Top 4 Roadblocks to SOC Productivity

Introduction

In an environment where threats change daily, and sometimes hourly, the security operations center protecting an organization's most valuable digital assets has to constantly adapt. Its success depends upon analysts' ability to perpetually learn about new threats and devise the best approaches to address them. In addition, staying informed about new defensive tools in this changing landscape is a key component to fighting the evolving tactics, techniques and procedures (TTPs) of attackers.

Organizations across the globe dedicate copious resources to cybersecurity, spending more than $150 billion[1] annually. This raises valid questions about whether or not security pros are satisfied with the tools at their disposal and confident in their security posture. To answer these questions, Awake Security (now Arista NDR) commissioned a survey of 300 cybersecurity professionals. The goal was to assess how effective existing tools are at helping them detect and investigate modern threats. Among the most surprising results were conflicting responses that seem to suggest the cybersecurity industry might have, or at least project, a false sense of confidence.

Arista also collaborated on a research project with the SANS Institute. The report[2] provides deeper context by illuminating specific challenges security professionals face with current tools. Together, this data helps indicate where the industry needs to focus most in order to provide security teams with the tools they need to improve security.

[1] https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

[2] https://awakesecurity.com/sans-soc-survey-key-findings/

The Emotional Roller Coaster

Gaining a better understanding of the challenges facing security operations centers is the ultimate goal of this research. And at a foundational level, learning about the emotional state of the people fighting cyber threats every day can provide telling evidence about the areas that need "fixing."

The survey asked security professionals to associate various words with their daily workloads. "Stressful" and "Worrisome" were the top two words selected when respondents were asked to describe their emotions. They outranked words including "Manageable," "Confident" and "Relaxed."

What's even more telling is that people who did not have security investigation tools in place at their organization were twice as likely to feel worried compared to those who did have the appropriate tools. In fact, those without these tools in place were more likely to feel worried, stressed and overwhelmed. On the other hand, "manageable" was the top emotion for those that had the right tools in place.

Industry professionals are clearly worried and stressed by daily security tasks like responding to alerts, and the right tools and technologies to make their day-to-day more manageable are critical.

In addition, it's interesting to note similarities or discrepancies in how the volume of alerts is perceived by people at different levels of a security team. For example, analysts, managers, directors and CISOs all generally agree that "Insignificant" and "Boring" are not words they'd use to describe their workload. However, analysts who are usually the first line of defense and are tasked with triaging alerts, have much different views than their superiors in some areas. Analysts see alert volume as "Extensive" and "Exciting" at a much higher rate than their colleagues do, but they're less likely to be stressed or worried by them.

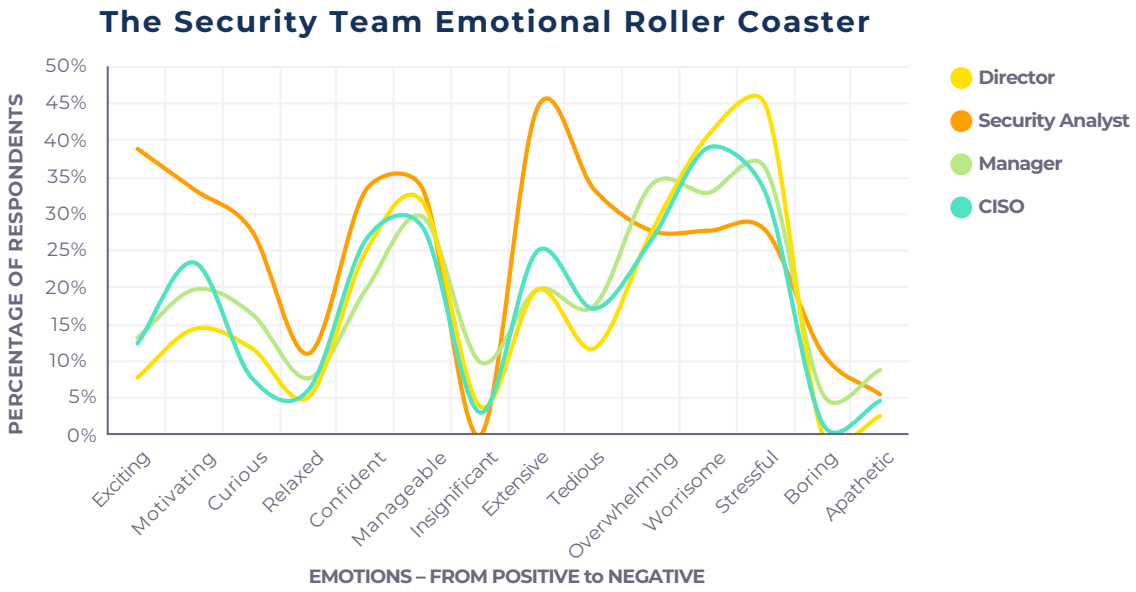
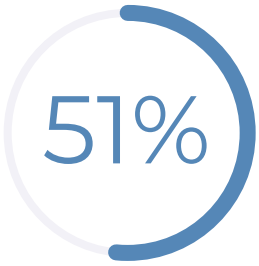


