NETENRICH

Netenrich Guide to Secure Operations

Strengthen cyber resiliency and reduce business risk

Netenrich Guide to Secure Operations

Strengthen cyber resiliency and reduce business risk

Secure operations is a holistic approach to digital operations and cybersecurity that improves cyber resiliency and reduces business risk efficiently and cost effectively, particularly at large scale. It reduces the business impact of cyber risks by operationalizing how you manage increasing infrastructure complexity, growing cyberthreats, and fallible humans.

Secure operations is not…

Secure operations is not the same as security operations or security operations centers (SOCs). Rather, it is a superset of security operations that encompasses all digital operations and breaks down the silos between them. Secure operations is not about having lots of cybersecurity and digital ops tools. It's about having the right technologies and the right data to support your digital ops and security teams working together with maximum effectiveness.

Why secure operations? Why now?

All digital operations should be secure, especially those that keep the business in business. No organization is immune to cyber threats, but larger organizations and service providers face significant challenges running all digital operations securely at scale. As CISOs and CIOs know, it's not a matter of whether you'll be breached, but when.

A note about scale: You need secure operations at scale whether or not your business is growing. That's because of the rapid increase of both infrastructure complexity and the frequency of cyber attacks. Current methods and tools can't handle it, and the numbers prove it:

- The average cost of a breach in the US is now $9.44 million, $4.62 million for ransomware breaches.
- The average time to respond to a breach is 277 days.
- If you can contain a data breach in 200 days or fewer, you can save $1.12 million on average.[1]

It's compelling cost justification for reducing resolution time and fortifying security postures to avoid breaches altogether. Yet cyber resiliency remains elusive despite increasing budgets and the high number of security tools in use. According to IBM's most recent Cyber Resilient Organization Study, 45% of respondents say their companies use more than 20 security tools, yet 70% say they don't have the right number of cybersecurity tools. That's because cyber resiliency is not a tools issue.

---

1 "Cost of a Data Breach 2022 Report," IBM.

The same report found that the top three reasons why cyber resiliency has not improved are all operational issues:

1. Inability to reduce silo and turf issues.
2. Fragmented IT and security infrastructure.
3. Lack of visibility into applications and data assets.

Secure operations solves all three of these key issues.

Converging security and digital operations improves availability and reduces risk

It's time to think differently about how we approach operational integrity and security, and that's what secure operations does. As described in Dark Reading commentary Better Together: Why It's Time for Ops and Security to Converge, operations and security organizations share two main goals:

1. **Availability:** Ops teams ensure business systems and information are readily available to all who need access. Security teams ensure the right data is available to the right people at the right times on the right devices.
2. **Risk:** The operations view of managing risk focuses on keeping systems up and running, avoiding downtime and poor performance, and supporting business productivity and efficiency. Security organizations view risk in terms of avoiding data loss, manipulation, and damage to the business.

The most effective — and cost-effective — way to achieve these goals is by converging digital operations and security, enabling them to work together with a common operational picture, shared data, and the right tools.

Secure operations from a technology perspective

The talent gap is a struggle. Digital ops and security teams continue to try to hire more people and acquire more tools to stay ahead of growing infrastructure complexity and increasing security threats. Secure operations leverages technology: Not more tools, but rather, the right tools that work together, without dangerous gaps or inefficient overlaps. And lots more data.

Technology for secure operations must deliver:

- Common operational view of all security and operations data, over time, fast and at scale. That means ingesting all data without filters, which can leave out important data points that hackers can exploit.
- Data analytics to reveal patterns that indicate incidents and, critically, potential incidents you can resolve proactively before actual incidents occur.
- Situational awareness and context tied to business risk awareness that enables fast, proactive response to what matters most.
- Mapping to best-practice operational frameworks that clarify not only what is or could soon happen, but how best to respond.

Ingesting all your data for a common operational view

Digital operations and security teams can't work together effectively without a common operational picture. The only way to achieve that is through shared data — all of it.

Any technology solution you rely on for performance and security needs to start with all your data. Filtering too early creates blind spots — any data point may be part of a pattern you will miss if you don't include it.

