



How to improve ROI and operational efficiency for cybersecurity

TABLE OF CONTENTS

Introduction	3
Areas of focus	3
A note on the scope of analysis.....	3
Vectra addresses the most critical skills shortages	3
The current skills gap.....	4
The Vectra value: Using automation to close the skills gap.....	4
Time: The most expensive metric in breach detection	4
The costs of security investigations and incident response	5
Calculating the cost of daily security analysis	5
The Vectra value	6
Calculating the costs of internal incident response.....	6
The Vectra value	6
Calculating the costs of external incident response	7
The Vectra value	7
Summing it up	7
Manual approach.....	7
Vectra approach	7
Conclusion	8

Introduction

IT security is an ongoing exercise in operational efficiency. Organizations have a limited set of resources to address an unlimited set of risks, threats and attackers. This asymmetry means that security products must always be evaluated in terms of security efficacy as well as their impact on the operational fitness of the organization. Is a solution a drain on manpower and resources or does it make staff more productive and nimble?

The need for efficiency is especially pronounced in the context of modern cyber attacks. Unlike commodity attacks, today's targeted threats are far more damaging and require more time and skill to detect.

In the past, security could rely on signatures to automatically deflect thousands of attacks without much thought. But more sophisticated attacks thrive on their ability to evade signatures and other preventive controls. This has created a need for new security approaches and put a premium on staff with strong cybersecurity skills.

To meet this challenge organizations must be able to automate the detection of sophisticated attacks, while making security staff as efficient and productive as possible. Vectra® Networks meets both these demands, and this document focuses on the many ways Vectra helps security teams get the most out of limited staff, time and resources.

Automated analysis lowers costs while analyzing all traffic

Manual analysis is expensive and can only analyze by exception



Vectra deployment

Manual investigation

Areas of focus

Today, the process of detecting targeted threats is manual and expensive. Vectra software is designed to automate the process and lower costs. The value of Vectra software can be illustrated in three ways:

Skill One of the biggest challenges of modern security teams involves recruiting and retaining exceptional security and data science staff. Talent and experience in these fields are rare, yet are required in order to recognize the subtle indicators of attackers that successfully infiltrate networks.

Time The most important factor in detecting network breaches is time. Attacks must be detected in near real time before key assets are stolen or damaged. Unfortunately, these attacks are also the most time consuming to detect. They require a variety of skills and in-depth investigative know-how to determine the reach of an attack.

Costs Cyber attacks have direct costs that extend beyond time and staffing. Expensive incident response and forensic analysis services are often required after an attack. Vectra helps avoid the cost of third-party investigations entirely, while lowering dependence on manual log analysis.

A note on the scope of analysis

The scope of this document is limited to savings that Vectra delivers to security teams within an organization. It **does not** estimate the total financial impact of a network breach. Consequently, potential fines, credit monitoring for affected customers, legal fees, brand damage and other costs associated with loss are not factored in.

While these costs are very real, the differences in organizations, the types of data they hold, and the wide range of hard and soft costs of a data breach make estimating the true cost of a breach notoriously difficult.

To meet this challenge organizations must be able to automate the detection of sophisticated attacks, while making security staff as efficient and productive as possible.

For example, leading industry research puts the cost of a breached data record anywhere from 58 cents over \$201 per record depending on the unique factors of the organization and whose estimates you use. As such, this document does not attempt to identify the full financial benefit of the Vectra software solution, but instead focuses on savings for security and IT teams.

Vectra addresses the most critical skills shortages

As security evolves, organizations increasingly find themselves searching for highly specialized and rare sets of skills. Security and data science skills are at the top of the most-wanted lists, making the best in these areas limited and costly. Vectra automates these key skills at scale, which reduces the overall need for dedicated specialists and makes all members of the existing security staff more efficient and productive.

The current skills gap

Based on surveys of CISOs, [IT analyst firm ESG](#) found that information security has been the most commonly reported skills shortage for four years. And [the SANS Institute states in a recent report](#) that it found that incident response skills would be in high demand in the next two years as organizations try to mitigate and prevent increasing cyber attacks. In addition to traditional security roles, data scientists are highly sought-after as security team members. This is due in part to increased reliance on data science for everything from getting more value out of SIEMs to building custom behavioral models to detect insider threats.

