Atlantic Vantage Point

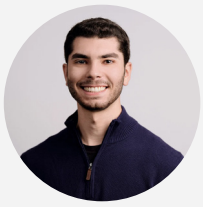
avpcap.com

Modernizing the Security Stack: Building Cyber Resilience for 2030

Part 1: SOC Automation and Threat Resolution

Jessica Hayes

Ethan Ellinger



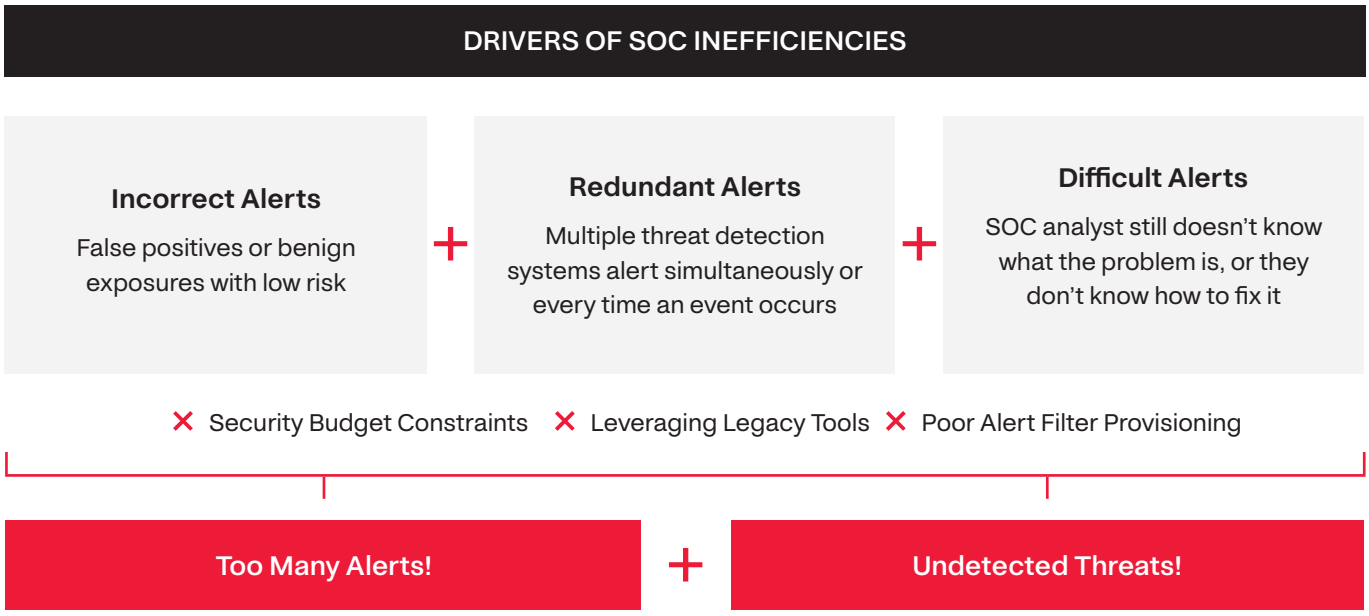
Ethan Volk

Bringing perspectives and investing in tech from both sides of the Atlantic

In 2025 so far, I've received 8 text messages telling me that my USPS package could not be delivered and 4 text messages telling me that I have unpaid tolls (I don't own a car). The suspicious messages ask me to enter personal details and credit card information in their online form - which I ignore and delete. However, when the time comes and a real postal worker can't find my apartment, my package will sit in a processing facility indefinitely, lonely and dusty.

This is a small, personal example of alert fatigue. I've been falsely told to take action a dozen times, so I am unlikely to act when I actually need to. It is a natural response - the more you're exposed to an alert, the more likely you are to ignore it[1].

