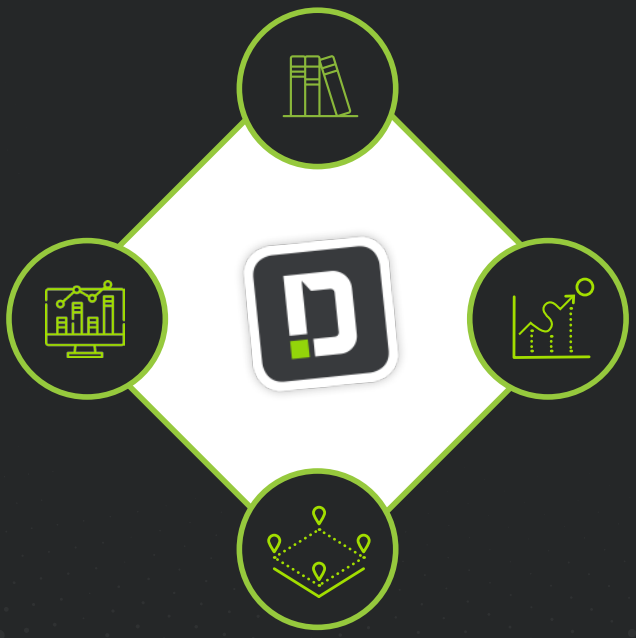
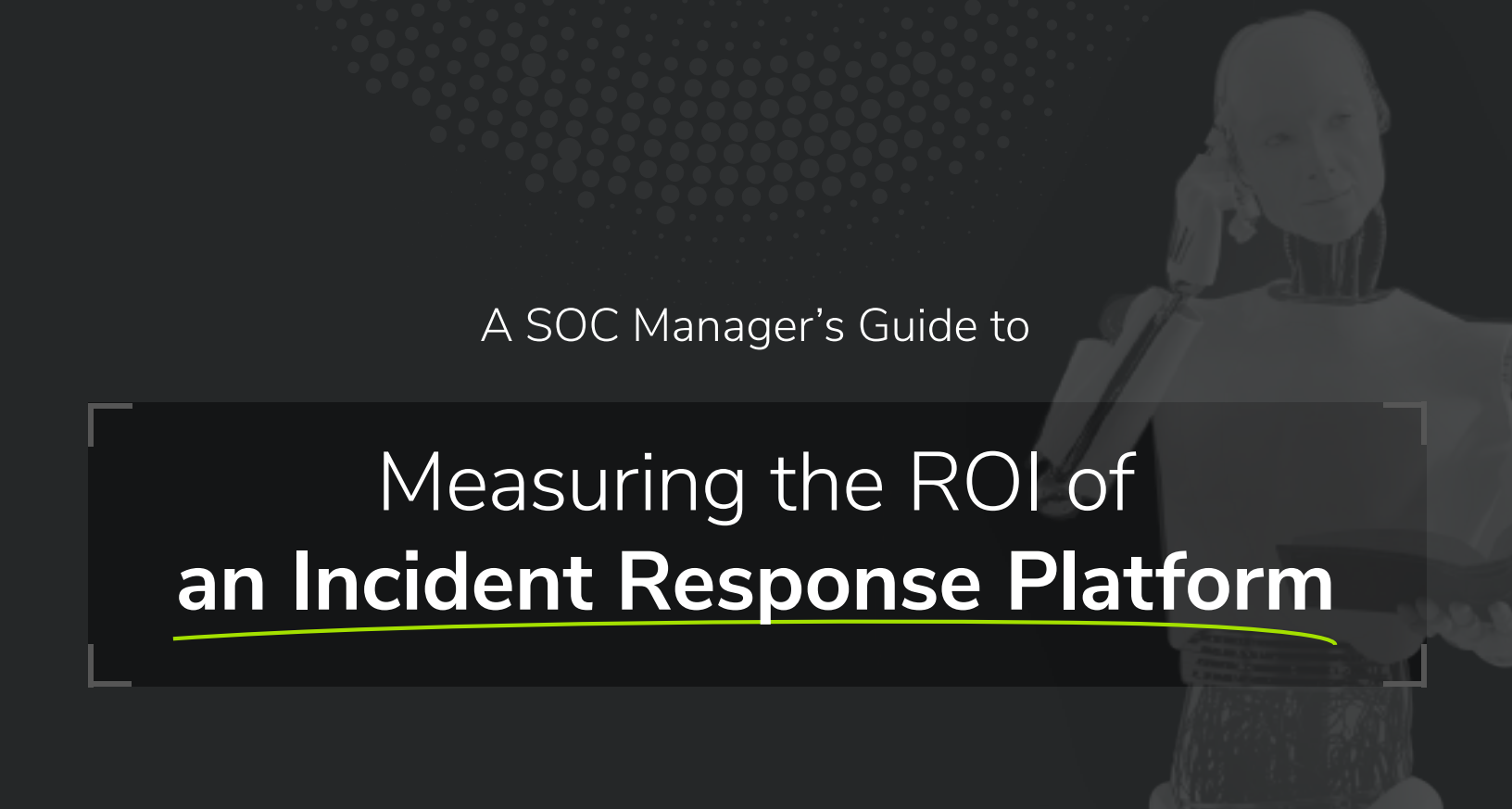
DEMISTO

