NETENRICH

HOW TO IMPLEMENT MITRE'S WORLD-CLASS SOC STRATEGIES WITH RESOLUTION INTELLIGENCE CLOUD

TABLE OF CONTENTS

As threat actors continue to innovate and the threat landscape continues to grow, enterprises cannot afford to rely on traditional, reactive solutions. Instead, they must consider taking a completely new approach to managing security and IT operations.

This e-book is intended to help chief information security officers (CISOs) and security operations center (SOC) teams understand how they can optimize and transform operations by using the Netenrich Resolution Intelligence Cloud™ platform to implement MITRE's recommended world-class SOC strategies.

This new and innovative data analytics approach helps teams to:

- Gain situational awareness across all security and operational data to improve threat detection and response while also improving availability and performance.
- Reduce noise and resolve incidents faster with extensive context and cross-functional collaboration.
- Proactively find and fix vulnerabilities and dramatically increase SOC effectiveness.

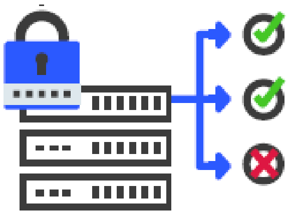
Executive Summary

In March 2022, MITRE, a U.S.-based tech foundation for the public good, released **11 Strategies of a World-class Cybersecurity Operations Center** — an amped-up practical guide to enhancing digital defenses and improving SOC efficacy. It dives deep into how the right approaches can help organizations — of any size or IT/SOC maturity level — overcome a multitude of challenges to optimize operations.

In this e-book, we deconstruct those strategies and show how Netenrich's Resolution Intelligence Cloud maps to each to improve an organization's security and risk posture while also shifting ops forward with data analytics and predictive and adaptive approach.

Data in Context Is Everything to Security Operations

Three decades ago, NBC's Tom Brokaw said, "The more you know about an impending disaster, the more likely you are to do something about it." He wasn't wrong. We would add that the more you know, the more likely you are to be able to respond quickly and appropriately, balancing risk, time, and cost.



MITRE Strategy 1: Know what you are protecting and why

THE CHALLENGE: *Cybersecurity operations exist to support their organizations' missions, so they need context for the data that they see and the action they take.*

The accelerated pace of business transformation is generating an explosion of infrastructure assets, applications, and data. We're talking volumes of data that analysts must investigate to discover the most critical issues.

Too much information (TMI) is rarely a good thing — and many organizations struggle with having to limit the security data they ingest and store because it's too expensive. On the flip side, if they don't have all the relevant data — from assets, apps, and users — they'll create blind spots and increase vulnerability. But what if you could turn TMI into a good thing, leveraging all your security data for threat forecasting and early detection without breaking the budget? MITRE suggests that SOC teams start by developing better situational awareness[1] across five key areas:

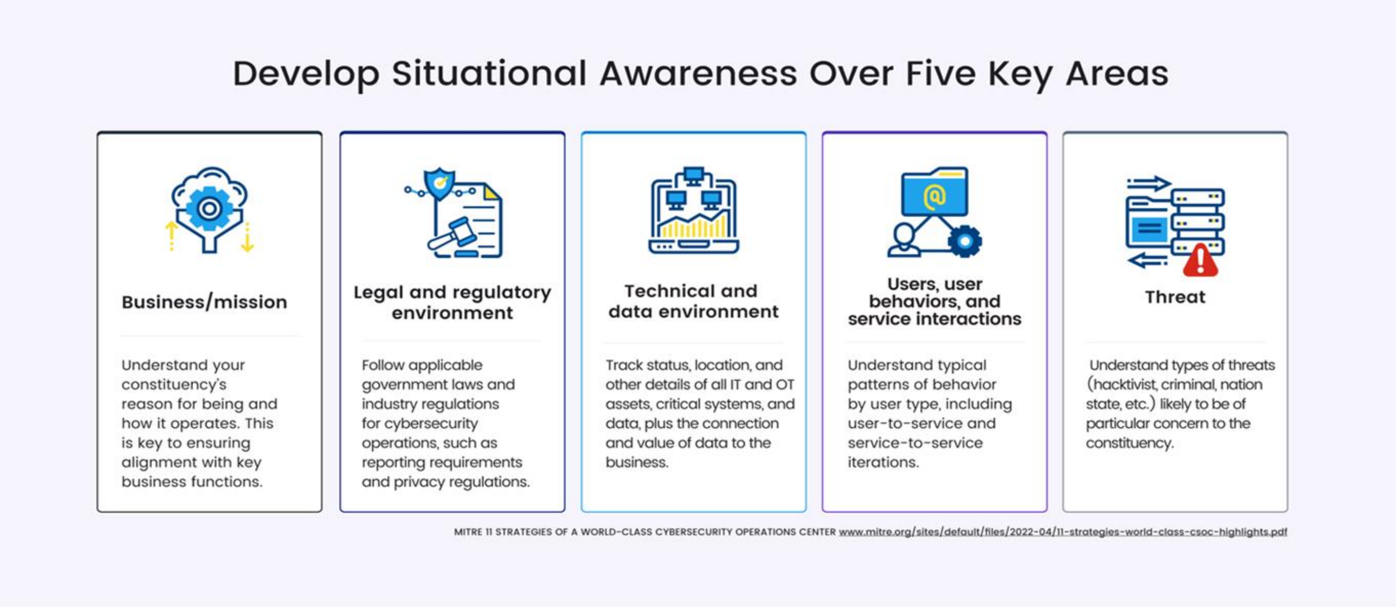
- The business/mission (what to prioritize).
- Legal and regulatory environment (what you have to do).
- Technical and data environment (what you are monitoring).
- Users, user behaviors, and service interactions (also what you are monitoring).
- Threat (what adversaries are trying to do).

How do you develop situational awareness? With contextualized data.

Data silos create blind spots and impede situational awareness

Data is meaningless without context. Sure, your car's blinking *check engine* light indicates there's an "issue," but it's not enough to tell you whether this is an emergency that may cause your car to explode or just a heads up that it's time for scheduled maintenance. In short, it's not a complete picture. The complete picture requires more data, leading to situational awareness.

In the cyber world, situational awareness is the basis for sound decision-making and improving outcomes. To establish it across security and digital operations, you need a common operational picture[2] — which is exactly what Resolution Intelligence Cloud provides.



Develop Situational Awareness Over Five Key Areas

Business/mission

Understand your constituency's reason for being and how it operates. This is key to ensuring alignment with key business functions.

Legal and regulatory environment

Follow applicable government laws and industry regulations for cybersecurity operations, such as reporting requirements and privacy regulations.

Technical and data environment

Track status, location, and other details of all IT and OT assets, critical systems, and data, plus the connection and value of data to the business.

Users, user behaviors, and service interactions

Understand typical patterns of behavior by user type, including user-to-service and service-to-service iterations.

Threat

Understand types of threats (hacktivist, criminal, nation state, etc.) likely to be of particular concern to the constituency.

MITRE 11 STRATEGIES OF A WORLD-CLASS CYBERSECURITY OPERATIONS CENTER www.mitre.org/sites/default/files/2022-04/11-strategies-world-class-csoc-highlights.pdf

If you can't pinpoint a problem, how can you resolve it?

Resolution Intelligence Cloud applies real-time data analytics, context, and correlation to identify patterns and anomalies across hybrid infrastructures that predefined rules can't. After all, to define a rule, you have to be aware of the threat.

