REVSOC

REVOLUTIONIZING SECURITY OPERATIONS

# Autonomous Incident Responder

The premier cloud-native, open XDR.

www.revsoc.ai | info@revsoc.ai | +1 (650)-830-1021


## Introduction

Hacker sophistication continues to outpace traditional defense technology such as SIEM, DLP, UEBA, and SOAR. The fallout of such breaches will continue to increase in magnitude due to widespread migration to multi-cloud platforms, serverless deployments and the large-scale adoption of SaaS applications.

Complex scenarios require sophisticated automation, especially with the explosion in the volume of data available for analysis. A 2020 Forrester Wave report laid out the future of security options and how tools need to be cloud-native and provide automation of all trivial processes to meet the demands of modern security.

Exclusively manual approaches lead to investment in more tools, and consequently, an unnecessarily long time to deploy & onboard. Consequently, the process of automating more and more runbooks does not scale. Furthermore, analysts need to proactively hunt for threats and respond to incidents, not learn a new scripting language for each new tool acquired. The detection capabilities of many current tools is limited to Boolean Logic matching encapsulated in what is usually referred to as rules, and this simply does not cut it anymore. Detecting today's attacks requires more complex data models.

## Log Collection/Data Quality

Depending on the number of employees, a company can average anywhere from ten million to six billion events daily for security analysis. Due to the sheer volume of data that needs to be cleaned, correlated, analyzed, and validated, existing manual methods to execute these processes simply cannot withstand the explosion of data resulting from increased digitization and the shift from on-premise to cloud-based infrastructure.

The enormity of this problem set the stage for what we wished to solve with the RevSoc Autonomous Incident Responder (AIR). Despite engineering a collection of over two-thousand detection models, we understood from the jump that detection is only as effective as the quality of the input data. With this in mind, we have created a robust collection and transformation pipeline for over one-hundred raw data sources to automate the organizational logic for an effective data model.

Beyond that, the RevSoc AIR is also capable of sitting upstream from your existing security stack with both agent-based connectors and understanding of APIs for commonly used log-management and security tools. Here is a condensed view on some of our most common integrations but you can get the full list from our Data Sheet at www.RevSoc.ai/resources.

### Data Integrations

| | |
|---|---|
| Cloud | AWS, Azure, GCP |
| IAM | Okta, BeyondTrust, Active Directory |
| Immutable | Kubernetes, Terraform |
| SaaS | Snowflake, Github, Slack, Netsuite, Zoom, O365 |
| Log Managment | Splunk, QRadar |
| EDR | Crowdstrike, Sophos, Rapid7 |
| Network | Palo Alto, Cisco, Zscaler |

[1] *Forrester. Zelonis, J. (2020). The Forrester Wave: Enterprise Detection and Response Q1 2020.*

## Digital Incident Responder

A survey of Fortune 500 companies from Crowdstrike has suggested that 35% of security alerts in the queue go uninvestigated. If over one-third of alerts go ignored by the companies with the most resources, this figure paints a grim picture for SMB and mid-market companies that are either just starting their SOC or still don't have a roadmap for one. This problem is a result of a lack of bandwidth to perform incident prioritization, root-cause analysis, and remediation in a timely manner.

Our goal has alway been to drastically reduce the mean-time-to-response (MTTR) and put time back in analysts' hands. So, we set out to automate the trivial areas of incident response like incident logging and alert prioritization. Our auto-incident creation mechanism autonomously prioritizes incidents without any analyst intervention so the incident responder can quickly get their hands on the most pressing alerts.

Moreover, the alerts that comprise each incident are organized in a chronological timeline view with analysis of each including how many other users triggered the same alert and AI fueled predictions on the likely next scenario to occur. These features enable the incident responder to take action quickly and confidently.

### Sample Alert--Lateral Movement


## Digital Threat Hunter

One of the greatest challenges in SecOps is understanding what to detect and what not to detect. Detection engineering, or the process of identifying and implementing detection capabilities, can be extremely difficult due to time and expertise required. Due to their relative ease of implementation, rules have been the most widely engineered detections. But, because they are essentially conditional statements, they result in high volumes of false positives. The complexity of modern threat vectors require dynamic solutions that not only provide a wide-breadth of coverage but are capable of improving to provide a limited set of accurate and actionable alerts.