Now overlay this issue in cybersecurity, where Security Operations Center (SOC) analysts are manually triaging ~4,500 threat alerts every day and 83% of them are false positives[2]. This daily cycle of finding true positive needles in a false positive haystack is driving alert fatigue and inefficiency in security organizations (and still, one in three cyberattacks go undetected). Below is a framework inspired by Anton Chuvakin (Security Advisor at Google) which unpacks these drivers further[3]:



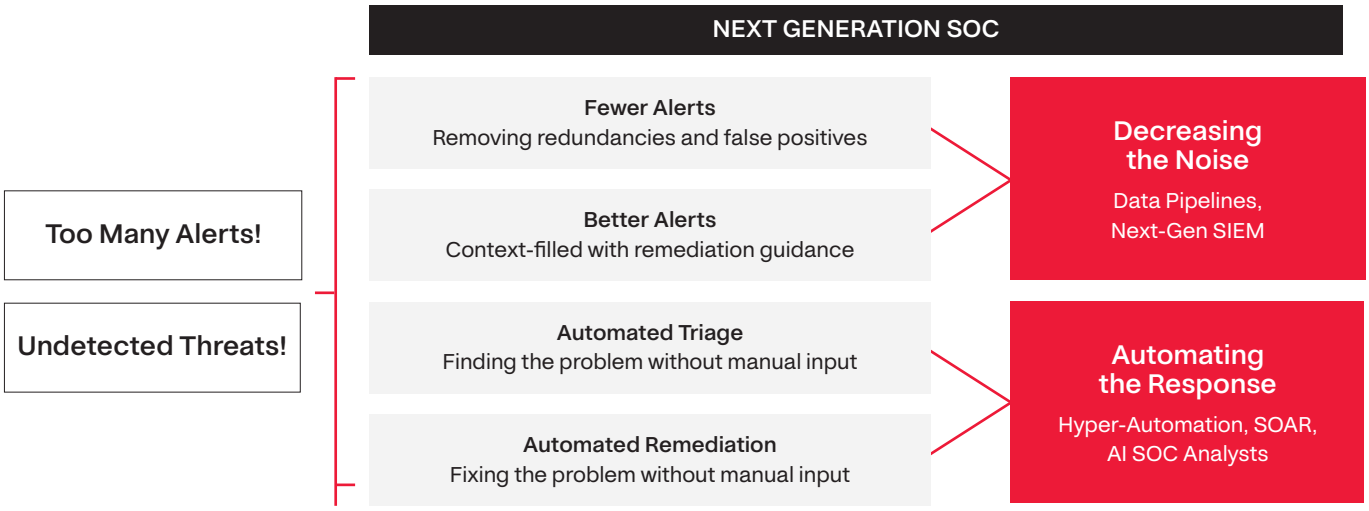
How'd we get here? In response to the increasing volume and sophistication of cyberattacks, security organizations implemented tools to detect cyber threats across each attack surface of their environment. Despite an effort to fine-tune these detections, most cybersecurity stacks still output thousands of incorrect or redundant alerts. Even the correct alerts (true positives) may not include the context a SOC analyst needs to properly address the problem. The result is detrimental to the organization's efficiency and security posture.

1. https://pmc.ncbi.nlm.nih.gov/articles/PMC5387195/
2. https://www.helpnetsecurity.com/2023/07/20/soc-analysts-tools-effectiveness/
3. https://medium.com/anton-on-security/antons-alert-fatigue-the-study-0ac0e6f5621c

What is the solution? In our view, solving the alert fatigue problem and optimizing for better security breaks down into two overarching themes:

- **Decreasing the Noise** - fine-tuning detections and consolidating alerts
- **Automating the Response** - resolving threat alerts with minimal human intervention

We believe this "Next Generation SOC" will have fewer, better threat detections and utilize automated systems to resolve alerts. This will allow our cybersecurity professionals to get off the metaphorical treadmill of alert triage to focus on strategy, risk mitigation, and proactive defense:



Why does AVP care about the next generation of the SOC organization? We see a very large, impactful problem - bad alerting, detection, and response - and we see new businesses offering creative solutions. At AVP, we've already invested in several leading players in cybersecurity like Contrast Security, SecurityScorecard, and Strider.

