Making Security Operations More Responsive, Efficient, and Business Aligned - With Performance Analytics

CONTENTS

INTRODUCTION

A December 2016 threat report found that 67% of the surveyed organizations had reported a rise in the number of security incidents they had to deal with, and 93% of the surveyed organizations believed that they were not in a position to triage all the possible threats they were encountering- The McAfee Labs Threats Report: December 2016[1]. It seems to be clear that the security threats organizations face are on the rise and that businesses are having difficulty in detecting, isolating, understanding, and fixing these threats.

This Whitepaper will examine some of the organizational challenges in the face of such threats. It will then attempt to make the case for Performance Analytics as an effective way to address these challenges in a timely fashion without any adverse impact to strategic business objectives and priorities.

THE SECURITY OPERATIONS CHALLENGES FOR ENTERPRISES

Wikipedia defines a Security Operations Center as, "A SOC is related with the people, processes and technologies involved in providing situational awareness through the detection, containment, and rededication of IT threats. A SOC manages incidents for the enterprise, ensuring they are properly identified, analyzed, communicated, actioned/defended, investigated and reported. The SOC also monitors applications to identify a possible cyber-attack or intrusion (event) and determines if it is a real, malicious threat (incident), and if it could have a business impact."[2]

The definition establishes how Security Operations focuses first on finding, isolating, and fixing security threats, and then on documenting those for categorization and analytics aimed at improving future incident-readiness.In this context Enterprises and smaller organizations face several challenges with being incident-ready.

Dynamic nature of threats: The nature of threats organizations have to deal with is constantly shifting as different types of malware get created all the time. Malicious code is also being camouflaged in more creative and hard to detect ways. Vincent Weafer, VP of Intel Security's McAfee Labs pointed to this when he said, "The more authentic a piece of code appears, the more likely it is to be overlooked."

Further, he added, “2016 saw more ransomware become sandbox-aware, the need to conceal malicious activity is driving a trend toward 'Trojanizing' legitimate applications.” Enterprises are forced to deal with these shifting goal-posts, and continuously improve their own capabilities to identify and address threats.

Volume: McAfee's December 2016 report found that there was an 80% increase in the number of new ransomware samples over 2016 and that adware drove a 637% increase in Mac OS malware. This surge in the number of security threats means organizations have to deal with a much greater volume of incidents. This puts pressure on the organization to respond at speed. It also puts pressure on the organization to define priorities among the various threats so that the most severe threats or those threats likely to affect the most users can be addressed first.

Complexity: As the IT infrastructure becomes more complex with the introduction of Cloud, Social, and Mobile strategies, the nature of the threats the organization has to face also becomes more complex. This is presenting a major challenge for these organizations. The Ponemon Institute for Lookout reported last year that 56% of corporate data was accessible over mobile devices but more than 1/3rd of organizations did not have formal policies for securing this data. In “A National Issue” in The Cipher Brief, Jon Olstik reported that 33% of organizations found that their greatest skills shortage was in the area of Cloud Security.

Reactive mode: As a direct consequence of the complexity, lack of skills, and sheer volume of threats organizations are forced to address these threats only when they occur. They function in a reactive mode rather than plan in proactive mode and this inevitably leads to delays. Ponemom Institute's 2016 Cyber Security Trend Report found that financial companies took an average of 98 days to detect data breaches. Retail organizations took as many as 197 days on average to detect such a breach. This delayed response carries the threat of greater damage being caused.

Inefficient Processes: The security-related processes within organizations are still largely manual. There are also gaps that exist between the organizational IT teams and the security teams – this leads to issues of trust as well as operational efficiency. For example, a SolarWinds study within the US Federal government staff reported that 48% of the staff believed that their security concerns were the direct result of IT modernization efforts. This creates operational inefficiency which leads to long detection cycles and further delayed response times.

Lack of real-time visibility: A lack of automation of processes leads to a lack of transparency. Gathering information is slow, inefficient, and even incomplete. The security team may be unable to accurately state the threat perception at any specific point in time or to project forwards to situations likely to develop from the current status as a consequence.

Alignment with business objectives: Given the volume of threats it is important to be able to direct the resources to address those threats that hold the most potential to impact business metrics. This calls for the ability to define priorities based alignment with the business values. A reactive, case-by-case, approach to addressing security threats prevents such effective alignment.