Resolution Intelligence Cloud turns an abundance of security and digital operations data into actionable intelligence — a clear, contextualized picture and advanced risk scoring — that allows SOC teams to determine which situations are incidents, prioritize them, and make faster, better informed security decisions in collaboration with other key stakeholders.

This picture is not static and can change quickly. Resolution Intelligence Cloud's machine learning capabilities constantly improve detection and automated responses over time to prevent or mitigate risks to mission-critical services — which vary by organization. As MITRE mentions, a legal firm may prioritize data confidentiality while a financial services company prioritizes data integrity, and a power company prioritizes availability and, literally, keeping the lights on.

Not all data is created equal

Data is a good thing, but it takes a lot of good data to get to the right data.

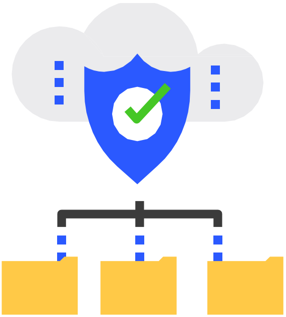
Historically, data ingestion, storage, and anything close to real-time analysis has been expensive. But without adequate data, not only from all security and operations telemetry but also over time, SOCs cannot determine when and if something is going wrong and how critical that something wrong may be.

The good news is that today, data intake doesn't have to be limited or expensive. Leveraging Google Chronicle as its security data lake, Resolution Intelligence Cloud ingests and unifies security telemetry — across endpoints, applications, hybrid infrastructure, and user behavior — at petabyte scale, but at low cost, and provides "hot data" for a year. Telemetry that's enriched with threat feeds, OSINT data, CVE information, and expert insights to provide even further granularity and context for investigation and triage. Thus, CISOs no longer have to choose between budgetary constraints and adequate security. They can scale to capture all the data they need.

What's more, in a single console, the platform gives SOC teams actionable insights called ActOns. These highly contextualized, pre-incident tickets give analysts the information they need — including a business risk score based on likelihood, impact, and confidence — to drive informed decisions and actions, whether that's proactively strengthening the organization's security posture or hastening response and remediation across an expanding attack surface.

Give SOCs the Authority to Be a Top Business Priority

MITRE states that while SOCs perform critical work protecting their organizations, they are often underfunded and undervalued. SOCs should align with, protect, and support the business — and Resolution Intelligence Cloud can help.



MITRE Strategy 2: Give SOC the authority to do its job.

CHALLENGE*: SOCs are on the front line in defending a constituency's cyber assets. Where they are in the organizational structure, and how they are funded, directly impacts their ability to fulfill their mission.*

Every day, SOCs are responsible for protecting an increasingly complex organizational infrastructure against sophisticated threat actors whose job is to find gaps, exploit vulnerabilities, breach networks, gain footholds, establish persistence, and steal, encrypt, or destroy valuable assets. That's a lot to tackle without adequate funding and, more importantly, without sufficient authority to determine cyber-protection priorities.

But getting authority and funding requires that SOCs show value to the powers that control budgets. So how can a SOC leader assess value of something not happening and quantify it in currency?

No news is good news — until it's not

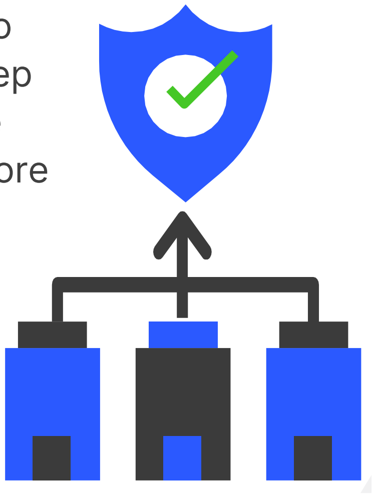
The SecurityWeek article "**Quantifying ROI in Cybersecurity Spend**" shows how it's not easy to place a value on cybersecurity, especially when nothing bad happens. Too often, executives see SOCs as cost centers, where a bunch of people seem to be sitting around not doing much. They begin to wonder what they are paying for, and CISOs begin to feel like fuse boxes, just waiting to get fired.

Put another way, CISOs are like goalies. People tend to remember goals scored, rather than goals saved. Inevitably, something will go wrong, a threat actor will score big, and fingers will point at CISOs, whether they had the latitude to make the save or not. It can seem like a no-win situation, and it's one of the reasons MITRE wrote this book: **The current system is broken.**

In its 2022 *Cyberthreat Defense Report*, CyberEdge reported an upward trend of organizations allocating more of their IT budgets to information security, year over year, from 2018 and 2020 — from 12.1% to 12.8%.[3] Over the next two years and despite no slowdown in emerging threats, that number leveled off to 12.7%. CyberEdge suggested a gating factor: Not enough skilled people to deploy and run new technologies.

A dearth of skilled people has several implications. Salaries go up as businesses compete to hire skilled staff. SOCs can't keep buying more tools and assume their current staff can manage them effectively. The more stressed the SOC staff are, the more likely they are to quit.

No one wants to spend money on security if they believe it could be better spent on business innovation and revenue-generating services. But also, there's no game without defense — and with defenders in short supply, it's a delicate balancing act.



Awareness is life!

In his novel *Anna Karenina*, Tolstoy posits that every unhappy family is unhappy in its own way. The same could be said about unhappy SOCs. Every SOC has its own story, its unique challenges, but also, what seems to be a rather strange, universal barrier to success: A lack of authority to do its job. Ubiquitous or not, it's a big enough problem for MITRE to call it out.

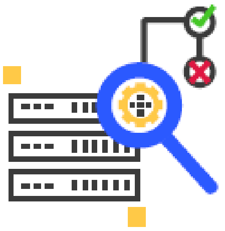
Now, imagine a world where SOCs and CISOs could more easily demonstrate their value. Where they could show executives the threats they are thwarting, the business disruption they are preventing, the dollars in lost business they are saving. Where they could provide the situational awareness needed to command authority and show that they are taking proactive steps to protect the business.

Authority and trust go a long way in creating and maintaining a happier and more effective team. Competent people like to make decisions, and good managers must give them the support and flexibility to do so.

With Resolution Intelligence Cloud, they can. The platform ingests all of an organization's security and operations data and empowers SOCs and their digital ops colleagues with a common operational picture that allows them — and in turn, their business leaders — to have situational awareness. With this complete picture, they can identify risky behaviors and pre-incident situations, rank them by business risk, and correlate extensive context to take fast, decisive action to minimize any potential damage.

They can show their leadership the damage they've avoided — goals saved — which enables them to start quantifying value and assess business risk that the SOC addresses. And they can up-level their current staff, making them over 80% more effective and a lot less stressed, so that SOC leaders can get out of the hiring craze.

A Prism of Data — Focused on Risk Management



As we dive into MITRE's third strategy, you'll see a pattern emerging: Secure operations require that everyone is working from the same data, aka a common operational picture.

MITRE Strategy 3: Build a SOC structure to match your organizational needs

CHALLENGE: *What's appropriate for one organization may not work for another; there are many models to build from.*

Cybersecurity is more than a technical problem, it’s an organizational problem. And while it’s not possible to have absolute protection in a connected world, you can lessen the odds and impact of cyberattacks by taking a risk-based, business-aligned approach to managing cybersecurity and building an effective SOC structure.

As per MITRE’s first strategy, organizations need to know what they are protecting and why. With that knowledge, they then need to dig deeper to understand where they are vulnerable — and the **MITRE ATT&CK® Framework** is a great resource for assessing risk.

A global knowledge base of cyber adversary behavior compiled into a taxonomy of tactics and techniques across the threat lifecycle, ATT&CK takes a threat actor’s point of view to help organizations understand how the bad guys conceive, prepare for, and execute attacks.