In fact, CIO.com recently [surveyed more than 500 CIOs](#) and found that data scientists and security staff topped the list of their skills shortage.

Unsurprisingly, the high demand for these rare skills has made cybersecurity analysts and data scientists some of the most highly paid positions in IT. [A recent report from Glassdoor](#) found that the average salary for a data scientist was \$118,709 compared to \$64,537 for a trained programmer.

The most qualified data scientists demand even higher salaries. [An analysis by recruiting firm Burtch Works](#) found that the median salary was \$175,000 for top individual-contributor data scientists.

Of course, salary is just a portion of the fully loaded cost of an employee, which will be much higher. However, this comparison of salaries gives a view into the premium associated with security and data science talent.

» The Vectra value: Using automation to close the skills gap

By automating the process of threat detection and data science, Vectra identifies threats that would be impossible to find through manual investigation, while simultaneously lifting the time and resource burden from security teams.

The intelligence in Vectra software is driven by a dedicated team of security researchers and data scientists who focus exclusively on the most advanced cybersecurity techniques and detection strategies.

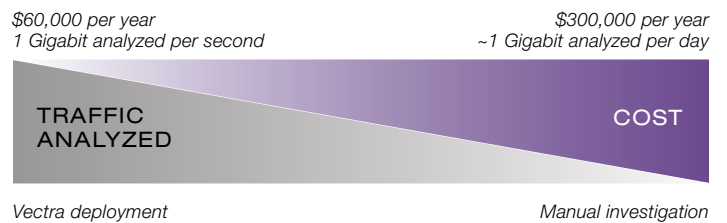
These researchers analyze millions of malware samples, attack tools and evasion techniques, as well as monitor metadata from Vectra customers worldwide to identify the latest trends and attack techniques. The sweeping, global scope of this data reveals trends that would not be obvious by simply analyzing data.

This global data set continually drives the Vectra automated analysis. Vectra software uniquely automates security investigations that would normally require hours of manual effort from highly trained security analysts and data scientists.

As a result, Vectra enables organizations to directly address the most pressing skills shortages in IT security – cybersecurity analysis, incident response and data science. And unlike manual approaches that focus on small amounts of suspicious traffic, Vectra analyzes **all** traffic.

A simple analysis shows just how valuable this level of automation can be. The annual license for Vectra software to monitor a 500-host network is \$60,000 per year. While the actual throughput could vary, we will estimate this 500-host network to generate around 1 gigabit per second of traffic.

Based on the previous example, a high-end security analyst and data scientist would cost about \$300,000 a year and would only analyze a fraction of the total traffic. The image below is an update of the previous one with more precise metrics about the cost per analyzed gigabit.



Based on this ability to automate analysis, customers can manage security incidents faster and without the need to hire additional expert staff. Deferring hiring can have significant financial value.

Yearly savings in staffing costs

New headcount deferred	1
Fully loaded cost for expert talent per hour (NSS Explanation)	\$75
Yearly cost	\$156,000

Get the Vectra Value Calculator – It's free!

The *Vectra Value Calculator* lets you customize this and other calculation tables in this paper to estimate the cost savings with Vectra in your own network. [Click here](#) to request your calculator.

Time: The most expensive metric in breach detection

Time is the most important factor in the detection of network breaches. To mitigate damage, attacks must be detected in near real time before key assets are stolen or damaged. The problem for security teams is that these attacks are the most time-consuming to detect.

Once an attacker bypasses prevention controls at the perimeter, the job of threat detection becomes a very manual and time-consuming process. Investigations require a variety of forensic analysis skills – malware analysis, forensic packet and log analysis – and the correlation of massive amounts of data from a wide range of sources. This set of tasks requires a broad and specialized set of skills and a significant amount of time.

Advanced threats have become quite adept at bypassing signatures, sandboxes and other security techniques deployed at the perimeter. Simple investigations into these events can last hours, and a full analysis of an Advanced Persistent Threat (APT) can take days or weeks.

