issues quickly.

The top benefits of ServiceNow® Security Operations include -

Connection Between Security and IT

The ServiceNow® Security Operations suite acts as a single platform to hand off tasks easily between security and IT. While offering the complete flexibility of data sharing, it ensures data security through tight access control. SLA tracking promotes accountability across the organization.

Efficient Security Response

The security suite allows seamless integration with a variety of security and vulnerability products allowing organizations to leverage their existing investments. Through automatic access to threat intelligence data, it allows organizations to enrich their security incidents. With the use of orchestration tools, organizations can save a huge amount of time and costs by reducing the time spent on basic tasks.

Clear View of Security Posture

The powerful reporting and role-based dashboards allow the organization stakeholders get a clear picture of the overall system security. It allows them to closely monitor the functioning of the critical assets.

The key components of ServiceNow® Security Operations include -

Security Incident Response Application

Security Incident Response helps in simplifying the identification of critical incidents and provides workflow and automation tools to speed up the rededication.

- It allows the import of the data from existing security point products or Security Information and Event Management System (SIEM).
- It allows teams to create customized workflows based on the organization's specific security run-book.
- The easy tracking of tasks allows everyone get a clear picture – it also sends reminders to assignees for incomplete tasks or it can escalate tasks if necessary.
- It facilitates smooth collaboration between the teams through the ServiceNow platform via conference calls or Connect chat.
- It automates the basic tasks, including approval requests, malware scans, or the retrieval of running processes. This allows the security teams to spend their time on more complex threats.
- Not only are the activities in an incident lifecycle tracked from beginning to end, but once the incident is closed, the system automatically generates a post-incident review (PIR) report as a historical audit record.

Vulnerability Response Application

The Vulnerability Response application helps in the prioritization of vulnerable items and helps in addinga business context to that. It, thus, helps the security and IT teams determine if business critical systems are at risk.

- It automatically identifies dependencies across systems and quickly assesses the business impact of changes or downtime.
- It offers a complete view of all vulnerabilities not only with respect to the given service but also all the vulnerabilities affecting the organization.
- When critical vulnerabilities are found, the system automatically initiates an emergency patch approval request. Once the request is approved, orchestration tools automatically apply the patch and trigger an additional vulnerability scan to ensure the issue has been resolved.

Threat Intelligence Application

The threat intelligence application included in ServiceNow® Security Operations helps incident responders find Indicators of Compromise and identify low-lying attacks and threats. When an indicator is connected to a security incident, it automatically searches for relevant information. Through support for multiple threat feeds as well as STIX and TAXII, it comprehensively incorporates threat intelligence data from a variety of sources. Apart from this, companies can also add their own custom feeds.

Performance Analytics for Security Operations

Performance Analytics allows the creation of advanced real-time dashboards and reports. Apart from the included built-in key performance indicators (KPIs), it also allows the creation of additional custom KPIs and allows organizations track the specific metrics which are most important for them. Using the historical data, organizations can do a deeper analysis and identify the tasks most suitable for automation.

ALCOR'S EXPERTISE IN THE SERVICENOW® SECURITY OPERATIONS SUITE

The key concern every CISO or other security professionals asks themselves is “Are we secure and are things getting better or worse?”. Events and alerts are being generated from dozens of security products and creating work for the security and IT teams. In many cases, organizations are getting thousands of alerts per day and people can’t scale to meet the volume. There is a clear need for something beyond enforcement, detection and visibility. It’s response.

With ServiceNow® Security Operations, security professionals bring incident data from their security tools into a structured response engine that uses intelligent workflows, automation, and a deep connection with IT to prioritize and resolve threats based on the impact they pose to your organization.

Alcor has a structured approach to help your organization leverage the ServiceNow® Security Operations suite. We integrate your security products to bring security incidents from your existing security tools so that you can automatically prioritize security incidents based on business impact. Automated response workflows and threat analysis drive comprehensive response actions based on industry data and business priority.

Remediation tasks are assigned to the appropriate teams and post incident reports are dynamically built for audit purposes to close out the security incidents. All information can be tracked in executive and operational dashboards to ensure the right information goes to the right teams.

Alcor takes a strategic service management implementation approach and focuses on solving the business problems of their clients by leveraging an integrated business process design and technology implementation capability.
Alcor offers strategic security consulting, security response design and implementation, and security incident analysis managed services.

CONCLUSION

With growing security attacks and vulnerabilities, organizations have started investing heavily in tools for security threats identification and rededication. However, the key question which bothers them is “Are we getting better at security or worse?”. Simply investing in tools and technologies to identify more threats is not sufficient. Organizations need a solid back end infrastructure and workflows to support faster re-dedication. They need to stop relying on the manual processes in incident response because manual processes not only cause inordinate delays but also cost business continuity and money.
Apart from the manual processes, another reason why organizations are not able to offer efficient and effective incident response is the non-coordination between the security and IT teams. Automation plays a big role in resolving all such issues and helps organizations in faster and more efficient incident response. ServiceNow®, the leading IT Service Management Platform, has recently launched it’s ServiceNow® Security Operations. With ServiceNow® Security Operations Suite. Organizations can replace their manual response patterns with intelligent automated workflows, and respond to threats in a faster and more efficient manner.

ABOUT ALCOR SOLUTIONS

Alcor is a global cloud advisory and implementation services company serving Fortune 500, Government Agencies, and other leading organizations in multiple industry verticals across the Americas, Canada and India. Alcor is a ServiceNow® Gold Services Partner and also partners to Salesforce®, FireEye™, Microsoft®, Dell Boomi, BOMGAR®, and BigPanda® amongst others. They advise leading businesses on cloud platforms, architecture, enterprise service management and integrating IT service delivery. They also provide business process consulting to capture, re-engineer and improve processes that can easily be automated to deliver real value. The Alcor consulting team has excellence in Business strategy, Cloud Technology and Organizational Change Management.

For more information, connect with them at information@alcortech.com.

REFERENCES

1. https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

2. http://www.csoonline.com/article/2926727/data-protection/ponemon-data-breach-costs-now-average-154-per-record.html

3. http://www.businesswire.com/news/home/20161006005128/en/100-North-American-Professionals-Surveyed-ESG-Admit

4. https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

5. #G00251917 April 10, 2015. Analyst: Rob McMillan

ALCOR
ENABLING CLOUD

Alcor is a technology implementation company focusing on Enterprise and Government technology needs in ITSM, systems integration, web development and mobility space. We provide a strategic ITSM implementation approach to our clients and focus on solving business problems by leveraging an integrated business process design and technology implementation capability.

7600 Dublin Blvd, Suite 230 Dublin, CA 94568 / (925) 248-2344, (925) 361-7247

The Dineen building, 140, Younge Street, Suite 200, Toronto, Ontario, MSC 1X6 / (905) 867-3990

308, Hemkunt Chambers, 89, Nehru Place, New Delhi-110 019

www.alcortech.com