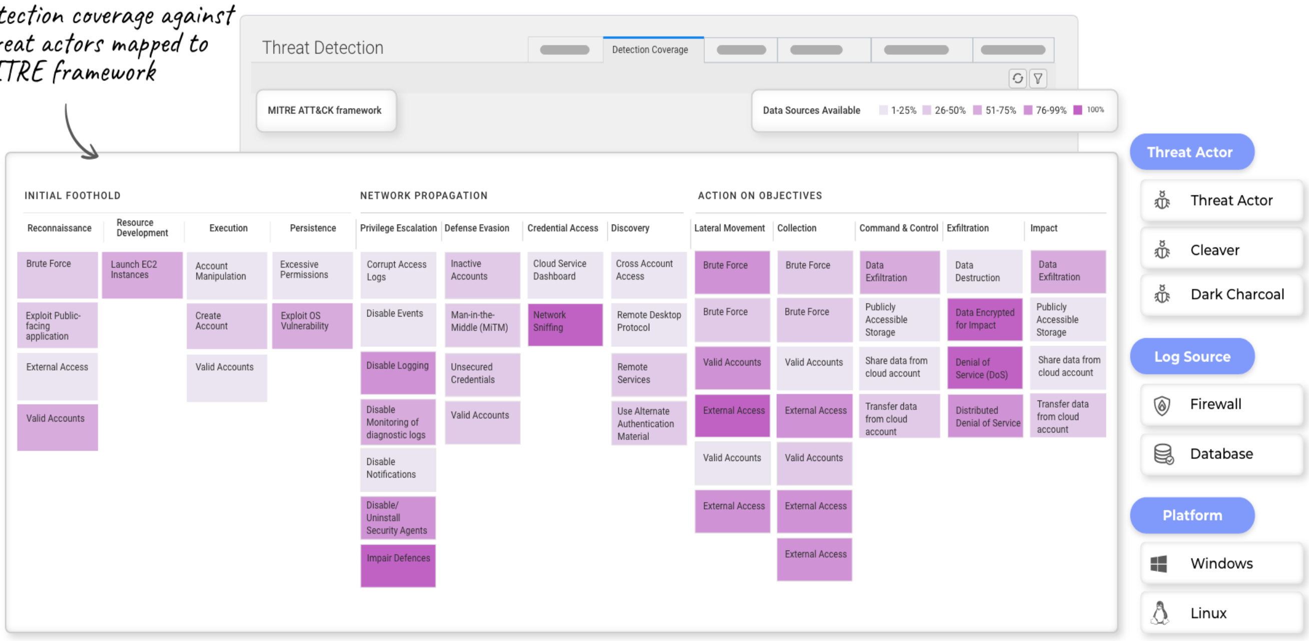
SOCs can use the ATT&CK taxonomy to understand the “footprint” of known, real-world attacks and identify where their organization may be vulnerable. Next, they can focus on minimizing the greatest risks in the most cost-effective manner to meet their business’ risk tolerance.

For example, by implementing a platform like Resolution Intelligence Cloud, they can:

- Leverage automation, machine learning, and artificial intelligence to reduce noise, raise fidelity, speed response, and increase productivity, pivoting away from the traditional 24/7 "alert monitoring" model to focus on high-priority issues and proactive threat hunting.
- Apply attack surface management (ASM) strategies and leverage threat research for more proactive identification and remediation of vulnerabilities on key assets.
- Detect patterns of risky behavior most relevant to your company, industry, and known exploits.
- Correlate events from multiple detection sources and use behavioral analytics not only to find and respond to threats more quickly, but also proactively shape and strengthen defenses.

- Gain the context to know if situations require action with ActOns. These highly contextualized, pre-incident tickets correlate detections, user and asset data, evidence, ATT&CK mapping, and graphs, reducing noise by 80% and saving analysts hours of research time. Prioritized by risk and impact to the business, ActOns let them — and by them, we mean all key stakeholders on a ticket — know where to focus their attention.

Detection coverage against threat actors mapped to MITRE framework



Threat Detection

Detection Coverage

MITRE ATT&CK framework

Data Sources Available ▫ 1-25% ▫ 26-50% ▫ 51-75% ▫ 76-99% ■ 100%

INITIAL FOOTHOLD				NETWORK PROPAGATION				ACTION ON OBJECTIVES				
Reconnaissance	Resource Development	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Brute Force	Launch EC2 Instances	Account Manipulation	Excessive Permissions	Corrupt Access Logs	Inactive Accounts	Cloud Service Dashboard	Cross Account Access	Brute Force	Brute Force	Data Exfiltration	Data Destruction	Data Exfiltration
Exploit Public-facing application		Create Account	Exploit OS Vulnerability	Disable Events	Man-in-the-Middle (MiTM)	Network Sniffing	Remote Desktop Protocol	Brute Force	Brute Force	Publicly Accessible Storage	Data Encrypted for Impact	Publicly Accessible Storage
External Access		Valid Accounts		Disable Logging	Unsecured Credentials		Remote Services	Valid Accounts	Valid Accounts	Share data from cloud account	Denial of Service (DoS)	Share data from cloud account
Valid Accounts				Disable Monitoring of diagnostic logs	Valid Accounts		Use Alternate Authentication Material	External Access	External Access	Transfer data from cloud account	Distributed Denial of Service	Transfer data from cloud account
				Disable Notifications				Valid Accounts	Valid Accounts			
				Disable/ Uninstall Security Agents				External Access	External Access			
				Impair Defences					External Access			

Threat Actor

Threat Actor

Cleaver

Dark Charcoal

Log Source

Firewall

Database

Platform

Windows

Linux

Building situational awareness by bridging silos

“You can’t fight in here. This is the war room!” said President Merkin Muffley.

Both iconic and ironic, the line from Dr. Strangelove is meant to amuse. But what if there were no fighting in war rooms? Like the virtual war rooms in Resolution Intelligence Cloud that you can initiate from the ActOn console. These war rooms streamline processes, eliminate redundant work, and most importantly, facilitate collaboration and faster decision-making across siloed departments. In these war rooms, everyone is on the same page, turning alert detections into actions with a focus on solving the most critical, confirmed issues first. In these war rooms, there’s no fighting — except against threat actors.

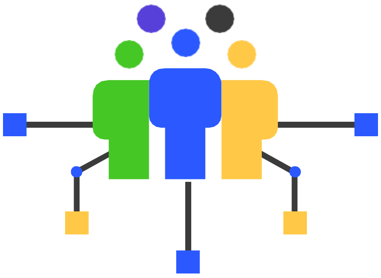
Here are some examples of what happens in Resolution Intelligence Cloud's ActOn war rooms:

- SOC experts chat with IT managers to shut down devices that are at risk. When another team member starts a shift, the handover is easy because conversations and actions are documented in one place.
- Service-provider security experts work directly with their customers, sharing insights and conferring on appropriate actions to take for swift resolution. They can review what happened — from ActOn to actions — to ensure there are no repeats.
- Converge people, process, and tools into cohesive and consolidated digital operations.

Building the right structure for a modern SOC may require re-imagining and breaking down traditional constructs. It's not about SecOps. It's not about ITOps. It's not about CloudOps. It's about secure operations across all ops, which requires enhanced transparency and better use of data — the more, the better — from across the entire organization for a common operational picture that helps make the business as secure and successful as possible.

Data Is the Key to Growing Your Staff the Right Way

MITRE Strategy 4 highlights the "people problem" in security these days. Let's take a look at the issue and ways to address it.