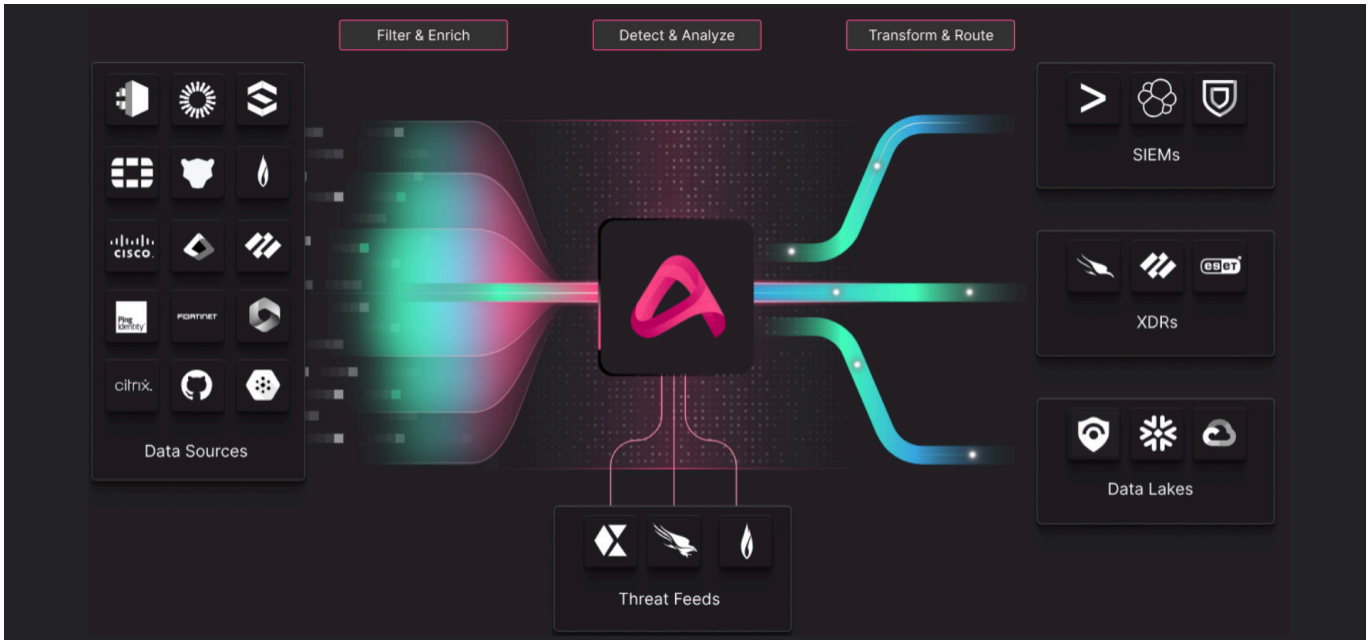
While we're cautious not to assume more SaaS tools and vendors = better cybersecurity, we see an exciting opportunity for businesses building next-gen SOC platforms. This is the first paper in a two-part series on modernizing the cybersecurity stack. In this paper, we will further detail the companies and technologies building the next generation SOC, from threat detection to resolution.

How can security teams decrease the noise from alerts?

Security Information and Event Management (SIEM) platforms provide a centralized solution to collect log and event data for threat detection, alerting, and analysis. Data is exploding, creating a wild west of logs, traces, and metrics that only make it harder to locate the signal in the noise. Existing tools flood SIEMs with more security telemetry than necessary, with data ingested by SIEMs covering ~87% of all MITRE ATT&CK techniques[4].

4. Sate of SIEM Detection (2024), CardinalOps

Most of this data can either be discarded or put into cold storage, something that **security data pipeline** companies like Cribl help companies achieve through their data filtering and reduction capabilities. Earlier stage companies like Abstract Security and Axoflow are also leading the charge on this problem, focusing more specifically on refining security data ingestion, enrichment, and real-time threat detection at an earlier point. These tools help companies proactively decide what data warrants immediate analysis, is needed for long term retention or is safe to discard. **Reducing noise at the source** — before it even hits the SIEM — not only saves on storage costs but also gives SOC analysts cleaner, more relevant data to work with.