“PERFORMANCE ANALYTICS” AND WHAT IT ENTAILS

Wikipedia defines Analytics as, “the discovery, interpretation, and communication of meaningful patterns in data.”[3] Taking this further in the context of Performance Analytics, specifically for IT infrastructure and systems, we can say that Performance Analytics is a process of using performance data, to understand how the IT systems and infrastructure are performing, to continuously make them better. By linking data to organizational priorities, collecting and analyzing, data and metrics, and defining the desired outputs and results, the IT department can use performance analytics to align the resources, priorities, investments and efforts for optimum performance in the furthering of specific business goals.

There are some key points that emerge from this definition.

First, it is key to define exactly which metrics matter. This means identifying the systems that contribute to the delivery of the business service and the optimum required performance level they need, to perform at, for the service delivery, and then to identify which metrics to track for those systems. Identifying the right metrics often calls for understanding the business needs. There are multiple metrics IT systems measure and report – the need is to identify exactly which are relevant for the business service. For example, metrics like load-handling capacity may be more relevant to customer-facing systems but the speed of output may be more relevant to systems involved with financial transactions.

The next step is to define the best way to collect these metrics. There may be multiple sources for the same pieces of performance data and in some cases, these may be out of synch with each other due to specific local issues. Under such situations, the need is to identify exactly which data is the most relevant data and to set into place an automated process to collect that data.

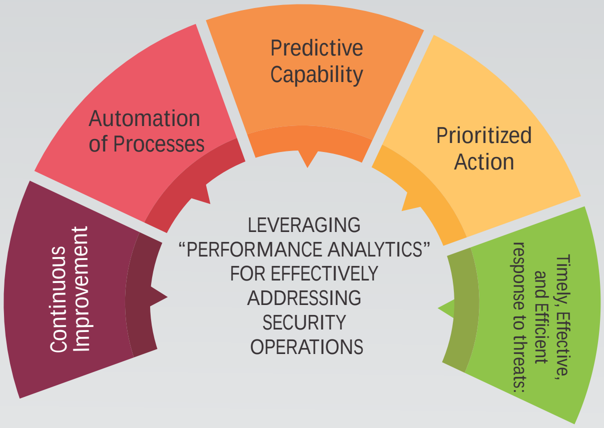
Then, coming to the Analytics part of the activity – once the right data has been gathered, the need is to organize it and to look for the trends hidden therein. The objective is two-fold – to identify trends in past performance and the factors influencing that performance, and then to use these insights to project forward to the future. One important part of this is how these insights are communicated to the IT department. These need to be delivered in easy-to-understand visualizations and dashboards, so that the IT department can get an unambiguous view of what is needed. This allows the IT department to anticipate possible problems and to proactively address or mitigate against conditions that could adversely impact performance.

With such a spread and depth of historical data, real-time data, and forward-looking projections available, Enterprises can also address Security Operations more effectively. A tightly integrated approach provides the IT & Security teams' comprehensive reports as well as Analytics. This allows them to benchmark themselves against industry best-practices, measure their performance against pre-determined goals, and also plan better for the future based on data-driven insights.

It is necessary to view all these activities through the prism of the business needs. The specific systems that contribute to the performance of business service delivery, the performance they need to maintain to ensure continued service delivery at the required service level and the possible future conditions, including security threats, that could impact those business services have to be always kept in focus. This is key because the insights gained from Performance Analytics are then used to organize the available resources, priorities, and efforts so that the most important business goals are best served – aligning them specifically with the business priorities.

LEVERAGING “PERFORMANCE ANALYTICS” FOR EFFECTIVELY ADDRESSING SECURITY OPERATIONS

Previously in this White Paper, we have outlined several challenges Enterprises face in their quest to detect, identify, isolate, fix, and document security threats, given the volume and complexity with which they occur. The challenges are exacerbated by operational challenges like a misalignment between IT & Security. The wealth of operational data, real-time visibility, and predictive insights available to the Enterprise through the implementation of a robust and comprehensive Performance Analytics solution helps them address the operational challenges and become more effective.