A PALO ALTO NETWORKS® COMPANY





A SOC Manager's Guide to

Measuring the ROI of an Incident Response Platform

1. Overview

"You can't manage what you can't measure."

Despite the widespread media attention given to an ever-increasing number of breaches, many companies have no workable plan to respond to these incidents. In fact, according to a recent study conducted by the Ponemon Institute, **75 percent of all organizations in the United States are not prepared to respond to an attack.**[1]

Many organizations try to ride the "victory wagon" by placing incident response and security recovery on the back burner, considering them unnecessary expenses. Why spend money on "what if" scenarios when those funds can be better utilized on security products that deal with protection and detection?

And while detection and protection are vital to an organization's security posture, treating incident response as a second fiddle act while drawing up budgets may come back to haunt the organization and lead to greater monetary losses than initially anticipated. The Ponemon Institute study found that more than 25 percent of all businesses that close due to "what if" events never come to the floor again.

Even transitory downtime can be incredibly costly, with post breach loss of productivity, revenue, and reputation ranging from thousands to sometimes millions of dollars. In such a potentially pernicious scenario, **shifting focus from expense to measurement is key**. Identifying a positive return on investment can demonstrably improve how incident response and recovery are viewed, leading to increased adoption and more secure business operations.

Today's organizations spend a significant amount of time and money on ecosystem technologies to help reduce risk. However, these solutions often operate in silos and don't run as a harmonized unit. Despite organizational efforts, measuring the effectiveness of a security system is often tricky to implement from a business standpoint.

This paper will discuss the key challenges that stand in the way of the effective measurement of security posture, as well as solutions that aid in quantification of security improvement. We will also cover a clear way of measuring the effectiveness and ROI of an incident response platform.

1. Source: Ponemon Institute: http://www.ponemon.org/

2. Challenges of Implementing an Effective Incident Response Program

Today's criminals have an unfair advantage over the incident response teams who are endeavoring to keep the bad guys from running roughshod through organizational systems. Adversaries have more time, more resources, and a surfeit of targets and entry points. Response teams often have limited resources and tight schedules, forcing them to prioritize alerts, underuse certain technologies, and leave some alerts unhandled. These unhandled alerts and siloed technologies increase security risks and inevitably pave the way for major breaches.

CHALLENGE #1: STAFFING ISSUES

Research provided by EMA[2] found that 92 percent of companies receive at least 500 alerts per day, which equates to 15,000 alerts each month. Assuming it takes an analyst one full day to clear 30 alerts manually, one analyst would be able to handle a mere 900 alerts out of these 15,000 each month. Handling 15,000 alerts would require more than 15 analysts working without a day off! Most organizations cannot afford to invest in 15 employees solely dedicated to incident response.