Source: Abstract Security

Once relevant security data hits the SIEM, there are still pain points to address. Legacy SIEMs like Splunk have taken a **static or signature-based approach** to threat detection, looking for patterns that may point to malicious activity. This would work well in a world with a pre-defined universe of security threats and attack signatures, but today's threat landscape is anything but predictable. There are also several additional challenges with what legacy SIEMs offer today:

1. Often requires **significant implementation**
2. **Requires trained security professionals** to monitor and maintain the platform
3. **Cost can be exorbitant** as data ingested scales
4. On average, SIEMs have detection coverage for **only 1-in-5 techniques** in the MITRE ATT&CK framework[5]

With the growing variety of threats, detection methodologies demand repeated and ongoing **fine-tuning** to both adjust for new threats and minimize false positives. This can be a time intensive and manual task — with limited SOC resources and an overflow of unaddressed alerts, there just isn't enough time or money to go around.

5. State of SIEM Detection Risk (2024), CardinalOps

That's where AI-driven detection comes in. **Next-gen SIEMs** including Anvilogic, Panther and Hunters take more modern approaches to automating threat detections. Anvilogic's low-code detection builder helps SOC teams create and deploy detections in minutes while offering AI-powered recommendations to automatically fine-tune detection methodologies over time with a single click; Panther and Hunters both leverage out-of-the-box, pre-built detections and AI to automate the process of building detections while also offering tooling to tune and optimize detection queries.

Source: Panther

Legacy SIEMs weren't built for today's pace of threats — AI-native tools help teams detect faster, tune smarter, and finally start winning the battle against false positives.

How can security teams effectively respond to and resolve alerts?

As the SIEM triggers alerts, the SOC team jumps in to respond to threats. In large organizations with thousands of employees, SOCs operate 24/7 as a critical defense line. These centers often cost millions annually - mostly spent on human talent. Meanwhile, small to mid-sized companies typically outsource SOC functions to Managed Security Services Providers (MSSPs), which also rely heavily on human analysts.

A SOC's frontline team includes:

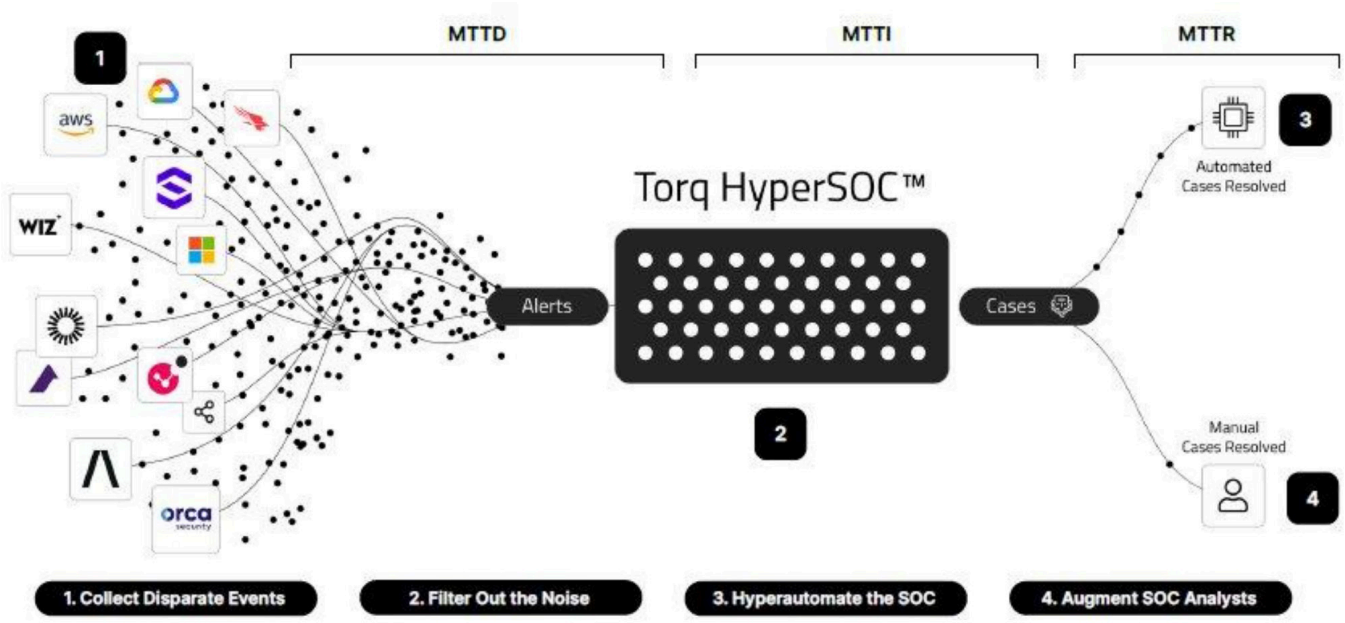
- **L1 analysts** juggling thousands of alerts daily, racing against the clock to resolve or escalate them within 30 minutes
- **L2 analysts** diving into the root causes of malicious threats
- **L3 analysts** proactively hunting down cyber threats before they escalate