Figure 1: Respondents to Arista NDR's survey were asked to describe their feelings related to the number of security alerts their organization receives.

The Right Tools… Right?

But what tools? Nearly two thirds (61%) of respondents to the Arista NDR survey said they have the technology and processes in place to effectively investigate threats, showing that a solid margin of security pros are confident in their security posture. However, taking a deeper look at the responses related to specific concerns or challenges shows that confidence is fleeting. For example:



When asked about the most urgent issues, more than half (51%) said they can't stay ahead of "new & emerging threats," which was the number one answer.

Perhaps most telling, 56% are seeking new tools to address the fact that they can't stay ahead of threats with their current tools.

If nearly two-thirds of respondents say they're confident in their current technology, the fact that more than half of them are seeking new tools because they can't stay ahead of threats reveals a striking contrast. This suggests something that has perhaps been an age-old problem in security: that new technology is viewed as an insurance policy against "new threats." But simultaneously, a significant number of security professionals – perhaps unconsciously – project a false sense of confidence based on their current technology stack.

To help right this perplexity, it's important to understand security professionals' biggest challenges and how to address them. The data above offers hints, such as the fact that security pros said their inability to stay ahead of "new & emerging threats" was their most urgent issue. This would include evolving tactics that attackers are using to circumvent traditional malware-based tools and their growing propensity towards techniques that blend in with business-justified activity.

You Can't Protect What You Can't See

One of the reasons "new & emerging threats" are a concern is because they often target entities or devices that are not so obvious, such as IoT devices or the security cameras or IP phones in an organization. They also use TTPs that blend in with regular, business-justified activity.

The research from SANS Institute sheds some light on this. Respondents were asked to rank their satisfaction with 40 different categories of security tools. "Asset discovery and inventory" tools ranked dead last, and if they were evaluated by letter grade would receive an "F" (59% satisfaction).

Respondents feel like they have a good handle on their assets, and most respondents believe they maintain inventories on more than 75% of the assets in their environment. However, they admit to using time- and resource-intensive methods (i.e. manually looking up IP addresses, checking logs, etc.) that will make it impossible to keep up with both the increasing rate of IT change but also the numbers of security alerts.

SANS researchers have drawn important conclusions from this data. As the report says:

"The high level of manual responses shows that both the capabilities of the products and the skills of the analysts using them must dramatically increase to support more automated, more repeatable maintenance of accurate hardware and software inventories."

Researchers also point out where the industry needs to focus:

An additional opportunity exists for real-time asset discovery and classification based on network traffic analysis."

To make matters worse, network operations and security operations appear disjointed based on the findings of SANS research. Through an extensive line of questioning about how closely Security Operations Centers (SOCs) and Network Operations Centers (NOCs) collaborate, SANS makes the value of network data crystal clear. However, very few respondents who have a NOC (14%) report fully-integrated functions and workflow with their organization's SOC. The report adds:

"Synergy between the NOC and SOC in terms of shared information and shared goals can be a driving force for SOC efficiency and effectiveness. However, the survey demonstrates SOC/NOC integration is a point of substantial frustration for many SOC managers and analysts."

