NETENRICH

Resolution Intelligence for Cyber Situational Awareness

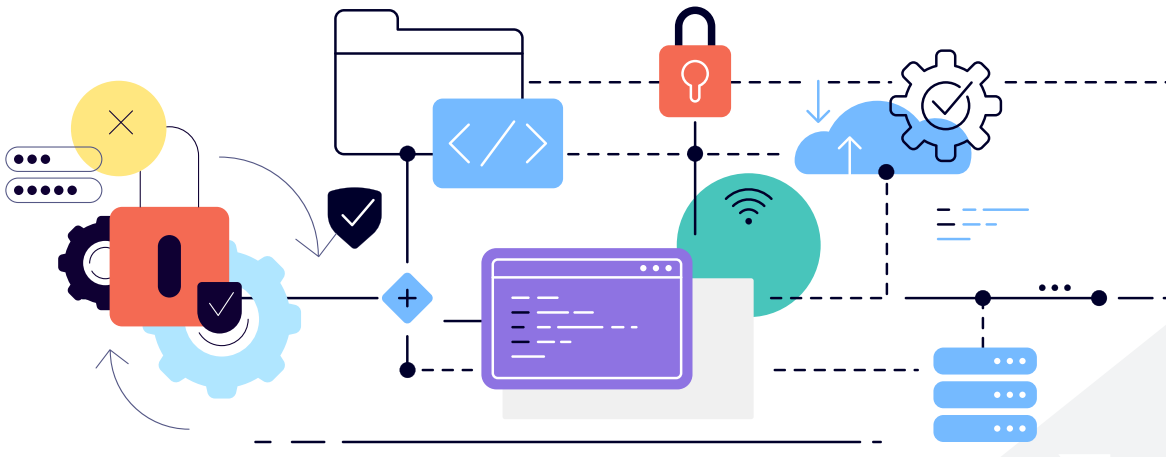
Align risk with operations to protect what matters

How do you improve resilience across an ever-changing threat landscape? Keeping security operations (SecOps) aligned to risk gives your business a lasting advantage over ransomware, malware, and other devastating cyberattacks. Netenrich Resolution Intelligence creates ongoing situational awareness based on potential impact so you can strengthen resilience while reducing complexity.

We operationalize risk management to deliver actionable insight that helps ensure availability, improve response, and maximize return on cybersecurity investments (ROI). Predictive analytics and actionable context help resolve customer issues quickly while keeping SecOps aligned to risk as your threat landscape changes.

Highlights

- Safeguard uptime
- Extend Mean Time to Compromise (MTTC)
- Improve readiness, response, resilience
- Keep SecOps aligned to business risk
- Always know what matters