Predictive Capability
Automation of Processes
Prioritized Action
Continuous Improvement
LEVERAGING "PERFORMANCE ANALYTICS" FOR EFFECTIVELY ADDRESSING SECURITY OPERATIONS
Timely, Effective, and Efficient response to threats:

This is achieved by:

Effectively integrating security & IT : The larger the Enterprise and the more complex the Infrastructure environment, the greater is the possibility of the creation of siloes, each addressing their own specific function or solution. An effective Performance Analytics solution will provide a common platform to bring together the IT & Security teams by integrating workflows, data from multiple sources, and the capabilities to manage the various systems at one place. This makes it possible to have greater coordination between these teams, clear demarcation of responsibilities, controlled access to security data, better tracking, and reduced ambiguity.

Clear security strategy: Improvement demands a clear understanding of the current situation – exactly what is the current level of security and where are the next threats likely to come from? With Performance Analytics come several dashboards, visualizations, and reports with varying degrees of customization. Real-time visibility across the Enterprise, forward-looking projections and the capability to maintain comprehensive records allow timely reaction to current threats as well as provide the opportunity to plan better for future threats.

Business alignment: Not all threats are created equal; in a resource-constrained environment the need is to focus the efforts on addressing those threats that are likely to have the maximum impact on business priorities. With the detailed insights provided by Performance Analytics and the deep integration with the overall operations focused on business services, it becomes easy for the security team to identify the likely business impact of each threat and then address them appropriately.

By leveraging Performance Analytics, Enterprises get :

Timely, Effective, and Efficient response to threats: Performance Analytics provides better visibility and better planning. As we have mentioned earlier, this also allows better alignment between the security teams. Both these promote faster response to current threats, as well as more proactive action for future threats.

Prioritized Action: The real-time visibility and the tighter integration with the business workflow provide more clear information about each threat and its likely business impact. This allows the security teams to focus their resources on the highest priority issues. This promotes more efficient utilization of resources.

Predictive Capability: Many Performance Analytics solutions provide information on industry best practices and KPIs. This, when combined with the real-time reporting and the deep insights allow the security teams to map their existing conditions and then project outwards to the future. This allows them to be ready for threats even before they occur.

Automation of Processes: The orchestration capabilities of Performance Analytics and the ability to create and integrate workflows allows the security team to automate a wide variety of basic tasks. The better visibility also allows better choices about the areas to automate for maximum impact.

Continuous Improvement: The security environment is made more complex by the dynamic nature of threats. As the nature of the threats is constantly changing the security organization has to constantly improve its responsiveness and effectiveness. The detailed reports, visualizations, and dashboards provided by a comprehensive Performance Analytics solution provide all the information the security organization needs to measure it, identify the areas that need to be improved, and progress on all ongoing improvement initiatives.

SERVICENOW® INTRODUCTION

IT Service Management is defined as a combination of people, processes, and tools that are deployed to support the production environment or for delivering other IT services to the organization's internal & external customers. ServiceNow® is aleading cloud-based ITSM tool focused on the enterprise.

ServiceNow® focuses on the workflows within the enterprise and helps enterprises define, codify and automate these workflows to ensure predictability and scalability on a day to day basis. Enterprises deploying leverage the capabilities of the product inIncident Management, Issue Management, Request Management, Knowledge Management and for Tracking and Reporting.

ServiceNow® focuses on a variety of business domains including Financial, Healthcare, Higher Education, Managed Services and various Government sectors.

SERVICENOW® PERFORMANCE ANALYTICS OVERVIEW

ServiceNow® Performance Analytics is an easy-to-use, integrated application designed for reporting and analyzing service performance in the ServiceNow® enterprise cloud[4]. It helps business leaders to visualize their data and implement continuous improvement programs so as to:

- Bring in improvements in the service delivery quality
- Enhance the speed of service delivery
- Reduce service delivery costs
- Maximize workforce efficiency

Some of the key features of ServiceNow® Performance Analytics are -

- Access to a large library of key performance indicators (KPIs) across business functions
- 350+ pre-defined KPIs for all major service management processes
- Mobile-enabled scorecards which help in getting up-to-date information and they also allow drill-down
- Responsive and interactive graphical dashboards
- Powerful analytics that offer actionable insights into how to improve the quality of business services

Performance Analytics helps business service owners access important and current information, from anywhere, anytime, and take real-time decisions that improve enterprise performance.

