CYBRAICS

A CISO'S GUIDE:

5 Ways to Reduce SG&A and Improve Security Through Automation

How confident are you in your cybersecurity posture? Do you have the right tools in place to be successful? When organizations have dozens of different security tools and still experience breaches and other threats, it's clear that throwing more products at the problem isn't the solution.[1]

When most of these security tools require human expertise and analysis, these "solutions" historically add complexity and cost to your security program. In a recent Ponemon Institute research study of IT leaders, almost half said they rely solely on manual products, and only 24% reported that they have an automated security solution.[2] Manual effort and siloed products lead to gaps in the security posture, which more manual effort simply cannot fix.

A monstrous IT tool stack taxes your Selling, General & Administrative Expense (SG&A) overhead and comes with a mixed bag of challenges.

Adding more security products to shore up security gaps means you get more alerts; it also means you need more skilled employees to decipher, organize, and correlate the data. The sheer quantity of these security alerts makes scalability difficult— and becomes truly impossible when your team has to manage millions of alerts. And let's not forget human error, which is one of the fastest-growing causes of breaches.[3] Ultimately, cybersecurity for most medium to large-sized organizations is too time-consuming and expensive to manage manually.

Automation is necessary and solves five core challenges that CISOs face:

- **Headcount:** automation dramatically reduces the need for multiple employees to spend hundreds of hours doing manual analysis.
- **Qualified Skills:** automation via a highly tuned security solution like Cybraics means the available talent pool can be assigned to higher value activities.
- **Scale:** automation simplifies the organization and prioritization of threats, empowering your IT team to investigate and mitigate cyber threats at scale.
- **Accuracy:** automation unites data from disparate security tools, reduces human error, and provides superior visibility for threat response.
- **ROI:** automation improves your SG&A expense, eliminates redundant security technologies, and replaces manual costs by automating your security stack.

CHALLENGE 1:

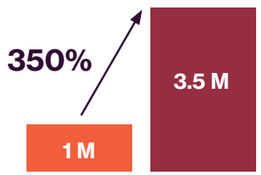
Headcount

While the demand for cybersecurity professionals is rapidly increasing, the available talent pool simply isn't big enough. In the 2021 ISACA State of Cybersecurity Report, 55% of hiring managers reported unfilled cybersecurity positions.[4] According to Cybersecurity Ventures, 3.5 million unfilled cybersecurity jobs are projected to be open worldwide by the end of the year, up from one million unfilled positions in 2014.[5] That gap means finding and hiring talented people can be very costly, difficult, and retaining them is critical.

Solving for Mundane Data Crunching

One of the primary reasons for the high demand for cybersecurity experts is the massive volume of security-related data most IT teams manage. Not only do you have information and alerts produced by dozens of security tools, but the network, device, and cloud logs also present a deluge of data to navigate. But what if you could take an ocean's worth of data and distill it down to a glass of water?

No matter how many human resources you have, there is no way for manual efforts to corrolate, process and prioritize all the security data from multiple tools. Fundamentally the only way to process all of this data is via automation that utilizes artificial intelligence (AI) and machine learning (ML) to categorize, correlate, and prioritize the data. Cybraics utilizes ML and AI-based behavioral analytics to identify threats and then presents your team with a handful of neatly bundled high-priority cases to remediate. It empowers your expert staff to quickly and easily resolve security threats instead of scrolling through alert logs, trying to sort, find and handle potential issues.



Unfilled cybersecurity jobs are expected to grow by **350%**, from one million positions in 2013 to 3.5 million in 2021.[5]

58% of CISOs believe that their problem of not having an expert cyber staff will only worsen.[6]

The Takeaway:
There's a greater demand for cybersecurity jobs than there are professionals to fill the positions. As a result, organizations are **persistently** concerned about their security effectiveness.

Automation is the solution, combined with AI and ML; it eliminates the need for multiple employees to spend hundreds of hours doing manual analysis.

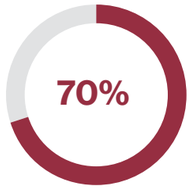
CHALLENGE 2:

Qualified Skills

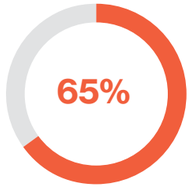
Finding the right employees to bring on board is even more difficult when many in the already slim candidate pool of cybersecurity professionals are under-qualified. According to the MIT Technology Review, fewer than one in four candidates are even qualified for the role they are applying for.[7] So, it is no surprise that 44% of organizations reported in the 2021 ISACA State of Cybersecurity Report that it takes them 3-6 months to fill a cybersecurity position with a qualified candidate. Think that sounds bad? Sixteen percent reported it takes even longer.[4]

Removing the Complexity in Hiring

The complexity of security information and event management (SIEM) and other security management tools is a driving factor in why it takes organizations so long to find the right hire. Too many security products in the market are difficult to operate and, as a result, require employees with high levels of expertise and certifications. Frequently, only a small subset of applicants even have these skill sets, and possible candidates are instantly whittled down when their resumes exclude them. Candidates who possess the requisite expertise also command higher salaries[8]— and often present higher demands— since they know they're desirable within the industry.