MITRE Strategy 4: Hire and grow quality staff

CHALLENGE: *People are the most important aspect of operating a world-class SOC. Ensuring you have qualified staff — through training and recruitment — is key.*

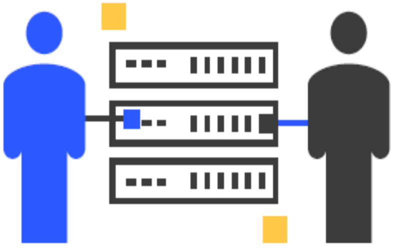
Time is the great equalizer. No one gets more than 24 hours in a day, but many could use more, including SOC analysts. As threats increase in sophistication and the attack surface expands, their jobs are becoming more and more challenging. The question is, what can help? Hint: It's not more tools.

Most companies have more than enough tools. The problem is not enough qualified experts to run them. While more tools provide more data, they also produce more noise, which has the knock-on effect of requiring someone to investigate every alert. Plus, each tool has to be configured, integrated, and managed in the stack. What a chore, and what a bore.

Talented, well-trained security analysts are in high demand but short supply — and those who understand the tools and your environments aren't easy to find. If you give them the tedious, stressful, time-consuming job of investigating every alert — which is ultimately, ineffective — you're going to lose them.

Humans and machines — together in perfect harmony

MITRE says hire and grow staff. Due to the skills shortage, you're better off developing existing talent than trying to hire a lot more staff — which isn't a sustainable business model anyway.



Another way to think about it is using a new approach that automates what is automatable, thus freeing staff from tedium and upleveling their skillset.

One that's not about more tools or more people but instead centers on making people more productive by leveraging the power of more data and using that data effectively and efficiently.

It may sound counter-intuitive at first. Why give SOC analysts more to wade through when they're already overwhelmed? But more data — in fact, the more, the better — provides more context, which drives faster, better decision-making.

The key is in leveraging a platform like Resolution Intelligence Cloud. It applies advanced analytics and machine learning across all security and operations data to enable machines to do what they do best — for example, sift through large volumes of data to find warning signs — and humans to do what they do best: get creative and solve the hard problems.

With Resolution Intelligence Cloud, organizations don't need to hire more experts or train junior staff to perform basic monitoring and triage tasks. Instead, they'll boost their current team's effectiveness and job satisfaction by using the platform to automate those basic tasks, identify pre-incident situations, see where to focus because the platform ranks ActOns by business risk, and correlate extensive content for proactive resolution.

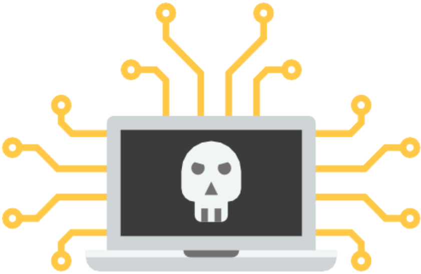
ActOns are like built-in experience for everyone. They provide all the information teams need in one place, sparing people the time and effort of investigating to gain situational awareness. ActOns distill data from a wide range of sources, much like Google Maps uses real-time data on traffic patterns, construction delays, speed traps, and more to update routes and offer the quickest, most fuel-efficient option.

In short, the platform makes time for teams to uncover and focus on more complex, covert threats. You know, those hard, mission-critical problems. It also frees time for them to learn new skills or train junior analysts on the skills required to become senior analysts. For hybrid operations, where personnel may be responsible for the ops gamut — NetOps, CloudOps, SecOps — there's an opportunity to improve security proficiency. Again, the objective is not eliminating jobs, but upleveling them.

Using Cyber Threat Intelligence in Context to Prevent and Withstand Threats

MITRE Strategy 5: Prioritize incident response

The fifth strategy in MITRE's book counsels organizations to prioritize incident response (IR) by defining response steps and escalation paths and codifying them in operating procedures and playbooks. Netenrich couldn't agree more.



One of the primary challenges of creating playbooks is that you need to start with effective operating procedures that you can turn into playbooks. That's where many organizations struggle.

SOAR technology helps coordinate, perform, and automate incident response. There are some excellent products out there for automating your playbooks, like Google's Chronicle SOAR (formerly Siemplify), which we've integrated with our Resolution Intelligence Cloud platform.

Resolution Intelligence Cloud provides extensive context — correlated alert, asset, user, and related data — to Chronicle SOAR, enabling smarter and faster resolution. However, since playbooks aren't our focus, let's jump to strategy 6 to discuss the key role cyber threat intelligence plays in response.

MITRE Strategy 6: Illuminate adversaries with cyber threat intelligence

CHALLENGE: *Finding malicious activity and other traces of adversaries can be challenging. SOCs need to be proactive and identify threats before they enter their constituency's environment.*

MITRE says, "Analysis and tailoring of CTI and establishing context enables the SOC to prioritize the actions of detection and prevention to conserve resources, honing the effectiveness of SOC operations."[4]

Once more, we agree, and we'd like to call out the importance of using context to prioritize actions.

Finding malicious activity and mapping threats against assets isn't easy, especially when assets are frequently coming on and offline, and when asset information isn't integrated with security data. Threat intel helps solve this problem by providing insight into the threat landscape and pointing to possible risks, vulnerabilities, and exposures. In other words, you can focus on warding off known threats and minimizing their damage.

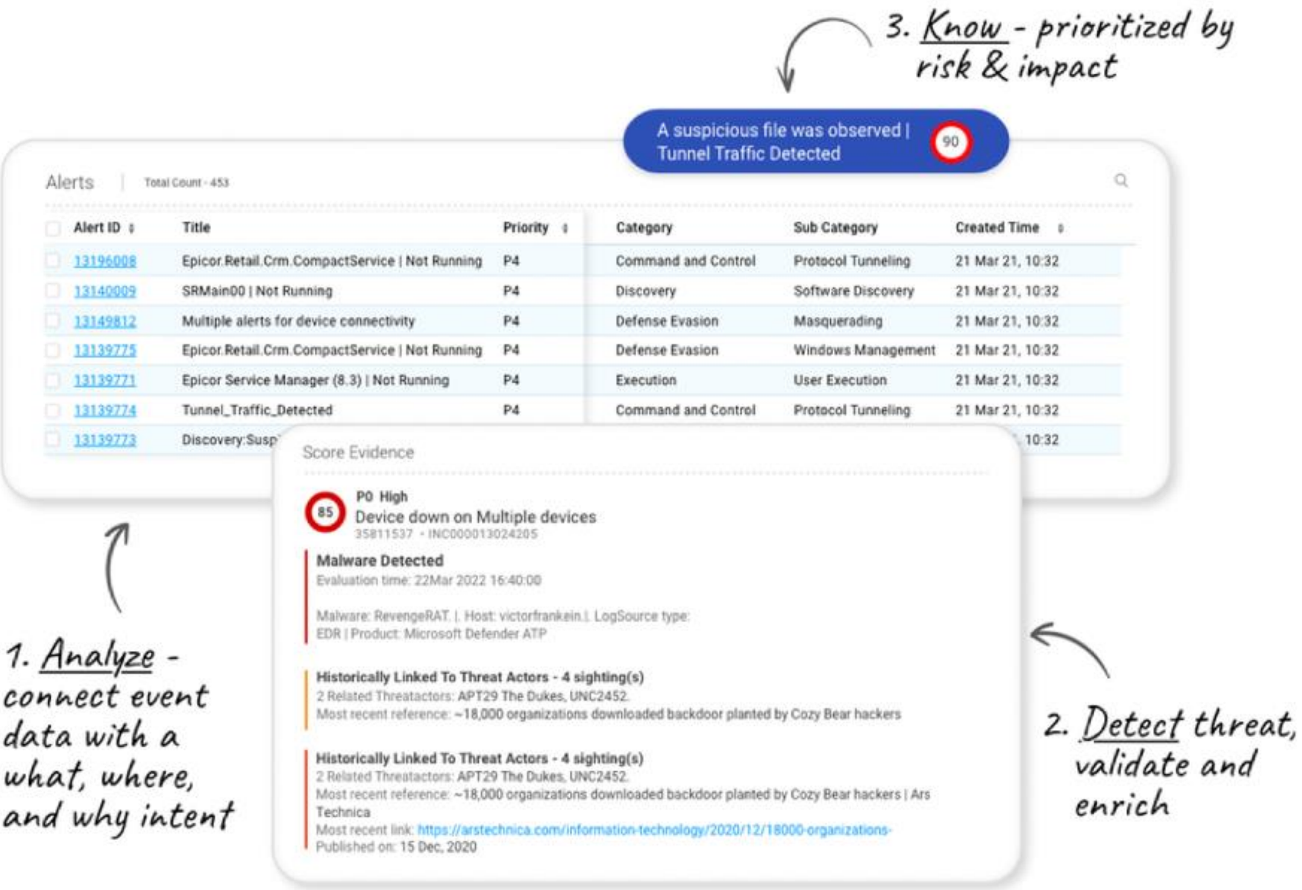
It's crucial — and extremely challenging — to determine whether a specific piece of intelligence applies to a situation or asset. For that, you need context that enables you to determine the risk the intelligence poses to your organization.