Vectra automates the analysis phase and detects threats immediately. The analysis process integrates many disciplines, including an understanding of malware behavior, evasion techniques, user behavior analysis, and the ability to correlate threats to identify the presence and location of a targeted network attack.

This approach finds threats that would otherwise be impossible to find and does so without human involvement. Vectra automatically prioritizes events, explains each phase of an attack, and provides quick access to the source packets to verify the detected threat.

Each detection includes prescriptive advice for next steps, enabling staff to take immediate corrective action. This allows security teams to condense hours and days of manual effort into minutes and seconds, and take action before damage is done.

The costs of security investigations and incident response

This section offers a basic framework for estimating the cost of investigating security events and incident response. Because no two cases are exactly alike, a variety of industry standards and benchmarks were used to estimate costs. It is possible to edit certain metrics so that they more closely reflect the realities of your organization.

The effort and expense of security investigations can be divided into three phases:

Daily security analysis and investigation This may include inspection of events and alerts from security solutions, analysis of logs, host-based alerts, and analysis of newly identified or common threats. The end goal is to determine if there is a significant security event. This phase can be particularly time-consuming if the goal is to detect the presence of an APT.

Internal incident response This phase picks up when a serious security event is identified in the previous phase. It is often dependent on a Security Incident Response Team (SIRT). The SIRT can consist of dedicated personnel or be formed ad hoc from existing staff. This phase continues until the event is contained and remediated, which can last from minutes to months.

External incident response External incident response services are often contracted in the event of a successful breach. It typically occurs if an attack goes undetected by internal staff or was discovered late in the attack lifecycle.

Each of these areas entails examining similar metrics – namely the frequency of an event, the amount of time it takes for staff to work the event, and the cost of staff time.

$$\text{ESTIMATED COST} = \text{Number of events} \times \text{Time-to-resolution} \times \text{Staff value}$$

While these factors are common to each phase, actual values will vary based on the phase of analysis. For instance, daily analyses may include a large number of brief investigations, while incident response may include an ongoing investigation over days, weeks or months. Calculations are shown separately for each phase to better account for these differences.

Calculating the cost of daily security analysis

The daily tasks of security investigation and analysis are handled differently by every organizations. Whether done by a dedicated team of experts or ad hoc by security generalists, virtually all security products require an investment of time to extract actionable cybersecurity intelligence. The analysis should identify if there are security events that require further inspection and response.

Analyzing the time spent on daily security activities requires an estimate in the amount of time per day spent investigating and analyzing events. This can be performed by a variety of staff with different levels of experience and expertise.

Hourly staff rate These calculations use the default rate of \$75 per hour to estimate the cost of a team member. This rate is used by NSS Labs when estimating the fully loaded cost of an experienced security engineer to determine the total cost of ownership (TCO) of a security solution.

The table below provides a very simple estimate of investigation costs for a small enterprise, using modest assumptions.

Staff costs of daily analysis

Percentage of day spent on investigations	20%
Number of staff involved in investigations	2
Average hours per year spent on investigation	832
Average hourly wage for staff	\$75
Yearly cost	\$62,400

» The Vectra value

Vectra consolidates and automates the identification of active threats inside a network. Detections can consolidate dozens to hundreds of underlying events and metadata samples to provide a final diagnosis.

Furthermore, each event is scored and prioritized based on its threat, certainty and phase of the attack lifecycle. This makes it easy for staff to distinguish adware botnets and other lower-priority threats from active targeted attacks that aim to steal corporate assets.

This automation offers two benefits – staff can perform investigations in less time and non-expert staff can handle more investigations.

Vectra customers have reported reductions in time spent on investigations by 75% to 90%, and have successfully deferred analysis to IT generalists instead of escalating incidents to higher-paid experts. The analysis below takes a conservative 50% reduction to the time of analysis and reduces the average hourly wage from \$75 to \$55. **Compared to the previous baseline, this leads to a savings of \$39,520 and a 63.3% reduction in costs.**

Staff costs of daily analysis with Vectra

Percentage of day spent on investigations	10%
Number of staff involved in investigations	2
Average hours per year spent on investigation	416
Average hourly wage for staff	\$55
Yearly cost	\$22,880
Yearly savings	\$39,520

Calculating the costs of internal incident response

The incident response volume and process varies greatly, depending on the organization. [The SANS Institute study of enterprise incident response](#) was used to set reasonable baselines.