70% say that **fewer than half** of their cybersecurity applicants are well qualified.[9]



65% of those in one survey cited "**shortage of skilled incident response personne**l" as an obstacle in their ability to effectively respond to cyberattacks.[2]

Automation, powered by AI and ML, helps reduce and even eliminate the requirement for specific human resource skills and certifications. At Cybraics, we recognize the challenges that CISOs face with the limited availability of qualified candidates, so we built our solution to automate and simplify security operations. We believe an intuitive solution with simple dashboards, guided remediation, and managed detection and response (MDR) as a service empowers all cybersecurity professionals to be successful.

The Takeaway:

As Cybersecurity Ventures so aptly quoted, "nowhere is the workforce-skills gap more pronounced than in cybersecurity."[5] Highly qualified security professionals are difficult to find and expensive to onboard and retain. While senior-level IT talent will always be an integral part of any organization's security posture, automation via a highly tuned security tool, such as that offered by Cybraics, means the available talent pool can more easily handle the responsibilities.

CHALLENGE 3:

Scale

Typical log management tools produce hundreds of millions of alerts each month. SIEM tools help reduce this down to hundreds of thousands, but that still leaves *hundreds of thousands* of potential threats to review. According to a Ponemon Institute study, the top two reasons potential threats don't receive the remediation attention they deserve boils down to "lack of visibility of threat activity across the enterprise" and the "inability to prioritize threats."[10] With such a flood of data, it's no wonder cybersecurity professionals struggle to get a handle on their actual threat landscape; it's simply unrealistic to monitor and address hundreds of thousands of alerts manually.

Making the Data Dump Manageable

To sort through and prioritize the millions or even just thousands of possible threats, medium to large-scale organizations need the help of automation. Beyond simple automation, Cybraics' proprietary behavior tracing reduces alerts into actionable cases by an astounding 97% compared to even the best SIEM and other automation tools combined.[11] When your security team is 26x more efficient, think about the true value they could deliver because they are no longer just responding to and triaging threats. Unlike typical claims of AI-powered technology, our analytics can detect 250+ behaviors, are more effective on day one, are constantly improving, and are proven to outperform leading SIEM tools in head-to-head customer bakeoffs.

31%
of security alerts go uninvestigated **due to volume.**[10]

Only 39%
of organizations consider themselves effective at detecting cyberattacks, while **only 17% feel they're effective at prioritizing alerts.**[10]

The Takeaway:
Most organizations simply have too much data across their threat detection toolset to assess it all manually. Automation simplifies organization and prioritization, empowering your IT team with the transparency needed to investigate and mitigate cyber threats at scale.

CHALLENGE 4:

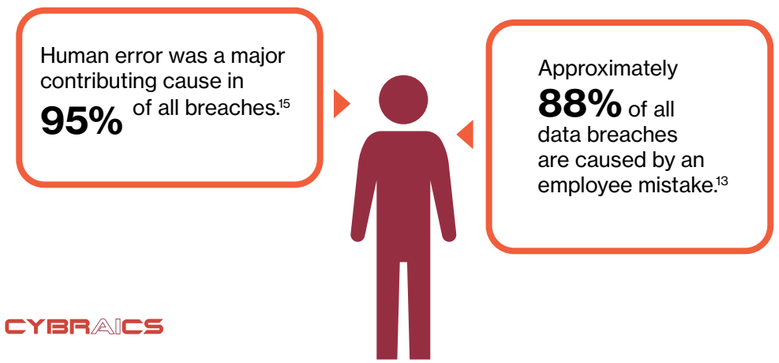
Accuracy

Despite most organizations' heavy tool stack, 53% of IT security leaders aren't sure their cybersecurity tools are working as promised and protecting their network, according to the Ponemon Institute Report.[2] This begs the question, why keep throwing software at the problem when adding more technology is part of what's making it worse? Alert fatigue plagues almost every cybersecurity team with millions of threats numbing analysts to the point of ignoring nearly a third of all alerts. Ironically, enterprises that deploy over 50 tools ranked themselves 8% lower in their ability to detect threats and 7% lower in their defensive capabilities than companies deploying fewer products.[12]

With a complicated mix of tools, not only is the accuracy of your actual security posture in question, but there's also concern with the accuracy of manual assessment to validate and address the alerts. After all, to err is human— and the majority of employees blame "stress" at work for their mistakes.[13] With all this data to organize while being grossly understaffed, it's no wonder they're feeling overextended.