To "conserve resources, honing the effectiveness of SOC operations" as MITRE advises, you need to focus on the intelligence that poses the greatest risk. Which begs the question, how do you figure that out? The key questions you need to answer are:

1. Is this intelligence relevant to my organization, users, assets, etc.? Which ones and how important are they to the business?
2. What is the potential impact of the intel?
3. What is the likelihood of that impact happening?
4. What is my confidence in the intel?

Context gives you a greater understanding of threats in terms of the risks they pose, their potential impact, and the potential damage they could cause. Context helps organizations prioritize action and fine-tune investigations to find the root cause of urgent problems and plug holes faster.

But how do you make threat intel and context actionable?



3. Know - prioritized by risk & impact

A suspicious file was observed | Tunnel Traffic Detected 90

Alerts | Total Count - 453

Alert ID	Title	Priority	Category	Sub Category	Created Time
13196008	Epicor.Retail.Crm.CompactService | Not Running	P4	Command and Control	Protocol Tunneling	21 Mar 21, 10:32
13140009	SRMain00 | Not Running	P4	Discovery	Software Discovery	21 Mar 21, 10:32
13149812	Multiple alerts for device connectivity	P4	Defense Evasion	Masquerading	21 Mar 21, 10:32
13139775	Epicor.Retail.Crm.CompactService | Not Running	P4	Defense Evasion	Windows Management	21 Mar 21, 10:32
13139771	Epicor Service Manager (8.3) | Not Running	P4	Execution	User Execution	21 Mar 21, 10:32
13139774	Tunnel_Traffic_Detected	P4	Command and Control	Protocol Tunneling	21 Mar 21, 10:32
13139773	Discovery:Susp				10:32

Score Evidence

85 P0 High
Device down on Multiple devices
35811537 • INC000013024205

Malware Detected
Evaluation time: 22Mar 2022 16:40:00

Malware: RevengeRAT |. Host: victorfrankein.|. LogSource type: EDR | Product: Microsoft Defender ATP

Historically Linked To Threat Actors - 4 sighting(s)
2 Related Threatactors: APT29 The Dukes, UNC2452.
Most recent reference: ~18,000 organizations downloaded backdoor planted by Cozy Bear hackers

Historically Linked To Threat Actors - 4 sighting(s)
2 Related Threatactors: APT29 The Dukes, UNC2452.
Most recent reference: ~18,000 organizations downloaded backdoor planted by Cozy Bear hackers | Ars Technica
Most recent link: https://arstechnica.com/information-technology/2020/12/18000-organizations-
Published on: 15 Dec, 2020

1. Analyze - connect event data with a what, where, and why intent

2. Detect threat, validate and enrich

Resolution Intelligence makes intel and context actionable

Resolution Intelligence Cloud makes context actionable. Because our focus at Netenrich is secure operations — not just security or detection — the platform reveals the context you need to optimize SOC operations effectiveness.

Organizations can be much more effective if, for example, they know whether an attack is targeting a high-value business resource or a more isolated, non-critical asset. With Resolution Intelligence Cloud, they can automatically discover and tag assets according to business importance. What's more, they can map known threats against any asset to see where the organization may not have sufficient log coverage for early detection — even for a particular known threat.

Resolution Intelligence Cloud illustrates detection coverage so you can visualize external threat exposure and severity, mapping an organization's security posture to the MITRE ATT&CK framework. This "lay of the land" overview shows risky behaviors, threats, and pre-incident situations correlated with information on related events, assets, and users.

Using advanced data analytics and machine learning, the platform provides ActOns — curated, contextual data including threat intel and related alerts, assets, and user data — that let analysts know which situations require immediate attention and, just as importantly, which don't. They aid security analysts in effectively responding to intel and suspicious activity before damage or disruption can occur.

Focus on adversaries instead of incidents

You can only prevent what you know. For example, data from solutions like endpoint detection and response solutions (EDRs) and SOARs lets organizations see what has occurred. But as MITRE says, the right threat intelligence in the right context gives organizations a proactive edge.

Resolution Intelligence Cloud not only helps you take *proactive* measures in response to threat intel, but as threats evolve, it also helps you predict future adversary behavior and prepare to withstand potential attacks.

So you have the context and framework you need to take advantage of threat intelligence to illuminate adversaries — and stop them.

The Goldilocks Principle of Security Data Collection: How to Get It Just Right

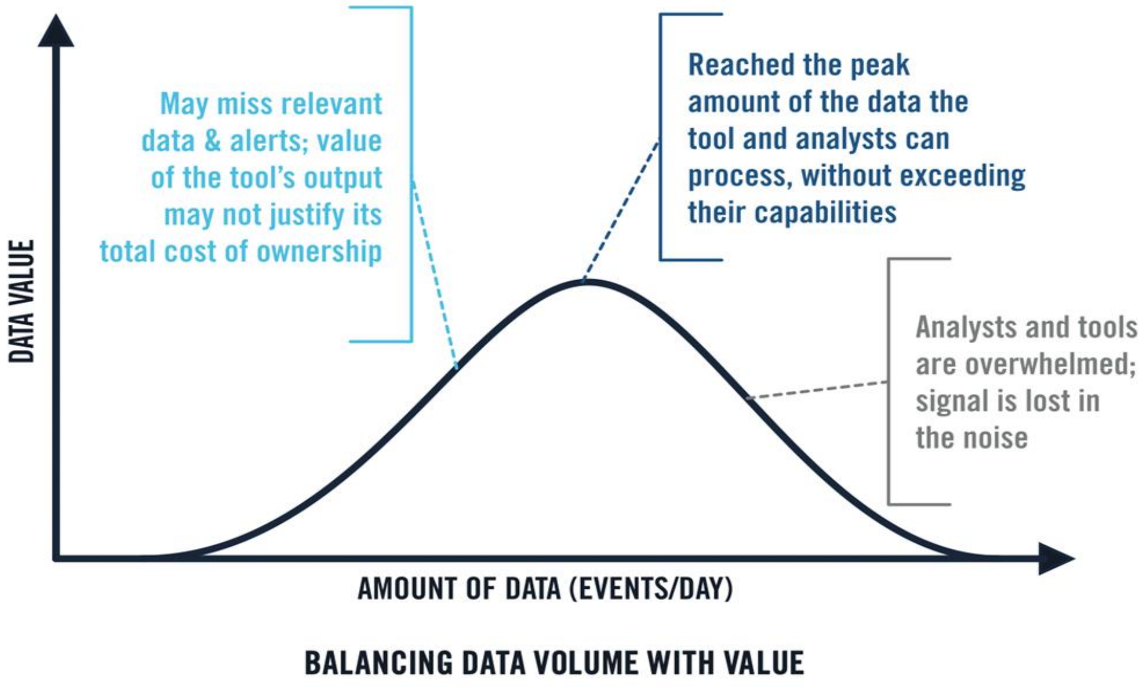
While strategy 6 focuses on cyber threat intelligence data, strategy 7 discusses log and sensor data — in other words, the largest chunk of data a SOC collects. At its core, this strategy is about balance. First through totality; and then, specificity.

