NETENRICH

# THE NETENRICH GUIDE TO AUTONOMIC SECURITY OPERATIONS

# TABLE OF CONTENTS



What exactly is Autonomic Security Operations (ASO), and why do many of the best minds in cybersecurity think it's the future of security operations?

This guide will give you an overview of key concepts and terms, explain why and when ASO is important, and point you to resources to learn more and help you get started on your ASO journey.

**4 pillars of Autonomic Security Operations**


As described in "**Autonomic Security Operations: 10X Transformation of the Security Operations Center**" by cybersecurity leaders Anton Chuvakin, senior security staff, Office of the CISO at Google, and Iman Ghanizada, global head of Autonomic Security at Google, ASO is a new approach for improving an organization's security posture and reducing risk. It addresses the increasingly difficult issues traditional Security Operations Centers (SOCs) face — including alert fatigue, false positives (and false negatives!), talent deficit, turnover and burnout. Issues that are hindering organizations from winning the war against ubiquitous threat actors, insider risk, misconfiguration, and configuration drift.

## What is Autonomic Security Operations?

Chuvakin and Ghanizada position ASO as "a combination of philosophies, practices, and tools that improve an organization's ability to withstand security attacks through an adaptive, agile, and highly automated approach to threat management."[1]

ASO uses automation, machine learning (ML), and artificial intelligence (AI) to minimize the need for human intervention while improving the effectiveness and efficiency of cybersecurity operations.

“Autonomic” computing refers to the idea of creating self-managing and self-healing computing systems. Think of it not just as a self-driving car, but a self-driving car that can also adjust and repair its own engine without disruption.

In security operations, autonomic capabilities go beyond automating repetitive tasks to free up resources. They also enable intelligent detection and response to security threats and improve risk management.

Key capabilities of ASO include:

1. **Automation of routine and repetitive tasks**, including things like log analysis, patch management, and vulnerability scanning. This automation eases drudgework for human analysts and can improve response times as well as overall execution.

2. **AI and ML** to detect anomalies, identify patterns, and improve decision-making based on very large and constantly growing volumes of data from security systems, network infrastructure, and tools. Using AI and ML technologies can improve threat detection and speed incident response, as well as pave the way for more predictive analytics that support more proactive risk mitigation/reduction.

3. **Threat intelligence and analytics** that continuously monitor and analyze data — from logs to threat feeds (both custom and established) and network traffic — to provide enhanced situational awareness. Autonomic systems identify threat trends, correlate data and events, and deliver near-real-time intelligence that further improves decision-making.

4. **Adaptive and dynamic defenses** that automatically adjust configurations and access and can deploy countermeasures. ASO is adaptable, so organizations can not only adapt to an evolving threat landscape, but also proactively change their own IT environments based on real-time analytics and extensive context to make it more difficult for threat actors to use automated tools to exploit vulnerabilities. In short, applying the concept that moving targets are harder to hit.

5. **Resilience and self-healing** systems that can automatically respond to incidents, isolate or contain affected systems, and proceed with remediation. These capabilities reduce the time (and cost) of incident response and help address and minimize potential damage.

6. **Integration and orchestration** across all security tools and systems — from firewalls to intrusion detection and security information and event management (SIEM) systems and more — to deliver greater visibility, context, coordination, response, and remediation.

Once again, it's about ASO using automation, AI/ML, and advanced intelligence and analytics to increase the efficiency and effectiveness of cybersecurity in a modern, connected, and cloud-centric world. By focusing on automating repetitive and manual work, faster threat detection and response, and increased situational awareness, companies can reduce risk and protect their most valuable assets.

| Autonomous vs. Autonomic | |
|---|---|
| "Autonomous" and "autonomic" often show up as synonyms, but in technology terms, they convey different meanings.<br><br>**Autonomous computing** means that a machine, a device, or software can operate with little or no human control; that is, it can operate independently. A self-driving car, for example, is operating autonomously. | **Autonomic computing** is not only about operating independently, but also having the awareness and adaptability to respond to its environment. Defined by IBM in a 2001 manifesto, "The Vision of Autonomic Computing," there are four areas of autonomic computing: self-configuration, self-healing, self-optimization, and self-protection.[2] A car that could self-tune and refuel without intervention would be operating autonomically. |