Until recently, ingesting all operations and security data has been extremely expensive and slow at scale for enterprises and service providers unless they spent millions and hired armies of skilled analysts. Even if they did bring in all that data, they didn't have effective ways to use it to improve outcomes. That's changed with new technology, like Resolution Intelligence Cloud.

Data analytics, machine learning, and automation

Data analytics, machine learning, and automation are core to secure operations at scale.

- **Data analytics** across all your data from operations and security reveals patterns of behaviors, connecting the dots — alerts, assets, users, known threats and their MITRE ATT&CK patterns, and more. Using detection rules is good (it's deterministic, so you can't detect what you don't have rules for), but finding patterns is critical to discovery left of boom (before cyberattacks are successful). Correlating data from disparate sources over time, data analytics surfaces related data — insights and context — for understanding and responding to threats and performance issues sooner and faster.
- **Machine learning** improves detection and resolution of security and ops issues in ways that humans can't. Learning from vast amounts of data, a machine learning system can identify trends and anomalies, then recommend and automate solutions. Over time, it continues to improve.
- **Automation** is critical to scale. Low-level tasks (often performed by Level 1 and 2 analysts) are completed consistently and faster, without human intervention, enabling analysts to focus on the hard challenges.

The combination of data analytics, machine learning and automation are also a requisite to creating an autonomic SOC, aka autonomous SOC.

Deduplication and grouping alerts is not enough — necessary but not sufficient. There are still far too many alerts, the vast majority of which are not important in and of themselves. Many don't require human intervention anyway — response can be automated, freeing analysts to focus on the most important situations that require their expertise.

What makes an alert important and worthy of time to investigate and respond? That depends on context — what else is happening, now and over time. It's the patterns that matter, such as what series of events have happened when, on which devices, by what users, located where, with what permissions, etc.

Technology for secure operations identifies risky patterns over time. Threat actors learn quickly how to bypass standard detection rules, which is why we see more incursions with long dwell times as they sneak in under the proverbial wire. So, you not only need all your data, you need it to be readily available over time. For IT, data analytics over time enables efficient, predictive operations.

Situational awareness: It's about context and risk

Situational awareness is core to secure operations. Situational awareness and context enable us to determine the appropriate action to take if, say, the low tire pressure light starts blinking on our car dashboard.

1. How dangerous is the situation — what is the risk? Are we driving on the freeway, at risk of an accident, or is the car parked in our driveway?
2. What is the potential impact if this turns out to be a serious tire issue? If it's a slow leak, then how much time do we have before we need to investigate?
3. How confident are we that this is actually a problem? Have we had other tire issues lately indicating that this is part of a bigger problem? Or does this light blink frequently for no reason, so it's probably a false alarm?

Similarly, when an alert or detection rule fires due to a potential cyber threat or performance issue, situational awareness is critical to confirm something is wrong, and to determine the appropriate response, such as immediately shutting down assets or accounts. You need more information: The right context to take appropriate action at the right time. What happened? On which device(s)? What user(s)? Where and when? Has it happened before? What other alerts might be related?

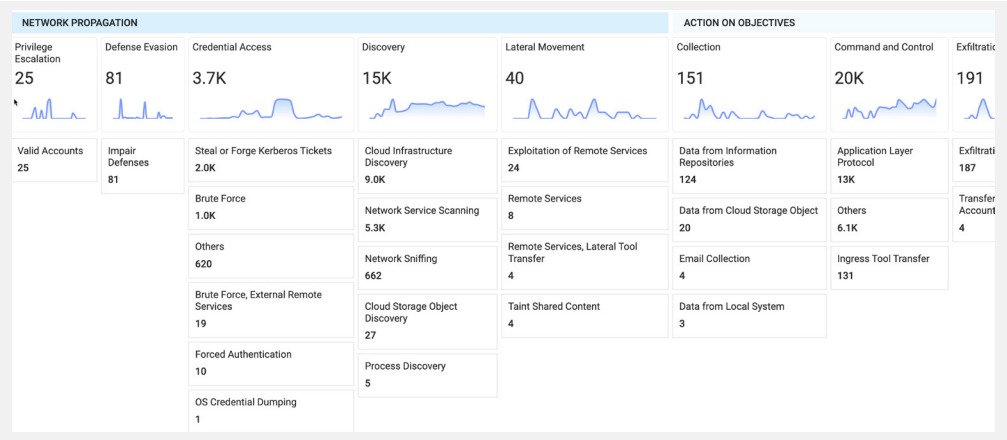
Just as with the blinking tire pressure light example, you need to know: What is the risk to the business, potential impact on data and assets, and confidence that something is actually wrong. Answers to these, along with related information that provides critical context, then guide what actions that analysts should take — or can kick off an automated response.