MITRE Strategy 7: Select and collect the right data

Challenge: Most constituencies generate more digital data than a SOC can possibly process and act upon.

When it comes to data selection and collection, MITRE states it's important to "consider the trade-offs of too little data (and therefore, not having the relevant information available) and too much data (such that tools and analysts become overwhelmed)."

Ugh. Trade-offs.



Finding the right balance. Source: 11 Strategies of a World-class Cybersecurity Operations Center, MITRE, 2022.

Most companies are either collecting too much or too little data — the right balance seemingly as elusive as a perfect porridge. But what if, like Goldilocks, you could get data collection just right? No trade-offs, no concessions. Just the right data at the right time in the right context. It is possible.

Not all data sources are created equal

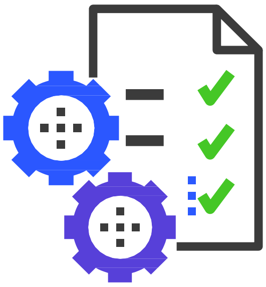
MITRE also says, "For both detecting and confirming intrusions, data and instrumentation from endpoints are generally considered more informative and provide more clarity than data from network traffic." In short, you have to carefully consider data sources.

Regardless of whether you're an enterprise, MSSP, or MDR services provider, if you're collecting network telemetry, for example, from a network detection and response (NDR) solution, an EDR platform, or a web application firewall (WAF), you need to collect the right information. For example, if you're a financial institution, you need to know that the tools you have in place are providing adequate coverage and protection against adversaries targeting your specific industry.

But given the fast-evolving sophistication and relentlessness of threat actors, you don't necessarily know in advance what data is most relevant. Clearly, if you filter the data you collect and/or don't store it for enough time, you risk important data gaps that disable you from detecting patterns in that data. Trust us, threat actors love to hide in these data gaps.

Why limit the security data you collect? Typically, it's because of budget and technology. When your costs soar as you ingest more data and store it for longer, you have to impose limits. Plus, there's the issue of managing and making sense of the data. Many tools don't help. They're notoriously slow for large queries required for threat hunting and threat detection. Or the data isn't real time, so you're late to the party before you even get started. And most teams don't have the necessary data science skills.

What if you could easily and cost-effectively collect all your data so you knew you had the right data over sufficient time? And what if you had the technology to make sense of all that data—without having to hire a team of security experts with PhDs in data science?



Unlimited but cost-effective data collection

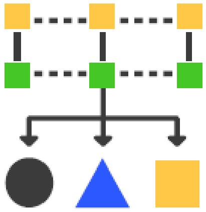
With Resolution Intelligence Cloud, you can have your data and eat it, too — that is, you can make sense of it to accomplish your security goals. Ingest any amount of data you need from any source. Store it hot for a year. That means storing data from across all security and digital operations without penalty — either in terms of ingestion expense or analyst overload.

Get sub-second response on petabytes and run data analytics out-of-the-box without hiring data scientists. Benefit from a no-code machine learning toolkit. The platform enables your existing team to do even more because they have the actionable insights, evidence, and information they need at their fingertips.

With the correct data volume and right tooling, you can start to see the big picture — especially if you leverage Resolution Intelligence Cloud. The platform uses 13 machine learning algorithms to connect the dots and display an organization's detection coverage on a heat map, identify risky behaviors, and discover situations — before they become incidents — prioritized by risk to the business based on impact, likelihood, and confidence. So you and your team know where to focus to keep digital operations secure.

Again, it's all about balance. Too much data = too hot. Too little data = too cold. Resolution Intelligence Cloud = just right.

A Single Pane of Glass Provides a Clear View for Security Operations



Previous MITRE strategies stressed the importance of collecting the right data — both threat intelligence (external) and log/sensor data (internal) — from the right tools.

While MITRE concedes that every tool and piece of data can add value, it also states that integration is crucial to deriving the most value. Thus, SOCs should look to bring all tools and data together into a single architecture that supports analyst workflow.

MITRE Strategy 8: Leverage tools to support analyst workflow

CHALLENGE: *SOCs bring vast amounts of disparate data together into an information architecture. Analysts need to be able to quickly evaluate the data, turn the data into information, and use the information to fulfill their mission.*

There is no one-size-fits-all workflow management solution. Depending on size and maturity, an organization may turn to a SOAR solution, a SIEM platform, a combination of a SOAR and a SIEM, or a mix of other threat detection and case management tools.

MITRE discusses at length the abilities, benefits, and shortcomings of several tools, but also states that "reducing the number of panes of glass and providing integration between them is the best strategy with an emphasis on automation and integration for repeated tasks, escalation, and incident handling."

The goal is to provide analysts with information they can use immediately and effectively, without distracting or exhausting them, without requiring extensive training — and without busting budgets.

SOAR vs. SIEM vs. other tools: What pane of glass is the best pane of glass?

SOARs can integrate with a variety of disparate systems to collect threat data and automate repeatable processes. SIEMs can be used for threat detection and hunting, incident analysis, workflow and escalation, configuration monitoring, and more. Both are used as aggregation points for different tools and platforms.

So, why not choose one of these as the single pane of glass? To begin, some traditional SIEMs have failed to deliver on their promises to increase visibility, enable detection of security events, and support incident response. They don't ingest all the data you need in a cost-effective, actionable, or timely way. Moreover, as MITRE points out, "Some SOCs struggle to realize the value proposition of SIEM, in large part due to their complexity, as effective correlation rule writing and upkeep can be resource consuming."

For SOARS, it's much the same story. Though they can integrate with other tools, it's not easy to do so. Integration requires technical expertise to implement and manage. Plus, SOARs orchestrate response. They don't detect threats or determine where the greatest security risks to the business are.
Bottom line, SOARs and SIEMs require a deft, often cost-prohibitive touch to reap maximum benefits.