ServiceNow®'s Performance Analytics does not replace the reporting. It, in fact, complements the existing reporting. While the reporting engine translates the raw data into information, Performance Analytics translates the information into Insights to drive change in the business. Reporting offers ad-hoc reports and operational reporting, which is very relevant to the process managers, service managers, and project managers. Performance Analytics offers exceptions, role-based KPIs, targets and thresholds, which are relevant for IT strategy, IT Management, CIO, and Executive teams. With such insights, executives can spend more time in making plans rather than analyzing data.

Specifically in the context of Security Operations, ServiceNow® Performance Analytics for Security Operations carries "the world's largest library of key performance indicators (KPIs) and comes with more than 300 pre-defined best practice KPIs for security operations processes."[5]

The application offers mobile-integrated real-time reports that can be analyzed at even greater depth to deliver insights that can help security teams become more responsive and more effective. These insights cover security incidents as well as projections of possible vulnerabilities – this allows a greater degree of planning, and hence faster and more effective response.

ALCOR CAPABILITIES IN SERVICENOW® & PERFORMANCE ANALYTICS

Alcor is a global cloud advisory and implementation services company serving Fortune 500, Government establishments, 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® and Bomgar™. 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 is derived from a combination of experts in Business strategy, Cloud Technology and Organizational Change Management.

Alcor takes a strategic ITSM implementation approach and focuses on solving the business problems of their clients by leveraging an integrated business process design and technology implementation capability. Alcor's ITSM solutions with ServiceNow® leverage a business view of IT services. The objective is to enable the IT support organization to:

- Quickly resolve or escalate issues and problems
- Improve root cause isolation, and
- Provide higher levels of business user satisfaction.

Alcor brings substantial process expertise, ServiceNow® experience and depth of organizational governance modeling to build solutions that are effective and provide complete life cycle support for incident Management, Problem Management, Change Management and Configuration Management. Alcor has experience in Automating ServiceNow® with external applications like emails, active directories, Adobe, assets, and Amazon Cloud Provision (LABS). This includes real-world experience of having worked with enterprises in the banking and financial services and retail sector where we have helped orchestrate transaction volumes running into the 100's of thousands.

Alcor Solutions deploys the best in class enterprise solutions to exploit the full measure of Performance Analytics across the business to deliver optimum benefits. This customized business solution has helped their clients gain insights into the performance of the IT systems critical to several areas of business operations, like human resources, finance, legal and administration. Their solution provides both performance reporting and predictive analytics, which in turn help's their clients gain insights that can help them get maximum benefit from their investments into their IT infrastructure.[6]

Alcor achieves this by leveraging their integrated business process design and technology implementation capability. Their professionals are the top talents in the business with a deep personal understanding of the business verticals they service. This allows them to deliver flexible solutions that work in the real world. Their strength lies in delivering solutions that are customized to the specific requirements of their customers including complex integrations with the other systems in the eco-system like Financial and Procurement Management systems. You can get more information about Alcor and their capabilities by writing to information@alcortech.com.

CONCLUSION

Inventor John C. Lilly said, "Our only security is our ability to change." In the context of Enterprises facing a complex, and highly-charged security environment that change has to be driven by insights, if it has to be effective as well as resource-efficient. Performance Analytics provides all the data for organizations to make these considered decisions and stay secure.

REFERENCES

(1) https://www.mcafee.com/us/about/news/2016/q4/20161213-01.aspx

(2) https://en.wikipedia.org/wiki/Information_security_operations_center

(3) https://en.wikipedia.org/wiki/Analytics

(4) http://www.servicenow.com/products/performance-analytics.html

(5) https://www.servicenow.com/products/security-operations.html

(6) http://www.alcortech.com/performance-analytics-empowering-enterprise-it/

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.

Alcor believes information in this publication is accurate as of its publication date. This publication could include technical inaccuracies or typographical errors. The information is subject to change without notice. Changes are periodically added to the information herein; these changes will be incorporated in new additions of the publication. Alcor may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time. Reproduction of this publication without prior written permission is forbidden. The information in this publication is provided "as is". Alcor makes no representations or warranties of any kind, with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.