# Why it's time for Autonomic Security Operations

Key characteristics of every autonomic computing system are "automation, adaptivity, and awareness." The concept itself is not new. In fact, IBM published a manifesto about it more than 20 years ago.[3]

However, the exponential shifts in computing power and scale over the past two decades have made it increasingly apparent that organizations must transform the way they secure and operate if they are to survive, never mind grow and scale.

## 4 Areas of Autonomic Computing

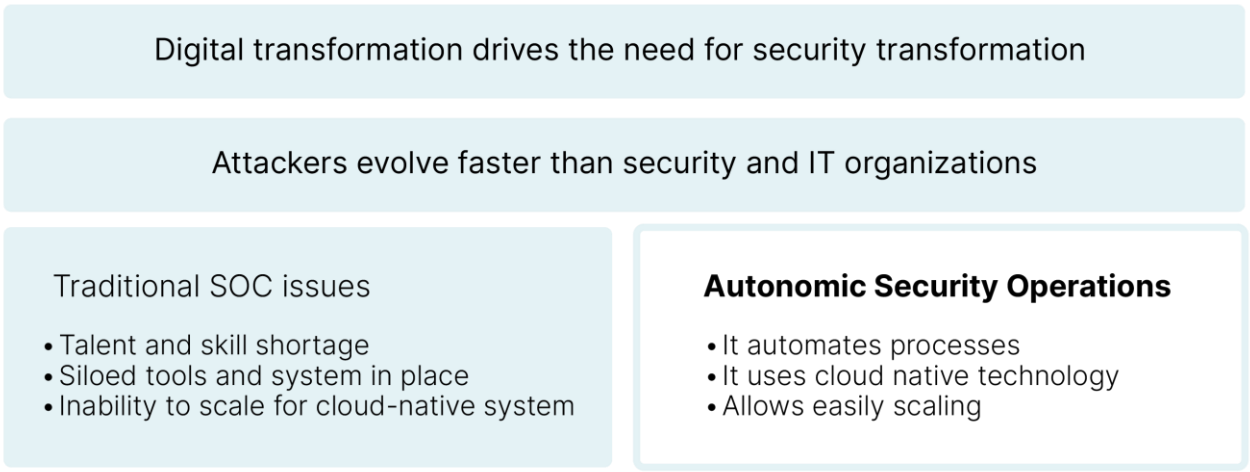

Today, there are two critical trends driving the need for a shift to **autonomic security operations** sooner rather than later:

- **Digital transformation drives the need for security transformation.**
    - A changing and dynamic attack surface expands security risks far beyond traditional SOC responsibilities to encompass things like fraud, identity theft, ransomware, and other threats. “Operational fusion is needed now more than ever,” according to Anton Chuvakin and Iman Ghanizada.
    - Modern computing environments are fluid and dynamic, with constantly increasing data volumes. More data and more potential for adverse events require more security coverage. Significant talent and skills gaps already hamper most security organizations, so adding more tools and people isn’t a viable solution.
- **Attackers are evolving faster than security and IT organizations.**
    - The increased complexity in modern computing environments creates a larger attack surface, giving attackers more opportunities and more ways to increase their stealth; they can get in and lurk within an organization, waiting to carry out their ultimate goal. Persistent threats “are often undetectable by traditional approaches,” say Chuvakin and Ghanizada. Companies need robust threat intelligence and threat hunting capabilities to maintain and secure their digital operations.

Traditional SOCs are just not set up to address these challenges. They face a shortage of talent and skills to run the tools and systems they already have. They operate with processes that aren’t designed to meet cloud-centric and hybrid workload needs.

And they're tasked with managing an existing arsenal of typically isolated tools and technologies that do not and cannot streamline and support detection and response at scale.