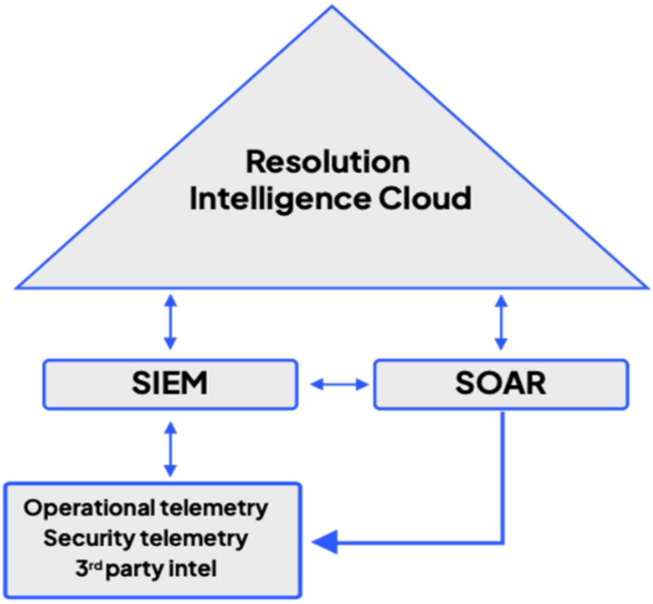
From a single pane of glass comes a common operational picture

Despite shortcomings of certain solutions, the notion of an aggregation point remains important — because perspective and visibility matter, visibility across all digital operations. And if fewer panes are better, wouldn't that single pane of glass across security and digital operations still be the best option?

As illustrated below, Resolution Intelligence Cloud sits at the apex of aggregation points — not only gluing everything together, but also sifting through, correlating, and contextualizing all telemetry data, at petabyte scale and Google speed. Resolution Intelligence Cloud dramatically reduces alert noise, presenting actionable insight and evidence based on real-time analytics of both security and operations data as well as asset and user data.

With it, SOCs gain a complete operational picture and thus, the situational awareness needed to identify true threats and drive the right action based on business risk.

Using the platform, SOC teams can leverage the unique capabilities and strengths of each security tool without needing to continually pivot between tools. They can directly dig deeper into alerts to investigate further and as necessary, establish war rooms, where they can instantly collaborate (or escalate) with key stakeholders — including digital operations and business stakeholders — to decide the best course of action (incident handling) for high-priority alerts.



Bonus! Resolution Intelligence Cloud stores petabytes of data for a long time

Most security tools offer neither petabyte scale nor long-term telemetry retention — and most that do charge you for all that data and availability. But to find threats, SOCs need scale, data over time, and speed — especially since the average time to identify and contain a data breach is 277 days.[5] (To put that into perspective, the average gestation period for a human is 266 days.)

Threats are growing and changing:
Constant, more sophisticate, more costly

277 days
Average time to respond

82%
of breaches are cloud based

169 days
Average time to detect with AI and automation investments

- Data problem: velocity & volume
- Soaring costs and risks
- Cannot hire enough trained people

$9.48m

Average cost of breach (US)

Sources:
(1) Check Point Research, Nov. 2022,
(2) The Cost of a Data Breach Report, 2023, Ponemon Institute and IBM

Historical hot data allows them to retrace an attacker's steps to understand exactly what happened with an incident. For instance, how attackers gained access to the network, where they went, and what they may have exfiltrated, damaged, or deleted. If stored telemetry data is limited, SOCs may never learn exactly how an incident started — or worse, may miss threats or incidents altogether, especially those with long dwell times. Either way, insufficient data limits their ability to forecast threats and prevent future incidents.

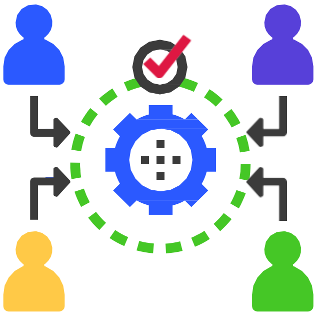
Resolution Intelligence Cloud ingests and analyses petabytes of data at speed, uses machine learning and behavioral analytics to find potential incidents and actual incidents — ActOns — so SOC analysts know where to focus. Plus, it automates level-1 and level-2 tasks.

Resolution Cloud Intelligence puts MITRE's "best strategy" into action by:

- Getting SOCs to one single pane of glass.
- Providing integration between technologies.
- Storing all your telemetry, hot, for a year without penalty.
- Identifying what matters most and reducing alert noise so analysts know where to focus.
- Automating level-1 and level-2 tasks.

In short, the platform provides analysts with information they can use immediately and effectively, without distracting or exhausting them, without requiring extensive training — and without busting budgets.

How to Improve Cross-functional Collaboration Between the SOC and IT



As MITRE points out in strategy 9, cross-functional communication is key to a SOC's success.

To support workflow processes, tools must integrate, and SOC teams must communicate and collaborate — not only among themselves, but also with the entire organization. Sounds simple enough, but it's surprisingly difficult to do effectively. Any failure to communicate can mean a failure to adequately secure the business.

MITRE Strategy 9: Communicate clearly, collaborate often, share generously

CHALLENGE: *No matter how well-funded or well-staffed a SOC is, SOC teams can never know everything about the cyber threats and vulnerabilities the organization faces. Collaboration — both internal and external — can provide valuable insight.*

Collaboration across functional areas may seem obvious, but traditionally, SOCs and IT departments have worked separately from one another. While SOCs focused on detecting, investigating, and responding to *threats*, IT focused on meeting the daily operational needs of the *business*. And rarely the twain did meet ... but it is critical that they do, now more than ever.

As stated in MITRE's first strategy, security analysts must know what they are protecting and why. By understanding their organization's mission and how the organization works to achieve it, they can better understand which assets and data are most critical to the business.

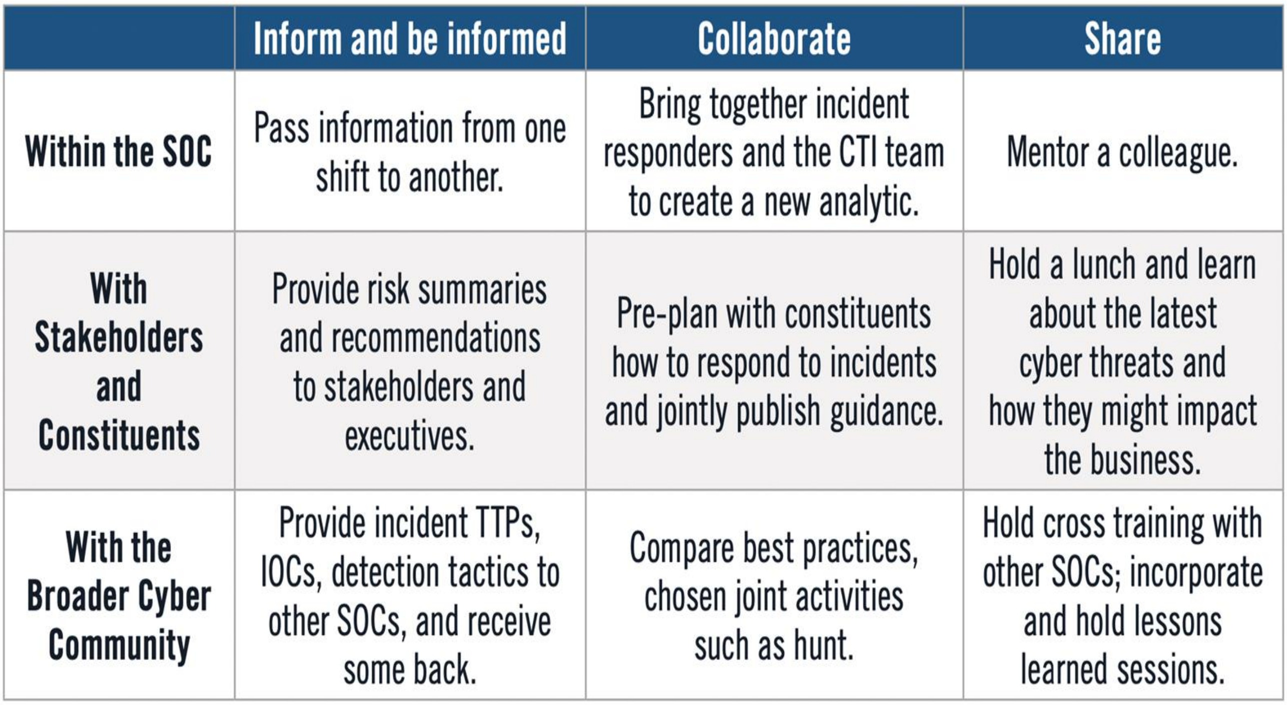
And how does this happen? By working across functions, collaborating with the IT operations team and other relevant parties to develop situational awareness to better coordinate actions and base decisions on what the business is telling them.