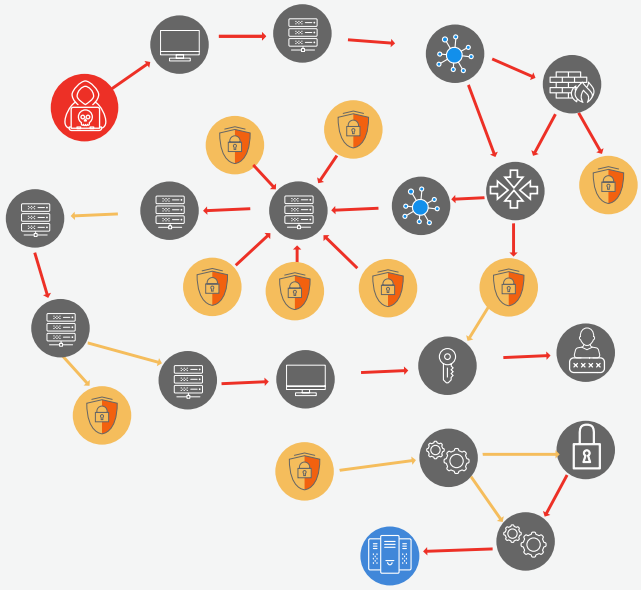


Insight to action in a fraction of the time

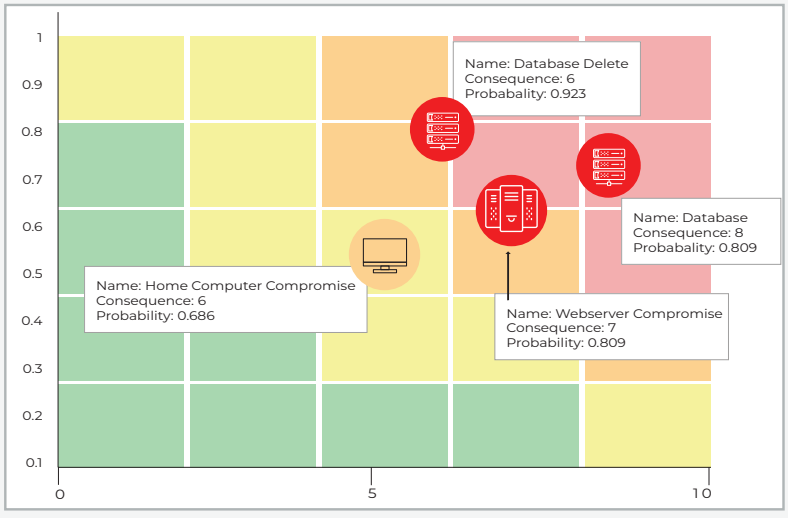
The Netenrich Resolution Intelligence Platform leverages machine learning (ML) and 13+ years' ops expertise to drive awareness when or even before you need it. Our platform takes in and enhances data from multiple sources to illustrate fast-changing dynamics between your business assets, security controls, and the various techniques used by attackers to steal data and hijack operations.

Our ongoing process combines:

- Asset management
- Threat and vulnerability intelligence
- External attack surface management (ASM)
- Threat modeling
- Adversary emulation



Advanced threat modeling charts the various paths attackers can take to compromise assets, operations, and data.



Graphical heat maps show which assets are easiest to compromise so IT and security teams can prioritize mitigation and be more proactive.

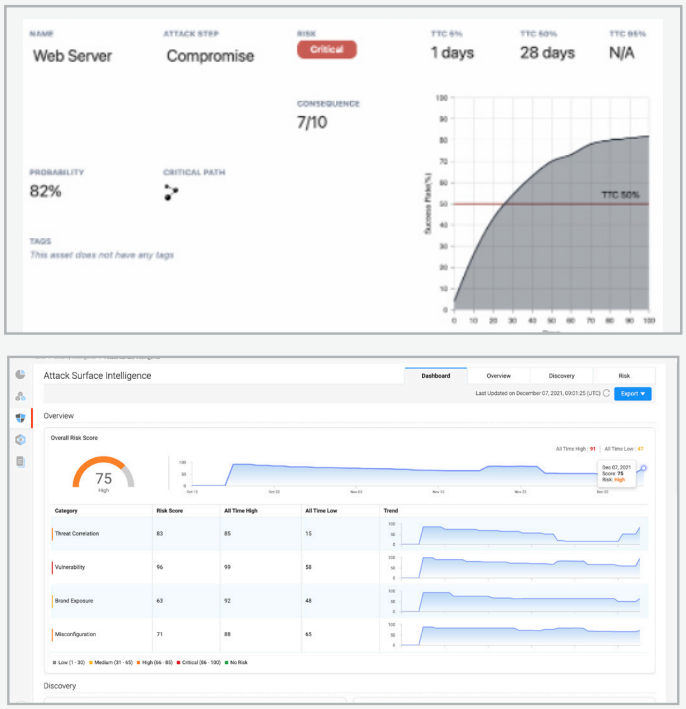
We quantify risk and deliver rich context, prioritization, and recommended steps to mitigate and avert risk. Prescriptive insights drive smarter, faster threat hunting, detection, response, and resolution out of the gate and over time.

The metric that matters: Quantify Mean Time to Compromise (MTTC)

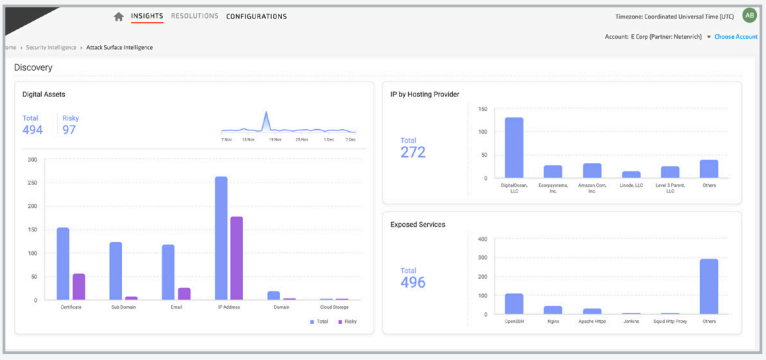
No security team can chase every alert or block every attack, but you should always know where to start. Resolution Intelligence for Situational Awareness quantifies risk based on likelihood of attack so your defenders can predict, intercept, and disrupt attacks based on impact.