Moreover, not only are qualified cybersecurity professionals hard to find, but they are also prone to burn-out due to overwork and the tedium of handling repetitive manual tasks. This phenomenon is called alert fatigue and is a pressing issue for analysts and SOCs worldwide. Considering the demand for employees with security skills and the turnover rate due to the high-pressure nature of the work, solving this challenge through hiring is impossible for most organizations.

2. Source: EMA Research: Achieving High-Fidelity Security: https://www.enterprisemanagement.com/research/asset.php/3187/Report-Summary---Achieving-High-Fidelity-Security

CHALLENGE #2: A SHORTAGE OF TIME

After an attack is detected, the speed of response and investigation is critical. Every minute the adversary spends in the network after the detection can cause severe damage in terms of stolen data, downtime and lateral movement. The consistency of response in times of crisis is another issue.

Time is also working against organizations in another way. SOCs cannot devote every minute of every day to handling threats. They must also invest time in building better cyber security strategies, training new employees, and day-to- day planning. Due to these responsibilities, SOCs wind up having to put out fires as they flare, leaving little time to proactively defend against threats.

CHALLENGE #3: LACK OF CONSISTENT INCIDENT RESPONSE PROCESSES

When designing security operations, organizations must make sure that there are clear guidelines and processes defined for incident response. If there are no consistent response practices, analysts can make mistakes and miss steps during an incident which can result in delays or further damage.

Additional challenges SOCs face here are ensuring that these standardized processes are enforced, shareable, and improve with time rather than remaining static.

3. The Solution: Automation and Collaboration with Prior Planning

For a robust security posture that effectively combats all the previously discussed challenges, cybersecurity should focus on three critical pillars: **people, processes, and technology**.

An effective security operation takes time, money, patience, and planning. In most organizations, time and money are two things that are in short supply for cybersecurity professionals. Automating simple, highly repetitive — but time-consuming— tasks can make SOCs more agile while providing a positive return on investment.