With a staggering 4.8 million unfilled cybersecurity positions globally[6], inconsistency in analyst expertise, and an overwhelming flood of security alerts, it's no wonder the industry is turning to automation solutions.

The first wave of **legacy Security Operations Automation & Response** (SOAR) platforms, such as Phantom Cyber (acquired by Splunk in 2018), pioneered automated workflows but came with a catch — they relied on rigid "if-then" logic, making playbook creation and maintenance costly and complex.

The 2020s brought about the rise of **Hyper-Automation SOAR**, with next-gen SOAR platforms like Tines and Torq aiming to handle most Tier 1 SOC tasks to decrease a large majority of alerts. These platforms super-charge security operations by:

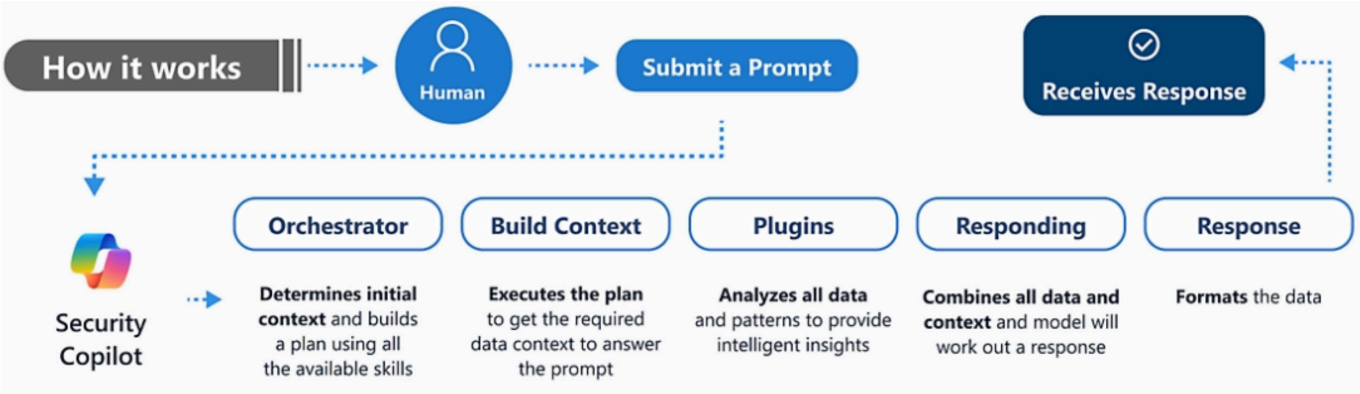
1. Using AI-powered filtering to correlate SIEM logs and tool-specific data via APIs, reducing false positive alerts
2. Enriching alerts with additional context such as threat intel and user behavior
3. Enabling intuitive automation workflows with natural language and flexible integrations, making triage playbooks easier to implement and adapt



Source: Torq

Over the last two years, **AI-driven Extended Detection and Response (XDR) platforms** have entered the automation scene, expanding beyond traditional Endpoint Detection and Response (EDR). Take Microsoft's Security Co-Pilot chatbot, which provides contextual insights and auto-generates reports for SOC analysts. But there's a catch: these tools are often limited to their own ecosystems and are limited to more basic capabilities.

6. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study



Source: Microsoft

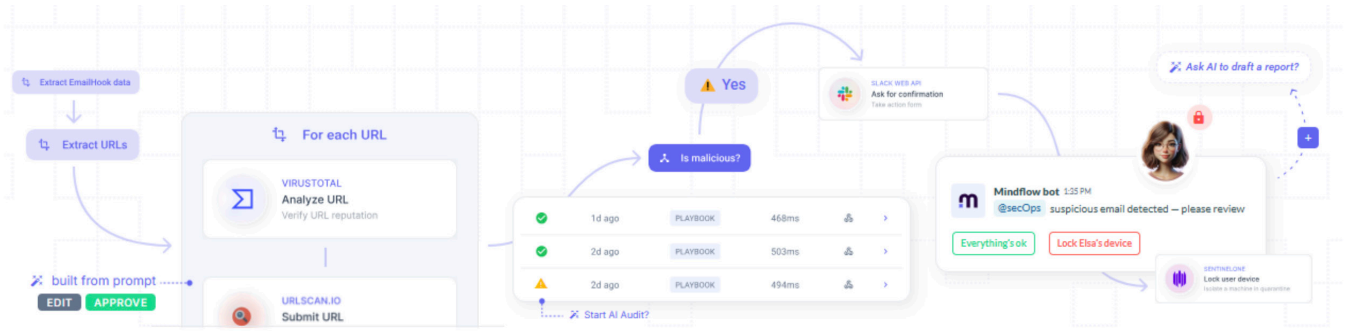
Market Opportunities and Considerations

Enterprise high cost of switching: Most Fortune 500 companies have already invested heavily in hyper-automation SOAR playbooks. Ripping out and replacing these systems is expensive, making the market tough for new entrants. Therefore, growth-stage companies like Tines and Torq are well-positioned to maintain their lead.

The mid-market dilemma: Emerging **Tier 1 AI SOC** solutions such as Dropzone, Radiant, and Prophet are focused on triaging and decreasing false positive alerts. Given the stickiness of enterprise solutions, they are better positioned to sell to mid-size companies; however, many mid-sized businesses prefer fully managed security services from managed detection and response (MDR) providers. Given this smaller market, some solutions are shifting their business models to target managed security services providers (MSSPs). For example, companies such as Guardz provides a AI-powered platform with multi-tenancy to address needs of MSSPs, while others such as AirMDR are looking to become an MSSP itself by blending automation with human oversight to provide a fully managed service.

Opportunity for nuanced investigation & threat detection: While AI has made strides in Tier 1 automation, solutions thin out for **Tier 2** (investigations) and **Tier 3** (proactive threat hunting) automations. This is an interesting opportunity for new entrants, as these areas require experienced SOC judgment. CommandZero, for example, assists analysts by suggesting investigative questions and guiding them through complex branches and queries. There's huge potential in reinforcement learning for AI-driven solutions that continuously refine their accuracy over time.

Shift towards ultra user-friendly: Simplicity is becoming a major differentiator, with companies such as Swimlane gaining traction thanks to its ease of use and high NPS scores. Emerging players like BlinkOps and Mindflow emphasize no-code automation, making security accessible to a broader audience. These tools integrate security and IT operations, allowing organizations to automate not just security workflows but broader processes like ticketing and incident management. These solutions can be a standalone SOAR solution for small to mid-size businesses and MSSPs or augment a SOAR platform for enterprises.