The process starts with identifying your organization's crown-jewel assets — the data, systems, operations, and processes the business cannot run without — and modeling step-by-step pathways to reach them. The Netenrich solution measures the likelihood of attack and applies trending threat intelligence about your environment to calculate attackers' mean time to compromise (MTTC) — a meaningful "true north" metric by which to manage SecOps.

Emulating adversary behaviors shows defenders how — and how quickly — intruders might navigate from various entry points to steal data or shut down operations. Even with unprecedented insight into attack probability, your defenders need to know more, like what steps to take and when something changes. Netenrich reports and dashboards features recommendations on what to do — and do first — to disrupt malicious behaviors. Ongoing discovery detects events that automatically trigger additional threat modeling and adversary emulation.

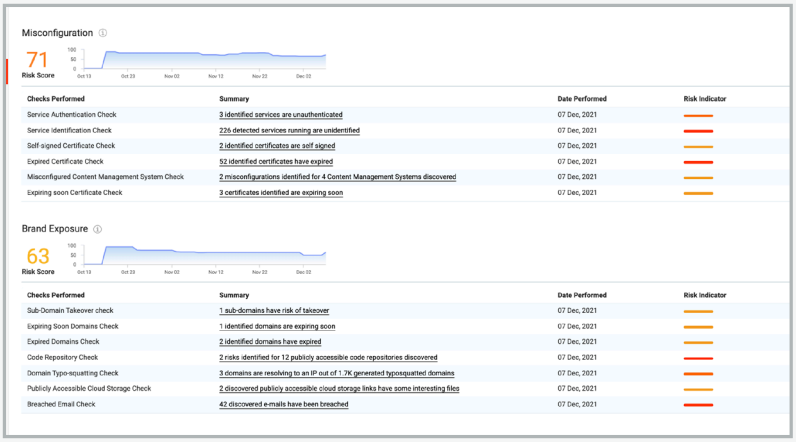


MTTC – Cybersec's new "True North."
The Resolution Intelligence dashboard shows the probability of a web server being compromised within one day is 6 percent. If the attack path goes unaddressed for 28 days, the probability of an attack succeeding rises to 50 percent.



Netenrich ASI automatically discovers risk from brand and domain exposure (sub-domains, web sites, certificates, content management systems, etc.) – unpatched vulnerabilities, and misconfigurations. Analysis and prioritization take place continuously with easy drill-down investigation into individual risks uncovered.

Compared with pen tests, red teams, and security ratings that provide only point-in-time perspective, Netenrich Attack Surface Intelligence (ASI) delivers ongoing coverage and assessment of brand risk from domains, cloud exposure, unpatched vulnerabilities, common misconfigurations, and shadow IT.



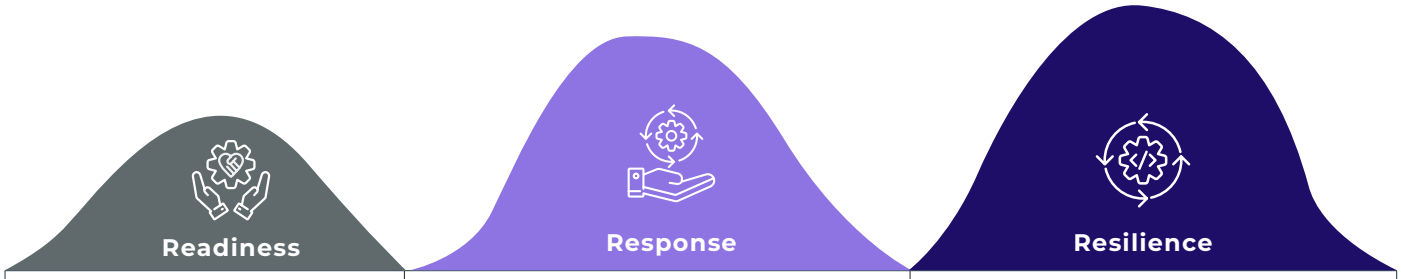
Staying aligned — less risk with less effort

To achieve resilience, SecOps and cyber risk must stay closely aligned. Netenrich Resolution Intelligence brings the right technology, automation, people, and processes in one powerful software-as-a-service (SaaS) platform to promote better collaboration across IT, security, and cloud operations. Sharing a common analytics platform helps to democratize security so all teams make better decisions to drive resolution in a fraction of the time.