Manual Event Correlation Causes Blind Spots

Another finding from SANS supports the thesis that organizations struggle to see the full picture with current tools. Survey responses show that SIEM and big data products are widely used for event correlation and are getting better but – much like asset discovery and inventory – most event correlation is still manual. A vast majority of organizations (75%) rely on their SIEM to correlate and analyze event data, indicators of compromise and other security and threat-related data, but don't get the information or context they need. As SANS researchers state in the report:

"SIEM and automation/orchestration tools have improved their capabilities via enrichment from threat intelligence data sources that allow increasing the fidelity and priority of alerts that match known attack indicators. However, the low level of satisfaction from asset discovery and inventory tools indicates that large blind spots still remain."

In fact, the survey showed that:

54% of respondents believe critical alerts go completely uninvestigated

30% of alerts that have been prioritized never get investigated

Process inhibitors appear to be the biggest factors impacting event correlation and response. For instance, in the survey, 73% of respondents said each alert investigation can take hours or even days. This data validates just how long and drawn-out each investigation can be, requiring security teams to talk to multiple people and consult many different tools. Each step in a manual investigation takes time and 33% said they had to take more than 10 steps for every alert. In addition, 53% use three or more data sources to get to the bottom of an investigation. This is also significant since many of those data sources (e.g. DHCP logs) were not built with the security operations team in mind.

Arista NDR bridges the Network Security Gap

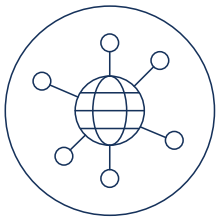
Looking at the key findings of these two surveys together highlights that security professionals are most concerned with protecting their hybrid networks from new and evolving threats, such as those that blend in with business-justified activity. They also expressed the sentiment that inefficient access to and use of network data is stopping them from improving security.

These are exactly the areas the Arista NDR platform was designed to address.

Arista NDR leverages its years of networking experience and integrates security into the network layer through its zero trust network detection and response capabilities that delivers a privacy-aware solution capable of detecting and visualizing behavioral, mal-intent and compliance incidents with full forensics context.

The Arista NDR platform protects against modern, non-malware threats such as malicious insiders, credential abuse, lateral movement and data exfiltration. As sophisticated attackers adapt tactics, techniques and procedures to blend in with business-justified activity and avoid detection, Arista NDRhelps organizations autonomously hunt and respond to threats missed by traditional security solutions especially in the middle of the kill chain when the attacker is inside the network and rather than using malware, uses existing business justified tools.

Arista's NDR Platform is comprised of three foundational components:



AVA Sensors

The Arista NDR Platform is built on a foundation of deep network analysis within AVA Sensors that span the "new network"—including the data center, perimeter, core, Internet of things and operational technology networks and those connecting cloud and SaaS resources. Unlike other network detection and response solutions, Arista NDR parses and processes layer 2 through layer 7 data, including performing encrypted traffic analysis. With this information, Arista NDR autonomously profiles entities such as devices, users and applications, while also preserving these communications to provide historical forensic context.

AVA Nucleus

Extracted activity data feeds into the AVA Nucleus which then identifies and visualizes incidents through automatic correlation across entities, time, protocols and attack stage. The platform also learns from past incidents as well as Arista NDR's customized cyber security, governance, risk and compliance playbooks to provide the security analyst with both automated and manual response options. These can trigger workflows within integrated solutions or simply recommend remediation steps such as evidence collection.

Arista AVA

Arista's AVA is the world's first privacy-aware security expert system. Arista AVA brings both a global and an industry specific perspective to perform autonomous incident triage. Using a combination of cloud-scale federated machine learning, open source intelligence and human expertise, Arista AVA minimizes the number of incidents the security team must act on. Through Arista AVA, customers also have on-demand access to Arista NDR experts for up-to-the-minute threat research, hunting and investigation support.

More information on Arista's NDR platform can be found at https://www.arista.com/en/products/network-detection-and-response.

SANS Survey Findings

Additional information on the SANS survey and a full version of the report, "The Definition of SOC-cess? SANS 2018 Security Operations Center Survey," can be found at https://awakesecurity.com/sans-soc-survey-key-findings.

SANS Survey Findings

Arista NDR partnered with Drive Research to conduct an in-depth survey of 300 Chief Information Security Officers, Directors and Managers as well as front-line security analysts. Qualified survey respondents had to be knowledgeable about the security operations, investigation and incident response processes for their organizations and the organizations themselves needed to have at least 51 or more employees. This white paper discusses the results of that research and analysis of the survey data.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office
1390 Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062