Interoperability & Visibility at its Finest

Automation solves for both data volume inundation and the human error that comes with it. AI and ML prioritize millions of alerts by severity, and when tools are consolidated and interconnected simultaneously, AI and ML also increase visibility. This interoperability streamlines IT workflows— saving time and resources, improving accuracy, increasing actionability, and helping organizations scale.[14] Cybraics enhances over 80 leading security products like Palo Alto, CrowdStrike, Carbon Black, and more. At the same time, our ML and AI-based analytics adapt to automatically detect threats otherwise missed by popular security software.



CYBRAICS

The Takeaway:
Improving accuracy to understand the actual threat landscape and reduce manual error is key to saving time and money and improving your security posture. Automation unites data from disparate security tools and provides better visibility than manual effort ever could.

CHALLENGE 5:
ROI

Hidden behind each monthly subscription are associated headcount, management, and storage costs, not to mention the cost of running your own security operations center (SOC). On average, organizations spend $2.86 million annually on their in-house SOC.[8] As of January 2020, the average salary of an analyst is over $102K— and with the demand for qualified talent only increasing, the fully-loaded employee-related costs are likely to grow. [8]

Consolidating Tools & Headcount with Automated Threat Intelligence

Automation powered by AI and ML helps you slash software expenses and overhead, often eliminating the need for dozens of niche, siloed cybersecurity tools. In a recent IBM Cyber Resiliency Report, 55% of high-performing organizations reported improved cyber resilience through automation tools in addition to the instant ROI of removing extraneous siloed cyber tools.[14]

Although companies in one survey are spending an average of **$18.4M annually** on cybersecurity, data breaches still happen.[2]

45:
the average number of security solutions and technologies in use at organizations.[14]

The Takeaway:
Many organizations want to improve their SG&A expense but struggle to do so without consolidation, interconnectivity, and prioritization of their cybersecurity stack. Increase your ROI, eliminate redundant security technologies and choose trusted solutions that leverage true AI and ML to replace manual costs with automation.

THE *GROUNDBREAKING* SOLUTION YOU NEVER KNEW EXISTED

Reducing SG&A and improving cybersecurity are not mutually exclusive. Better security isn't about throwing more tools at the problem. It's about having the best coverage to identify and prioritize high-risk threats accurately, so your team can easily resolve them in real-time.

Improve your SG&A while transforming your security posture by adopting the most advanced ML and AI-based security analytics solution available, Cybraics.

See it in action by scheduling your complimentary demo today.

Sources

1 Sowell, Brad. "RSA 2019: Most Organizations Use Too Many Cybersecurity Tools." BizTech Magazine, 06 May 2019.
2 Ponemon Institute, LLC. "The Cybersecurity Illusion: The Emperor Has No Clothes." AttackIQ, July 2019.
3 Verizon. "2021 Data Breach Investigations Report." 2021.
4 ISACA. "State of Cybersecurity 2021, Part 1: Global Update on Workforce Efforts, Resources and Budgets." 2021.
5 Morgan, Steve. "Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021." Cybersecurity Ventures, 24 October 2019.
6 Harvard Business Review. "The Public-Private Partnership That's Working to Make New York City a Global Hub of Cybersecurity Talent." 18 June 2019.
7 Winick, Erin. "A cyber-skills shortage means students are being recruited to fight off hackers." MIT Technology Review, 18 October 2018.
8 Ponemon Institute, LLC. "The Economics of Security Operations Centers: What is the True Cost for Effective Results?" Respond Software, January 2020.
9 ISACA. "ISACA's Cybersecurity Study Reveals Struggles with Hiring and Retention Persist, More Diversity Progress Needed." 24 February 2020.
10 Ponemon Institute, LLC. "The State of Malware Detection & Prevention." Cyphort, March 2016.
11 Cybraics "Behavior Tracing: The Secret To Streamlining Your Cybersecurity Process" May 2021.
12 IBM. "IBM Study: Security Response Planning on the Rise, But Containing Attacks Remains an Issue." IBM News Room, 30 June 2020.
13 Tessian. "The Psychology of Human Error." 2020.
14 IBM Security. "Cyber Resilient Organization Report 2020." July 2020.
15 IBM. "IBM Security Services 2014 Cyber Security Intelligence Index." CRN, May 2014.

cybraics.com

2400 East Commercial Blvd.
Suite 215, Ft Lauderdale, FL
33308

CYBRAICS

Cybraics was developed out of a long-term, award-winning machine learning and AI research program designed to support the U.S. Department of Defense. With the rigorous demands of national defense as our foundation, we've continued to improve and evolve our nLighten™ platform to be the world's only fully autonomous SIEM and MDR solution, with proven success across industries like energy and entertainment, finance to healthcare, government to education and more.

See Cybraics nLighten in action with a personalized demo or give us a call at (844) 283-0458.