One key goal of ASO is to automate processes and use more cloud-native technologies that can address the expanding attack surface and manage modern threats at cloud scale. So how can you get started?

## Getting started with the journey to Autonomic Security Operations

If getting started with ASO seems like an insurmountable task, it doesn't have to be. While the Google paper indicates a need for 10x the resources currently in place, it's really about getting to 10x the productivity — and it is possible to do that by taking advantage of specific technologies, like Netenrich **Resolution Intelligence Cloud**. This platform leverages automation, machine learning, and other capabilities to drastically increase productivity, pivoting away from the traditional SOC model (aka 24/7 alert monitoring) to focus on high-priority issues and proactive threat hunting.

Getting started with ASO requires:

- Understanding what you have (inventory of all devices generating logs and data).
- Getting that data into one place (so it can be analyzed and correlated, using automation to address all the data).
- Applying AI/ML to the data (to gain context and understand what's happening and what matters).

- Gaining a better understanding of and visibility into threats (to see gaps in coverage using threat mapping, find anomalies, and uncover trends to strengthen threat hunting capabilities and augment threat intelligence).
- Implementing processes and technologies to bubble up the important events that require action and increase visibility (using patterns and rules, machine learning, and AI).

One key to accomplishing these tasks is to implement automation using a platform that has the right technology, can ensure the right processes are in place, is accessible to all the people in the organization (with the right roles and access in the system), and can be aligned with business needs (with the ability to automate processes and remediation and give authority to the right people).

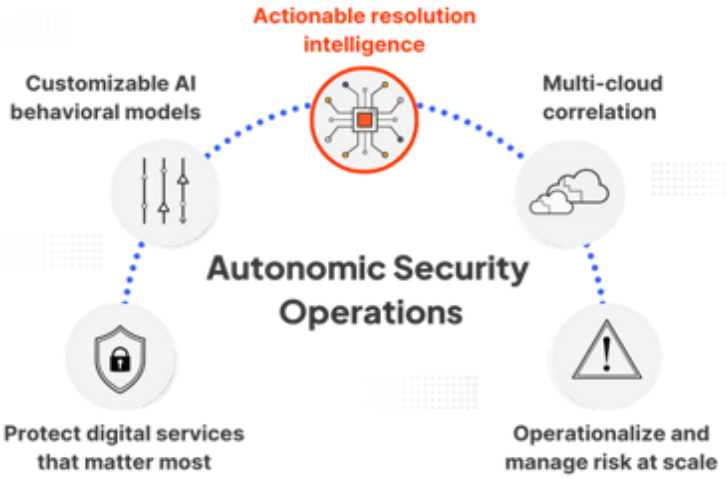
Achieving a state of ASO, as Google's Chuvakin and Ghanizada note, requires a combination of philosophies, practices, and tools that will improve an organization's ability to recognize the important threats, withstand security attacks, and have full visibility across their entire infrastructure. As part of this, they see a need to shift perspective on security operations to be more like Site Reliability Engineering (SRE), whereby teams spend 50% of their time on operations and 50% on automation with a relentless focus on reducing "toil." Per Chuvakin and Ghanizada, "Detection engineers develop solutions to solve detection challenges at scale and not shuffle through traditional analyst workflows. They also manage the alerts their solutions create, and use that data to further refine their detection logic."

## How to achieve Autonomic Security Operations with Resolution Intelligence Cloud

By implementing a solution like Netenrich **Resolution Intelligence Cloud**, organizations can take a first step toward exponentially improving the abilities and effectiveness of existing staff while also automating operations and security processes and workflows. Resolution Intelligence Cloud is a cloud-native technology that operates at Google speed and scale with minimal operational overhead, allowing customers to focus on solving today's security challenges and quickly adapting to evolving requirements. Further, the platform addresses the need for a flexible and scalable security foundation — for example, a cybersecurity mesh architecture (**CSMA**) — and leverages the **MITRE ATT&CK Framework** to improve threat hunting and incident response.