PEOPLE

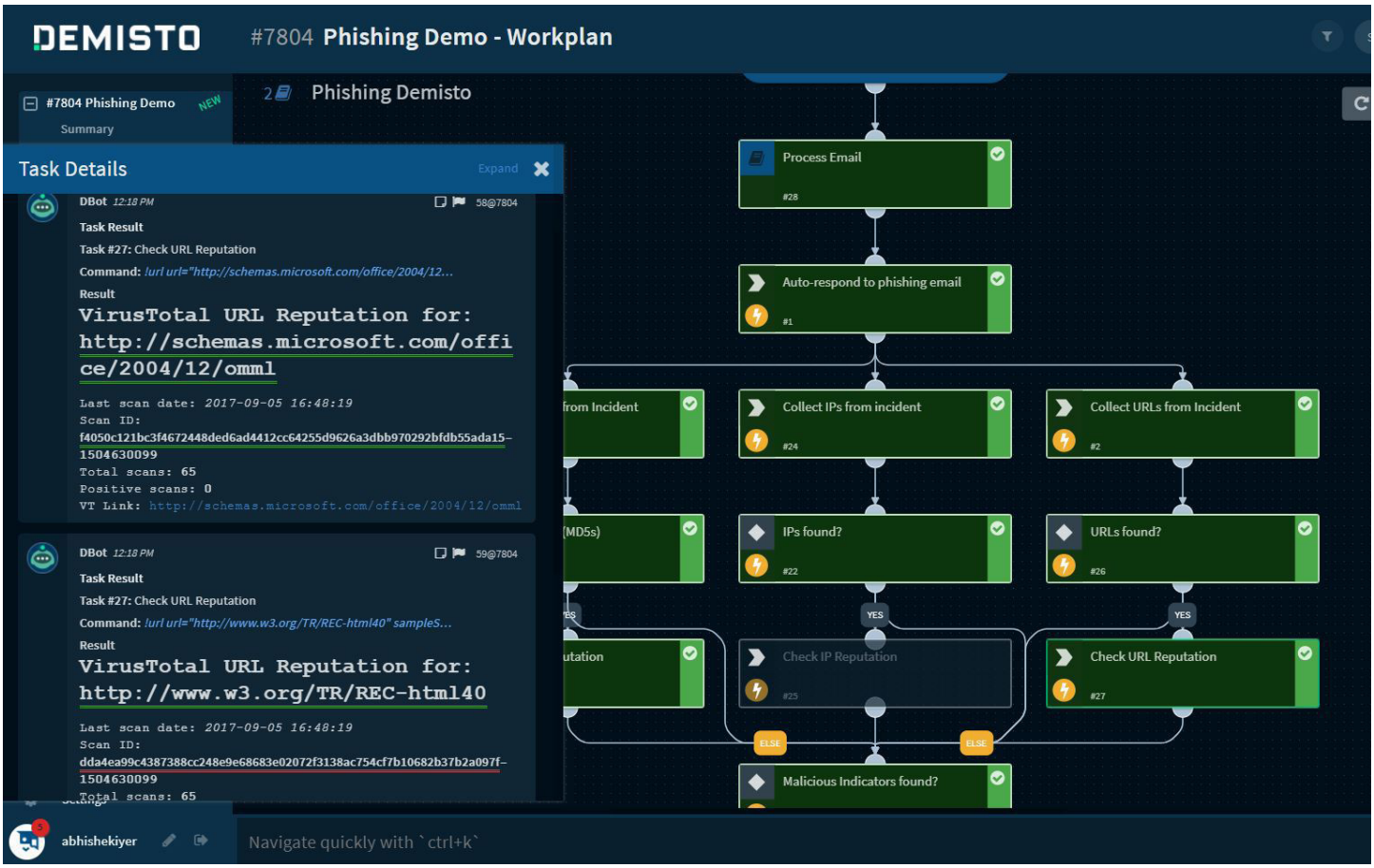
Technicians possessing expertise in incident response and cybersecurity and who have diverse skills represent a critical resource for success. They are also one of the most expensive assets available to a SOC and thus should not be spending most of their day performing boring repetitive tasks. Automating resource-intensive tasks will improve the efficiency of the SOC, boost morale, accelerate response times, and lower overall operating costs, thereby increasing ROI.

It's also common wisdom that incident response is often a team affair and should not be performed in silos. Having an effective collaboration platform allows analysts to share knowledge and learn from others, which can often be especially beneficial to newly hired employees.

PROCESSES

Processes are critical to the goals of the overall security program as well as to operations functions. In many cases, a single function may be associated with multiple processes. Automating tasks, tools and processes can eliminate many pitfalls that are common within the cybersecurity environment.

Consistent, documented processes help avoid inadvertently skipping a step or overlooking information during times of stress. Security orchestration helps capture procedures which are typically in big binders into a single step-by- step playbook which can be followed by an analyst.



TECHNOLOGY

Technology enhances and supports security operations through advanced detection, automated triage, transparency across systems, advanced analysis, and increased capabilities for investigation. Intelligent orchestration technologies for configuration tasks improve agility and flexibility as well as ROI.

4. Making a Case for Automation and Collaboration: Calculating ROI

It's essential to follow a process to ensure that organizations get the anticipated ROI on their cybersecurity spending. An ideal starting point is to list the most common incidents types and use cases that consume the majority of analyst time.

The most common incident types based on Demisto customer data includes phishing and malware. Determining the effectiveness and ROI on cybersecurity planning and technology requires an evaluation of five critical factors.

1. Volume:

Determine how many daily incidents are responded to and are in the queue respectively. Are all these incidents actually investigated? If not, the organization's risks and potential financial impact are dramatically increased.

2. People:

Skilled cybersecurity analysts are in extremely high demand. With a global shortage of analysts predicted over the coming years, Organizations should estimate labor costs and how much of those costs are going towards avoidable, repetitive work.