This is where alignment of business risk comes into play: Secure operations accounts for the business value of data and assets to running the business, as well as the organization's risk tolerance.

Operational frameworks to optimize operations

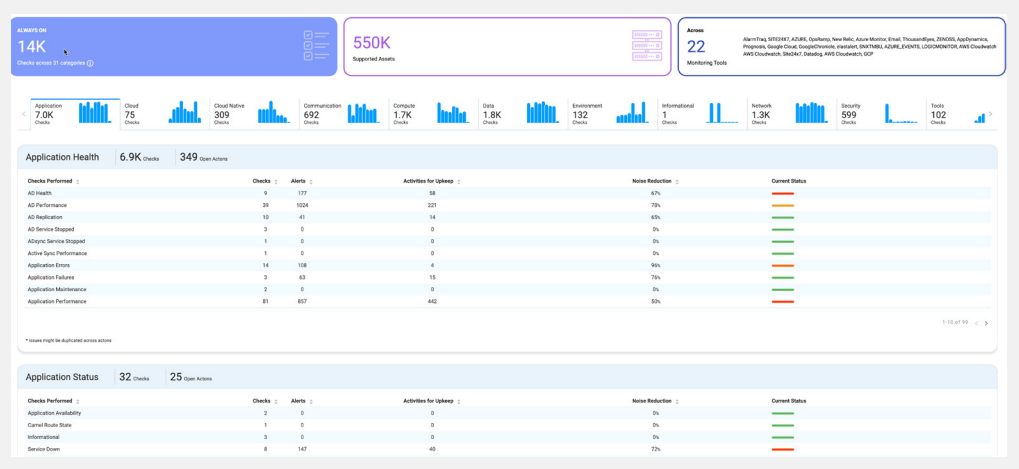
Operational frameworks help teams understand when a situation warrants attention and what actions to take to maximize availability and minimize risk to the business. The best frameworks provide ways for teams to diagnose, communicate about, and resolve issues faster with a common ontology and language. They also enable you to automate more.

On the security side, these frameworks include MITRE ATT&CK and the cyber kill chain. Your data mapped to these frameworks reveals: What tactics and techniques are in play? Where should we focus to stop threat actors before an incursion?



On the digital operations side, Resolution Intelligence Cloud from Netenrich ingests ops data from all sources (on prem, cloud, network, etc.), then normalizes it to standard categories so you can see exactly what is going on across the environment(s). It reveals health, availability, performance, and monitoring of applications, devices, as well as connectivity, automation, and more.

Learn more in this eBook:
[How to Implement MITRE's World-class SOC Strategies with Resoultion Intelligence Cloud]



How do you implement secure operations?

You want to stop working in silos, duplicating efforts, struggling with coverage gaps, managing too many tools that aren't helping. You're ready to take a more proactive approach to security and digital ops. You need a cost-effective, fast way to bring in all your data. Where do you start? With one or more of the following:

- Leverage all your security and operations data (cloud, on prem, all of it) and make sense of it so you spot risks and trends early.
- Focus ops and security teams on what matters most to the business and respond faster.
- Automate whatever you can to boost effectiveness.
- Enable ops and security teams to work collaboratively from a common operating picture, with observability across both security and ops data.
- Enable people and tools to work together.

"All of the above" is what Resolution Intelligence Cloud enables. And you don't have to do it all at once with a painful rip and replace. Resolution Intelligence Cloud works with the detection, SOAR, and ITSM tools you have and can streamline your tech stacks.