If you're looking to "future proof" your approach to securing your organization's digital operations and want to learn more about how to adopt ASO with Resolution Intelligence Cloud, check out the resources below or contact Netenrich to **set up a demo**.




## Retire your SOC by designing business-specific detections

For years, security vendors have been engineering detections (aka alerts) based on external global data and what they believe is important. Consequently, organizations need to hire a lot of people (aka a SOC) to sift through the tremendous amount of noise these broad detections create. Most SOCs are in panic-driven reaction mode, with too many tier-one analysts spending the majority of their time triaging a mountain of non-contextualized alerts (aka 24/7 monitoring).

Achieving ASO begins with metrics and data quality. That's why Netenrich focuses on filtering, analyzing, and proofing data for quality and then, continuously designing, redesigning, adapting, and finetuning detections that are unique to organizations' business to reduce noise and ensure high-fidelity signals.

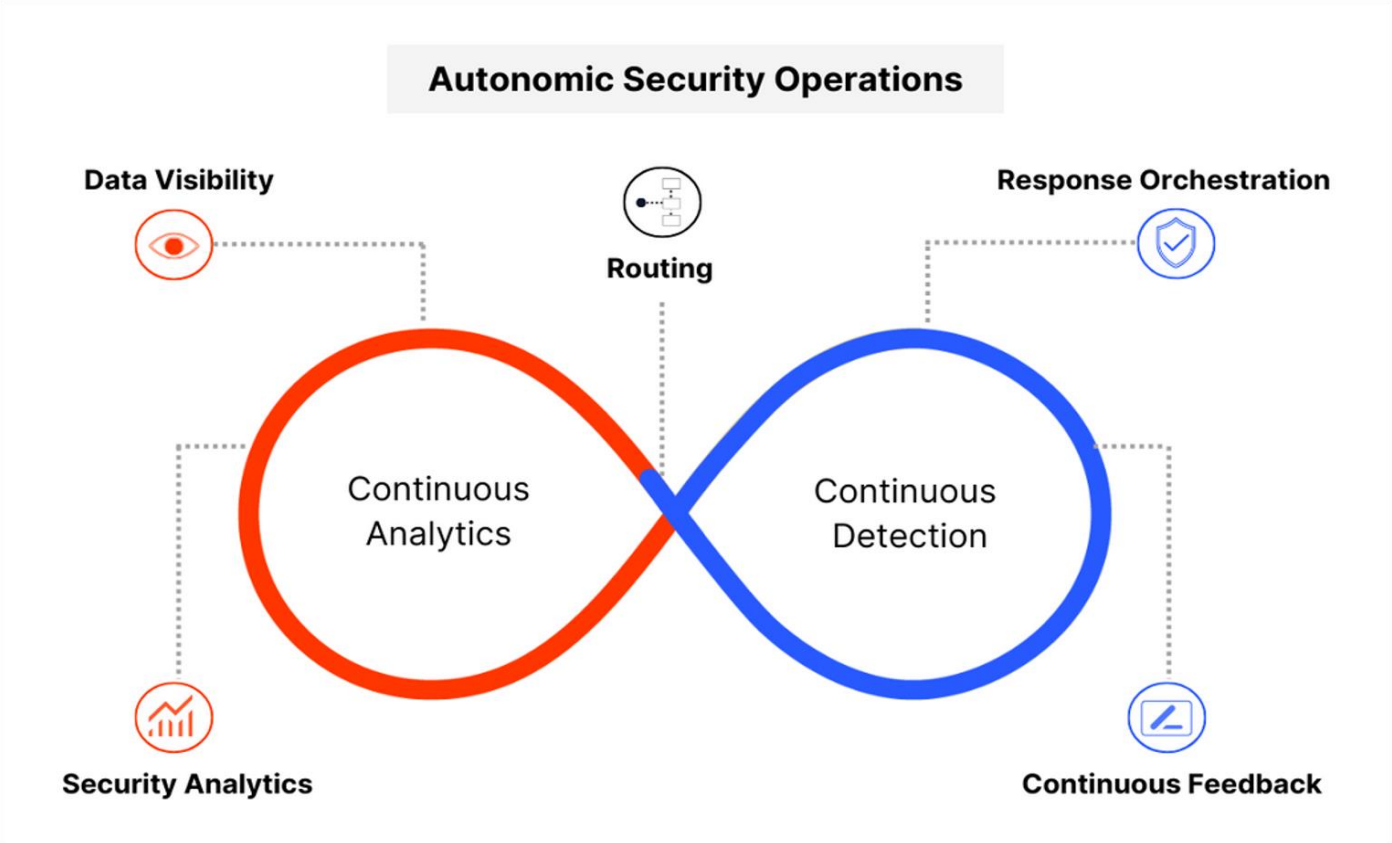
## Advanced data analytics and continuous adaptation to manage risk