3. Staffing Costs:

Divide the incident volume by the number of analysts required to handle them in a timely manner. Multiply the number of analysts by the average salary, then add the costs of benefits and recruiting to determine the overall cost to manage internal teams without automation.

4. Duplicates:

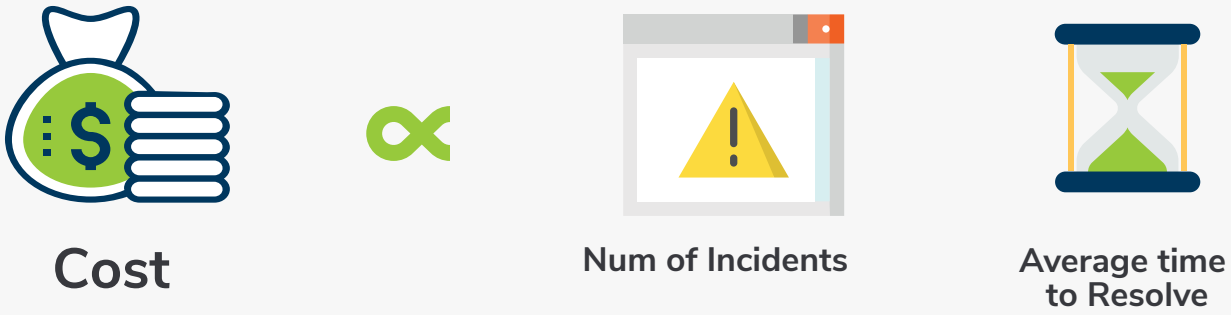
Attacks generate information, but it can be difficult to identify duplicates. If staff members are handling incidents through obsolete systems or manual processes, a great deal of time is being wasted (with little or no return) looking at artifacts from the same threat multiple times. Identifying the number of duplicates will give valuable insight into how much it is costing to deal with this avoidable aspect.

5. False Positives:

After an initial moment of panic, further investigation sometimes proves that the notification was nothing to worry about. If it happens only once, it's a minor inconvenience. When it happens multiple times every day — and there's no way to remove them from reports — staff members will end up spending their time (and the organization's money) to resolve false positives while the true incidents are delayed, or worse, neglected.

Once numbers for these five factors are calculated, the following formulae can be used to determine the exact amount that an organization has been spending without making significant progress.

COST METRICS



To reduce cost:

1. Reduce the number of incidents that need to be handled by IR team -> An IR platform can help do this.

2. Reduce the average time to resolve incidents -> An IR platform can help do this.

RISK METRICS

To reduce risk:

1. Increase the number of analysts -> Effective but costly, and even if budget allows, experience is in short supply.

2. Reduce the number of elements touched by analysts in incidents handled by IR team -> An IR platform can do this.

3. Reduce the MTTR -> An IR platform can help do this.

5. ROI of Incident Response Platform Using Demisto Enterprise: A Case-Study

THE CHALLENGE

Organizations rarely have sufficient people, processes, and technology to provide optimal security. Manual processes and countless repetitive tasks create burdens that can stress staff members and erode morale. Investigating incidents, dealing with false positives, and correlating data across systems and similar tasks can make it more difficult to recognize genuine threats when they occur. Furthermore, 75 percent of all alerts and/or events are ignored in the average large organization, according to Enterprise Strategy Group.[3]

For illustrative purposes, assume that the SOC has 10 analysts earning $80 per hour. They receive 300 alerts every day, and each analyst can handle 10 incidents per day. This means that approximately 66 percent of incidents each day are not being handled in a timely manner. Of the 100 total incidents that the entire team handles, there's a good chance that 90 of them are duplicates or false positives.

For a normal shift, the organization is spending $6,400 to handle 10 incidents that pose a potential threat, but while the analysts are dealing with those, genuine threats may be lurking in the incidents that the team was not able to handle. Most organizations cannot afford 20 more analysts or $12,800 per day required to cover the additional 200 alerts.