A single pane of glass to manage cybersecurity

Machines can automate certain tasks, but we need humans to solve the tough problems, to account for subtleties, situations, and business drivers. Another reason to focus on collaboration: If one mind is great, think about the power of brainstorming across departments.

With Resolution Intelligence Cloud, SOC and IT teams can collaborate within a single pane of glass to manage cybersecurity as a business risk and reduce exposure to harm.

EXAMPLES OF COMMUNICATING, COLLABORATING, AND SHARING WITH DIFFERENT GROUPS



	Inform and be informed	Collaborate	Share
Within the SOC	Pass information from one shift to another.	Bring together incident responders and the CTI team to create a new analytic.	Mentor a colleague.
With Stakeholders and Constituents	Provide risk summaries and recommendations to stakeholders and executives.	Pre-plan with constituents how to respond to incidents and jointly publish guidance.	Hold a lunch and learn about the latest cyber threats and how they might impact the business.
With the Broader Cyber Community	Provide incident TTPs, IOCs, detection tactics to other SOCs, and receive some back.	Compare best practices, chosen joint activities such as hunt.	Hold cross training with other SOCs; incorporate and hold lessons learned sessions.

- **Within the SOC.** The Resolution Intelligence Cloud platform promotes and supports communication with ActOns. Again, these are a correlated set of events, user data, and asset data that contains contextual information needed to determine that there is an incident and/or resolve one or more related incidents.

  The platform's war rooms enable secure collaboration among colleagues at any time to resolve ActOns. This makes it easy to bring together incident responders and the cyber threat intelligence team to share analytics and other information, even across shifts.

- **With stakeholders and constituents.** Resolution Intelligence Cloud dashboards can provide good data for stakeholders and executives, for example, identifying areas of vulnerability as assets go on and offline that can be proactively addressed.
- **With the broader cyber community.** Resolution Intelligence Cloud includes Netenrich's first-source and third-party curated threat intelligence. Additionally, Netenrich provides Threat Hunting Services tailored to customers' needs.

Remember, there's no fighting in war rooms

Security analysts can instantly create a war room from the ActOn console. Here, they can pull in the right experts and stakeholders — other SOC analysts, constituents from across the business, heads of business units, and/or third parties — to share insights and discuss appropriate actions for a swift resolution to the most critical, confirmed issues. For example, SOC teams and IT managers may need to collaborate to weigh the pros and cons of shutting down at-risk devices, then document what actions they take.

Moreover, if a breach occurs, the stakeholder teams can also invite individuals from legal, human resources, whatever business unit may be invested in the investigation and outcomes.

All in all, this shared situational awareness is good for security and good for the business.

Resolution Intelligence Cloud: Where people, tools, and processes converge

Resolution Intelligence Cloud is valuable for employee shift changes. When a team member starts his or her shift, Resolution Intelligence Cloud makes the handover easy with all case notes, conversations, and actions documented in one place. Incoming analysts can quickly get the lay of the land and know what to address first. At the same time, parting analysts can rest easy, no longer needing to worry if they've forgotten to share some vital piece of information.

In short, it's a seamless, stress-free transfer of information — on a need-to-know basis.

Amp up Security: MITRE's SOC Strategies Go to 11. But Can We Go Higher?

MITRE Strategy 10: Measure performance to improve performance

It's important to set a baseline of where resources spend their time and energy — and what results they achieve. Resolution Intelligence Cloud can help with this by providing visibility — the complete operational picture across security and operations — and the ability to prioritize incidents based on risk to the business (identifying and separating the mundane from the urgent). With that baseline established, organizations can then move to improve SOC and IT interoperability and functionality.

MITRE Strategy 11: Turn up the volume by expanding SOC functionality

CHALLENGE: *Cyber adversaries are continually evolving, and technology changes rapidly. SOCs need to keep pace.*

MITRE suggests that once incident response is mature, SOCs should enhance their programs with threat hunting, red teaming, deception, malware analysis, forensics, and tabletop exercises. Any of these can improve the likelihood of finding sophisticated adversaries.

We would add that there are already other, more advanced technologies to consider because they provide:

- More data in real time, over time, avoiding the risk of filtering out signals that turn out to be important when combined with other signals.
- More analytics and machine learning to identify patterns from disparate data sources over time, beyond what detection rules may miss.
- More automation to relieve alert fatigue and up-level analyst skill sets.
- More effectiveness, enabling analysts to move beyond a reactive, whack-a-mole approach to closing tickets and instead, focus on proactively avoiding vulnerabilities, predicting potential threats, and identifying where to focus first to minimize damage when incidents occur.

Resolution Intelligence Cloud does all of the above, today

Using first-source and third-party curated threat intelligence, the platform crawls the web and weaves together indicators of compromise (IoCs) associated with new threats. If it detects a high rate of similar IoCs, it searches for real-time and historical context — note, it's important to be able to store data for an extended period — to determine if there's been a breach. By taking this proactive step, SOCs can start to get ahead of threats, mitigating malicious compromises before they can cause damage.

And getting ahead is really what strategy 11 is all about. To beat the bad guys, you need to innovate, go beyond traditional constructs, rethink how to run both security and IT, and continuously adapt to best manage risk and optimize overall operations.

Resolution Intelligence Cloud makes noise by lessening noise

Resolution Intelligence Cloud is not just another technology platform, but a new way to run security and IT operations at scale and speed. Purpose-built to enable operational resilience, it not only improves threat detection and response but also availability and performance.

In short, Resolution Intelligence Cloud is a strategy in and of itself that helps SOCs implement and amp nearly all of MITRE's recommendations and ultimately, transform and optimize both security and IT operations to deliver better business results.

About Netenrich

Netenrich makes data the solution, not the problem. With Resolution Intelligence Cloud™, our secure analytics operations platform, we turn complex big data into actionable intelligence so enterprises can expose and manage security risk to reduce business impact. The platform leverages a cybersecurity mesh architecture (CSMA) to converge security and digital operations. Its data engineering, multitenant, and automation (AI, ML) capabilities improve current security systems, for more accurate threat management and response. More than 3,000 global customers rely on Netenrich to increase operations efficacy while scaling to meet the needs of the business.

[1] **Situational awareness**: The perception of environmental elements and events with respect to time or space, the comprehension of their meaning, and the projection of their future status.

[2] Common operational picture (COP): A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. Source: **Joint Publication [JP] 3-0**.

[3] "**2022 Cyberthreat Defense Report**," CyberEdge

[4] "**11 Strategies of a World-class Cybersecurity Operations Center**," MITRE.

[5] "**Cost of a Data Breach Report 2023**," Ponemon Institute & IBM.