Moving toward secure operations — starting now

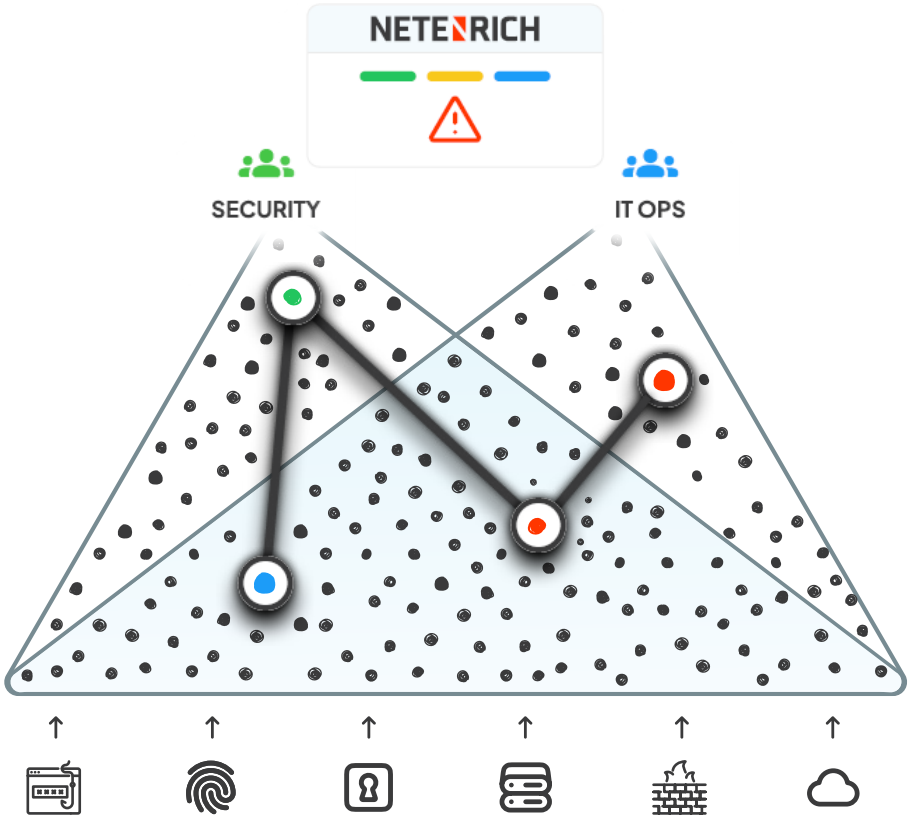
There are many reasons for making the shift to secure operations, improving cyber resiliency and reducing business risk at scale:

1. Be more efficient and effective at detecting and preventing issues before they put your business at risk.
2. Gain the context and intelligence necessary to manage cyber risk.
3. Operationalize cyber risk management aligned to your business. Strengthen cyber resiliency.

It's a journey that you can start now.

Focusing on the business benefits and outcomes can go a long way toward bringing siloed teams together around a shared goal. Most IT and security teams are stretched thin — and stressed — mired in floods of alerts and tickets, with more responsibilities and tasks than they can handle. Secure operations with Resolution Intelligence Cloud enables teams to run with more resiliency and effectiveness — and a lot less stress.

At Netenrich, we're here to help with Resolution Intelligence Cloud, our cloud-native platform for secure operations. Get a demo, or book a use-case session with one of our experts to chart your course of action.



NETENRICH

www.netenrich.com

Netenrich boosts the effectiveness of organizations' security and digital operations so they can avoid disruption and manage risk. Its Resolution Intelligence Cloud is a native cloud data analytics platform for enterprises and service providers that need highly scalable, multitenant secure incident and event management (SIEM) with advanced analytics to provide actionable insights to act on. The platform leverages Google Chronicle as its fast, scalable security data lake. Resolution Intelligence Cloud transforms security and operations data into intelligence that organizations can act on before critical issues occur. More than 3,000 customers and managed services providers rely on Netenrich to deliver secure operations at scale and speed.