THE SOLUTION

Solving these SOC challenges revolves around reducing costs and reducing risks.

To reduce costs, organizations can reduce the number of incidents and amount of redundant time spent on incidents. An IR platform can help accomplish both these goals.

To reduce risks, organizations can increase the number of analysts, but this method is not very cost-effective. Alternatively, they can use an IR platform to reduce the number of incidents handled by the IR team and thus reduce the MTTR.

3. Source: Enterprise Strategy Group: http://www.esg-global.com/

With cybersecurity automation, organizations can expect measurable outcomes that solve many of the toughest challenges faced by a SOC.

Demisto Enterprise is the first security operations platform to combine intelligent automation, incident management, and collaboration. Provided by DBot, Demisto's automation interacts with SOC teams via ChatOps for cross-correlation, playbook-based workflows and information sharing, helping teams scale while working and learning in the way that humans are "programmed" to do — together.

A review of the following graphic shows you how much organizations could save by harnessing the power of Demisto to automate incident response.

COST METRICS

Before Automation | After Automation

Type of Incident	Attachment Defense Alert		Carbon Black (Advanced Threat)		Symantec (Trojan or Backdoor)		Attchment Defense Alert (Malware)		URL Defense Alert (Phishing)	
	Before	After	Before	After	Before	After	Before	After	Before	After
No of Incidents/month	380	380	265	265	86	86	165	165	165	165
Duplicates	304	304	189	189	10	10	89	89	89	89
Analyst Time to Analyze Duplicates(mins)	5	0	5	0	5	0	5	-	5	-
Escalated/FPs	22	22	76	76	108	108	26	26	26	26
Analyst Time to Analyze Escalated FPs (mins)	30	15	45	15	30	15	35	15	35	15
Total Analyst time taken manually (hours/month)	36.33	36.33	72.75	19	54.83	27	22.58	6.5	22.58	6.5
Hourly Cost of Analyst time	$60	$60	$60	$60	$60	$60	$60	$60	$60	$60
Total Cost	$26,160	$22,235	$52,380	$38,762	$39,480	$20,072	$16,260	$11,598	$16,260	$11,598

According to this graphic, 50-75% of analyst time is saved while the number of incidents and manpower remain the same. Correspondingly, the cost reduces by 50-75%.

RISK METRICS

The graphic also illustrates that thrice as many incidents can be handled with the same number of incidents and manpower, reducing the MTTR by 67%.

BENEFITS

Automation has the potential to improve an analyst's mean time to threat mitigation, reduce customer exposure to security threats, create less risk, increase focus on threats that matter, and even create lower employee turnover.

Security automation has many benefits that can save a lot of money in the long run.

Reduces MTTR:

With the same number of incidents and manpower, three times as many incidents can be handled, reducing MTTR by 67 percent.

Time saved means money earned:

Demisto's platform saves you both time and money.

Reduces number of out-and- out incidents:

Automation can reduce the number of actual incidents that will need to be escalated and investigated. The lower volume of unnecessary incidents allows the team to work smarter and helps maximize the company's ROI.

Streamlines the resolution process:

To get the most out of security incident response, integration with automation is essential. This will help manage incoming alerts more effectively and it will also streamline security incident response and investigation workflows during the incident lifecycle.

Better communication and collaboration between departments:

The four key steps to implement a successful cybersecurity program are detection, diagnosis, repair, and recovery. Automation helps streamline the process and its repeatable, enforceable nature results in seamless communication between everyone involved.

Given the ever-increasing number and sophistication of threats, it is virtually impossible to manage incidents manually without the organization eventually landing in a puddle of cyberattacks. Using the inputs mentioned in this whitepaper is a good starting point to study whether the ROI of automating incident response is worth the effort.

Performing these calculations makes it quickly apparent that the ROI of security planning and automation tools can be very significant while simultaneously increasing the organization's overall security posture and reducing vulnerability levels.

Want to see Demisto in action?

SCHEDULE A DEMO

DOWNLOAD FREE EDITION