At RevSoc, we recognize the difficulty in not onl understanding what detections are required but also implementing them. This is why when we set out to begin detection engineering we surveyed hundreds of security analysts to get a grasp on what their biggest pain points were and what detections they believe they need but might not have the resources to implement.

From this research we were able to glean the most valuable use cases for SaaS applications, Cloud Posture Management, as well as serverless, container-based vulnerabilities. With our combined expertise in the domains of cybersecurity and data science, we proceeded to build out a catalogue of more than two-thousand detections encompassing rules, time-series models, and deep learning.

Furthermore, with our evolutionary learning mechanism and genetic algorithm, we are now able to constantly improve our existing detections and even generate new rule sets to ensure that many of our blind spots are covered.

[2] *IDC. Richmond, C. Robinson, C. Vasquez, M. (2021). The Voice of the Analysts Improving Security Operations Center Processes Through Advanced Technologies.*

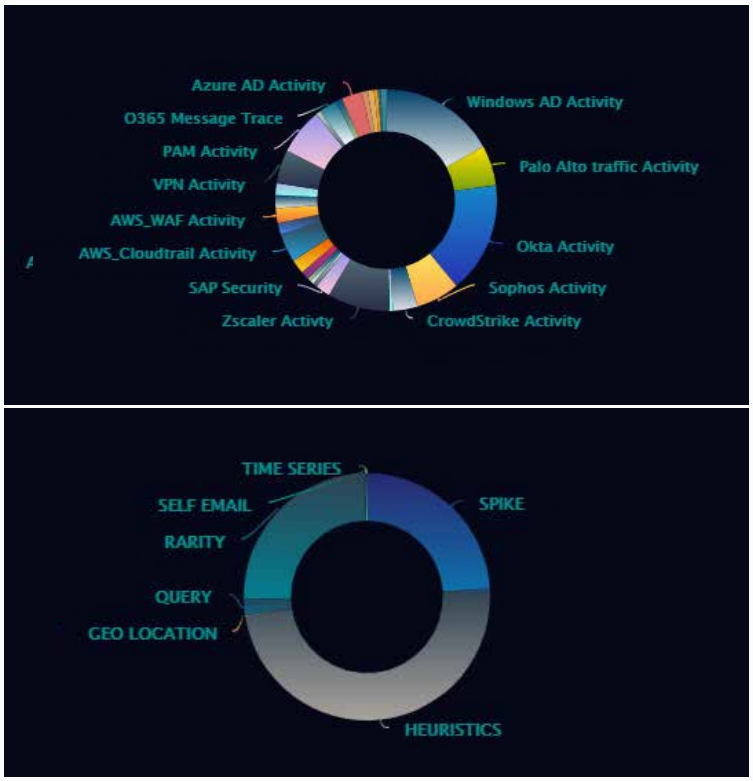
## ModelX

With over two thousand models available out-of-the-box, the RevSoc AIR is one of the most comprehensive detection platforms in terms of Tactics, Techniques, and Procedures (TTP) coverage. RevSoc invested the time in building this broad detection coverage so your security team can go from reacting to alerts to getting in front of them and focus on threat hunting. Of course, you won't be going at it alone.

The RevSoc ModelX is a mechanism where we are able to take the learnings from one customer environment and exchange that with the learnings of others. For example, if we find a new procedure used by attackers for privilege escalation on S3 buckets in one customer environment, we will transport the detection models based on these learnings to all other customers that deploy on AWS.

We believe this is an effective way to foster a community where our customer base works with us and each other to proactively ensure all our customers remain secure.

**Model Breakdown (by Data Source and Model Type)**




## Conclusion

The gradual, decade-long shift to cloud-based and serverless driven architecture has culminated in a new frontier of threats that will affect companies going forward. The volume of data needing monitoring has become so large and complex that the simple rules-exclusive approaches of the past are no longer sufficient. A manual approach exacerbates the issue through the volume of false positives it leads to, creating chaos across security operations.

In the past, observing breaches as they occurred may have been an acceptable risk, but the volume and velocity of modern-day threats require proactive and comprehensive defense capabilities. The new acceptable level of preparedness requires visibility across all SaaS configurations, access levels for all users, and autonomous detection and response methods when an exploitation occurs.

The RevSoc AIR materialized from witnessing these problems first-hand and continuously strives to answer the call by putting power back in the hands of the analyst and fostering strong partnerships to eliminate blind spots and secure any and all organizations.