Risk-aligned SecOps let you answer the question, “Are we safer today than we were yesterday?”

If, after aligning risk with operations, you need help with execution, Resolution Intelligence for Threat Detection can drive higher efficiencies within your security operations center (SOC). Our solutions span vulnerability management, detection and response, patching, and ASM on an ongoing basis.

Resolving for resilience



Readiness	Response	Resilience
What risks are we facing? Which matter most? Can we mitigate risk first?	How – and how fast – can we find, resolve, and recover from threats, attacks, and vulnerabilities in our environment?	What controls are we missing? What steps can we take to be better prepared?

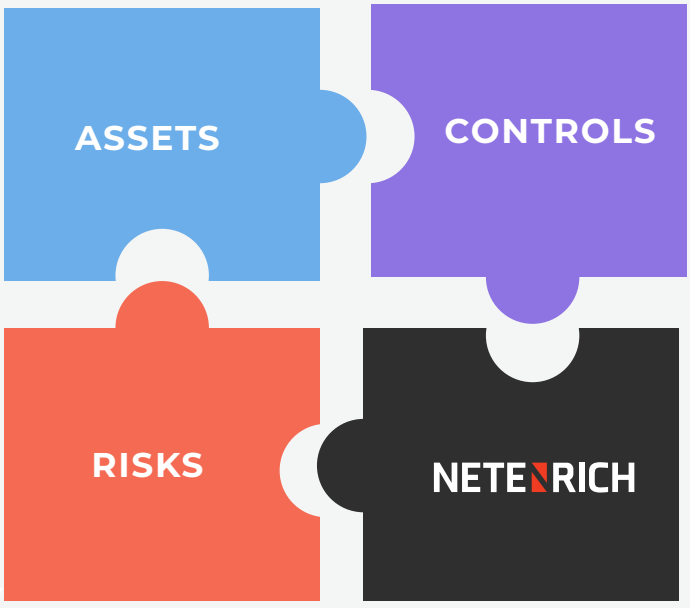
Netenrich Resolution Intelligence digital operations solutions add predictive analytics that help slow attacks and speed response based on risk and business impact.

Start today. Scale tomorrow.

Try Netenrich Resolution Intelligence for Situational Awareness to streamline SecOps, shrink your attack surface, and strengthen your cyber risk posture within weeks.

Flexible pricing tiers are based on the number of licenses, assets, and expert evaluations your environment requires.

Try it risk free.



The missing piece. Complete, ongoing cyber-situational awareness pulls together data, intelligence, and processes to document the relationship between your critical assets, internal and external risk, and IT and security controls.

Features and benefits

What you get	What you gain
Automated asset and privileged access discovery	• Visibility and control of users with privileged access to valuable assets • Discover shadow IT and deprecated assets • Eliminate manual asset discovery
High-value asset discovery	• Visibility and understanding of high-value assets • Risk-driven prioritization • Leverage controls in the attack path
Threat modeling and adversary emulation	• Map, rank, and shut down potential paths to attack high-value assets based on impact and likelihood • Align ops to mitigate the most critical threats first • Increase time to compromise assets • Threat intelligence contextualizes adversary emulation
Quantify Mean Time to Compromise (MTTC)	• Proactive risk mitigation • SecOps aligned around meaningful “north-star” metric • Contextualize and prioritize mitigation efforts
Regular/on-demand threat briefing calls	• Expert insight into how trending threats affect your business and critical assets
Attack Surface Intelligence (ASI)	• Discover external risk from publicly exposed or ty-po-squatted domains, compromised email credentials in breached databases, exposed credentials in public cose repositories and public cloud stage, unauthenticated services, content management systems (CMSs), expiring or abandoned certificates • Speed and prioritize threat hunting, detection and response efforts • Maintain Situational Awareness across dynamic threat landscape • Alert threat modelers to changes in the external attack surface