The study collected incident response data from over 250 companies and includes the frequency of events and overall time to containment. It also found that most organizations experienced security incidents, including some smaller companies with under 100 employees.

Number of incidents Most organizations reported between one and 25 incidents, with the most active environments reporting over 500. A conservative estimate with an average of 17 incidents per year, per organization was used, based on the SANS data.

Time to containment There was a wide variance in the time to containment. The most common response time was between six and eight hours, while the longest took more than six months. Only the most commonly reported categories were used to prevent the skewing of data, producing an average time to containment of 29 hours.

Staff costs of internal incident response

Number of events per year	17
Average time to containment in hours	29
Number of staff on SIRT team	3
Average hourly wage	\$75
Yearly staff costs of SIRT	\$110,925

» The Vectra value

In addition to detecting hidden signs of a threat, Vectra correlates the multiple phases of an attack to specific hosts that are under attack. The ability to condense massive amounts of data down to a few specific hosts is most critical to the rapid containment of a threat.

It is important to remember that most network intrusions remain undetected for an average of 205 days, according to the [2015 Mandiant M-Trends report](#). And according to the SANS Institute study, once a threat is detected, the time to containment can take days to months.

Vectra dramatically reduces both of these figures. The analysis by Vectra is limited to the direct comparison of incident response efforts to ensure a proper apples-to-apples comparison.

With the highest degree of certainty, Vectra discovers security events that would otherwise have gone unnoticed. This leads to a net increase in the number of events and precise and timely incident response. While many of these events are managed automatically, Vectra accounts for a doubling in the number of events detected.

Vectra also vastly reduces the amount of investigation needed to diagnose hosts that require remediation. By correlating and scoring specific hosts under attack, security teams using Vectra can perform analysis in minutes and eliminate days and weeks of investigation, log reviews, and SIEM-based analysis.

Once again this data is based on real-world examples from Vectra customers who reduced their average time to containment to 30 minutes or less. The calculations below are conservative estimates to reduce the overall time to containment to three hours. **These assumptions reduce the cost of incident response by \$87,975, which maps to a savings of 79.3%.**

Staff costs of daily analysis with Vectra

Number of events per year	34
Average time to containment in hours	3
Number of staff on SIRT team	3
Average hourly wage	\$75
Yearly staff costs of SIRT	\$22,950
Yearly savings	\$87,975

Vectra provides substantial yearly savings in the following key areas:

Category savings

Security and data science headcount	\$156,000
Time savings of daily security operations	\$39,500
Time savings of incident response	\$88,000
Avoidance of third-party incident response	\$50,000
Total	\$333,500

These savings naturally scale in larger organizations with larger security teams. The Vectra focus on automation ensures that all traffic is inspected, less time is spent on manual investigation and correlation, and all staff members are empowered to rapidly mitigate active threats. The following tables summarize the Vectra operational values compared to the manual approaches used today.

Conclusion

New types of threats naturally require new types of security. But most security products require a significant investment in human time and talent in order to deliver value. Organizations are often full of security products that were either never fully deployed or simply aren't used because the staff can't support them.

Vectra is one of the few cost-effective solutions that finds threats that others can't while saving time, headcount, and money for security organizations.

By automating the time-consuming tasks required to investigate cyber threats, Vectra software is expressly designed to serve the needs of security teams and not the other way around. This lets organizations build an efficient security architecture that removes bottlenecks and empowers all members of the IT and security staff to do more.

Get the Vectra Value Calculator – It's free!

The *Vectra Value Calculator* lets you customize this and other calculation tables in this paper to estimate the cost savings with Vectra in your own network. [Click here](#) to request your calculator.



Email info@vectranetworks.com Phone +1 408-326-2020
www.vectranetworks.com