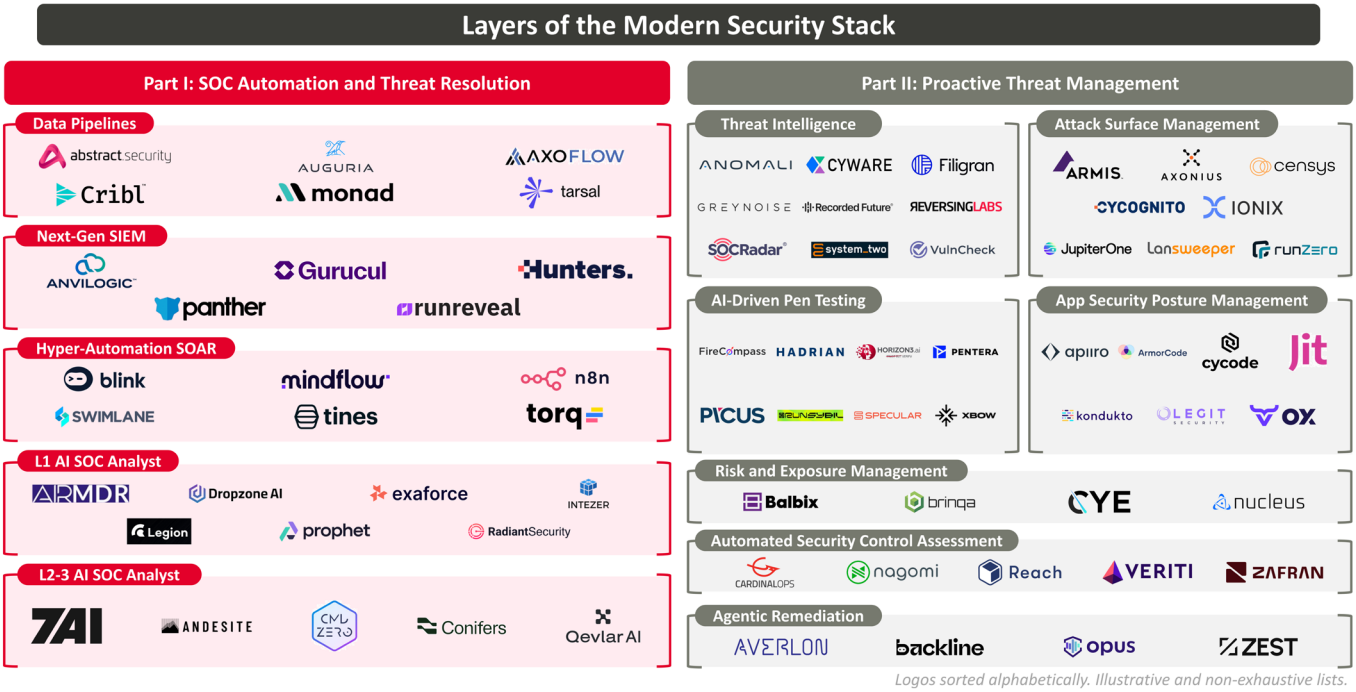
Source: Mindflow

By utilizing next-gen SOAR and AI SOC platforms, organizations can automate and streamline workflows, ultimately allowing human analysts to focus on more complex tasks for quicker threat resolution.

Conclusion

Despite multiple decades of progress and automation in cybersecurity, the SOC faces similar problems as they did 20+ years ago: too many alerts, too few people, and difficult threats to triage. Fortunately, we believe in a near-term inflection point where threat alerts generate less noise, and responses become more automated.

We see an exciting market opportunity for companies solving these problems and building the Next Gen SOC:



Logos sorted alphabetically. Illustrative and non-exhaustive lists.

What will cybersecurity analysts do with all this newfound free time? We believe the next step is proactive threat management - mitigating risks and exposures, patching vulnerabilities, simulating security breaches, and so on. Stay tuned for the next paper in our two-part series on proactive threat management in a modern security stack.

At AVP, we are eager to partner with the people creating next generation platforms that protect our data, physical infrastructure, and IT systems. If you are building an early stage or growth stage company in this space, we would welcome an opportunity to meet with you.

You can reach out to jessica.hayes@avpcap.com, ethan.volk@avpcap.com, ethan.ellinger@avpcap.com, or connect with the rest of our colleagues at avpcap.com.

avpcap.com

Atlantic Vantage Point

Bringing perspectives and investing in tech
from both sides of the Atlantic

New York Paris London