Netenrich also focuses on quantifiably managing risk by using advanced data analytics and machine learning algorithms to monitor and tune processes and systems. The goal is to understand what's normal and acceptable across environments so we can engineer detections that drastically reduce false positives while also performing control engineering on the backend to make continual improvements and ensure optimal efficiency.

With the Resolution Intelligence Cloud platform, we can automate, for example, log analysis, patch management, and vulnerability scanning while also crunching alerts down to a manageable number so teams can shorten their response pipeline and have more time for other higher-priority tasks.

## The Pillars of ASO



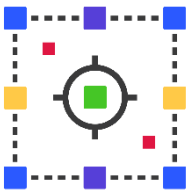
## Data Visibility

Data quality begins with data visibility. This step is about discovering what's in an environment and determining what data to collect.

## Security Analytics

Security analytics is about gaining situational awareness and quantifying risk. At Netenrich, we use behavioral modeling to create deeper risk profiles and perform enrichment on particular events or assets to gain greater context before tying it all together to better understand potential impact.

## Intelligent Routing

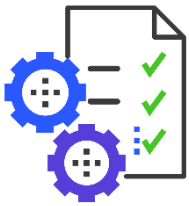


Intelligent routing means getting the right information to the right people at the right time. With Resolution Intelligence Cloud, there are impact-based escalation policies that dictate the distribution of actionable insights (ActOns) to specific individuals for review and response.

## Response Orchestration

For response orchestration, Resolution Intelligence Cloud automates data aggregation and analysis to reduce manual toil and free teams to work on more challenging work. When an alert is routed to an end user, that user has a clear picture (ActOn) of what's affected, what the impact is, and what the associated threat intelligence is. This actionable intelligence is also tied into a collaborative workbench, where users can bring in other relevant people to decide on a course of action.

## Continuous Feedback



Netenrich is constantly measuring various metrics and reviewing historical trends to improve data quality and adapt workflows. From every lesson learned, we tune systems and make changes to improve processes and ultimately, achieve specific organizational KPIs.

# WATCH: How to achieve ASO with Resolution Intelligence Cloud

# WATCH: Evolution of SIEM and the Rocky Journey to Autonomic Security Operations

Dr. Anton Chuvakin of Google Cloud Security's Office of the CISO and John Bambenek, principal threat hunter at Netenrich, discuss the progression of SIEM from on-premises to the cloud to autonomic security operations. They discuss our industry and whether it can exceed SIEM limits to achieve "ops nirvana" or data analytics-powered security operations.


# WATCH: SIEM in the Modern Era

Google Cloud security specialists Dr. Anton Chuvakin and Timothy Peacock lead a challenging discussion about modern-day SIEM. David Swift, a Netenrich expert, joins them to share real-world observations on the daily threat hunting and threat research grind.

[1] "**Autonomic Security Operations: 10X Transformation of the Security Operations Center**," Iman Ghanizada and Dr. Anton Chuvakin, 2023.

[2] "**The Vision of Autonomic Computing**," Jeffrey Kephart and David Chess, IBM, 2001.

[3] Techopedia: **Autonomic Computing**