Attack Surface Intelligence (ASI)

See what threat actors see before they target your brand

You can't control everything on the public Internet, or even beyond your firewall, but you can still act first to protect your brand. Attack Surface Intelligence (ASI) from Netenrich gives your IT and Security teams actionable "outside-in" insight into your digital exposure so you can prevent breaches before adversaries strike.

ASI combines security expert and artificial intelligence (AI) to deliver complete Resolution Intelligence. First, machines perform external attack surface assessments to discover risks related to domains, IPs, digital brand exposure, certificates, misconfigurations, and vulnerabilities. Netenrich's intuitive, drill-down dashboard presents data for easy consumption by your team.

From there, Netenrich security analysts take the next critical steps to evaluate and prioritize risk, provide impact analysis, and recommend remediation strategies.

ASI complements "point in time" assessments such as pen testing and Red Team exercises for continuous coverage and mitigation of today's highly dynamic attack surface. Flexible "do it yourself" (DIY) offerings and high-touch concierge services bridge skills gaps to complement your company's IT and SecOps efforts.

Part of Netenrich's integrated Threat & Attack Surface Intelligence, ASI leverages our free Knowledge NOW (KNOW) Global Threat Intelligence to promote fast, innovative, proactive management of your ever-changing threat landscape.

HIGHLIGHTS

See what threat actors see—and act before they do

Experts prioritize risk and propose rapid mitigation

Continuous, always-on protection

Proactively reduce your digital attack surface

Instantly bridge SecOps skills gaps

How Attack Surface Intelligence Works

Discovery

With a single seed of data, such as an email address or domain name, our custom-built scanning engines explore billions of data points, pivoting through them to identify all associated digital assets and shadow IT related to your brand. These engines were designed to dig deep into areas that generally take significant time to research, associate and assess.

Assessment is continuous and automated from the first run. Easy to read dashboards group potential risks for rapid consumption and investigation by your team.

Analysis

Extensive automated evaluation follows discovery to correlate data, identify false positives, and perform risk-checks to assess your overall attack surface status. Evaluation includes validating data as legitimate, and correlating against KNOW global threat intelligence.

Analysis sets the stage for deep dives led by experts.

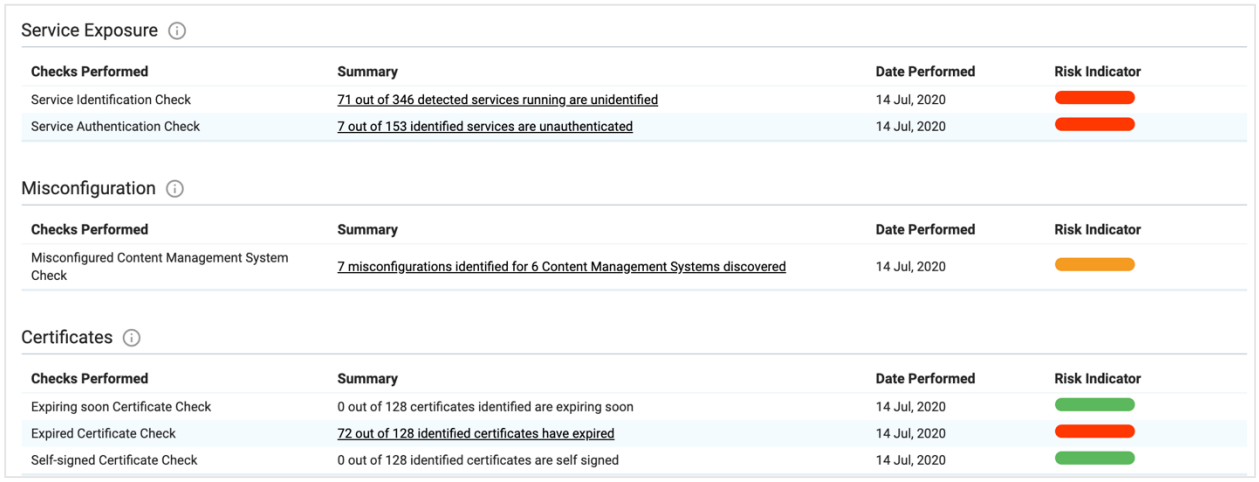
Prioritization

Machines automatically propose priorities for your team to mitigate. Netenrich cybersecurity analysts vet findings to validate the AI-driven recommendations.

Remediation

The final phase of Netenrich's high-touch ASI is analyst-led threat impact analysis and remediation recommendations. A team of experts reviews discoveries, prioritizes risks, and delivers actionable reports that contain affected assets, technical details, context, and technical remediation advice.

Dashboards Show Digital Brand Exposure at a Glance



Service Exposure

Checks Performed	Summary	Date Performed	Risk Indicator
Service Identification Check	71 out of 346 detected services running are unidentified	14 Jul, 2020	
Service Authentication Check	7 out of 153 identified services are unauthenticated	14 Jul, 2020	

Misconfiguration

Checks Performed	Summary	Date Performed	Risk Indicator
Misconfigured Content Management System Check	7 misconfigurations identified for 6 Content Management Systems discovered	14 Jul, 2020	

Certificates

Checks Performed	Summary	Date Performed	Risk Indicator
Expiring soon Certificate Check	0 out of 128 certificates identified are expiring soon	14 Jul, 2020	
Expired Certificate Check	72 out of 128 identified certificates have expired	14 Jul, 2020	
Self-signed Certificate Check	0 out of 128 identified certificates are self signed	14 Jul, 2020	

Figure 1. ASI displays your attack surface status with risk indicators per category. Issues are identified by technical checks performed for each category with three levels of risk indicated. Assessments can serve as a benchmark for audits of issues to demonstrate successful and continuous mitigation. In this example Service Exposure is putting the organization under high risk that needs immediate and ongoing attention.

Key Features

Attack surface scans include:

- Associated domain and sub-domain exposure
- Lookalike active domains
- Email addresses found in breached databases
- Open or misconfigured ports
- Expiring or abandoned certificates
- Vulnerability exposures
- Exposure from code repositories, public cloud storage
- Abandoned servers, sites, domains, pages
- Unauthenticated services
- Database exposures

Findings can be correlated with Knowledge NOW to determine whether you have a compromised infrastructure. With zero-effort onboarding, ASI features continuous coverage and can deliver significantly higher value versus point-in-time assessments such as pen testing, Red Team exercises, and other resource-intensive efforts that might be limited by pre-existing awareness of risk.

Example of domain assets discovered with quick indicators and risks

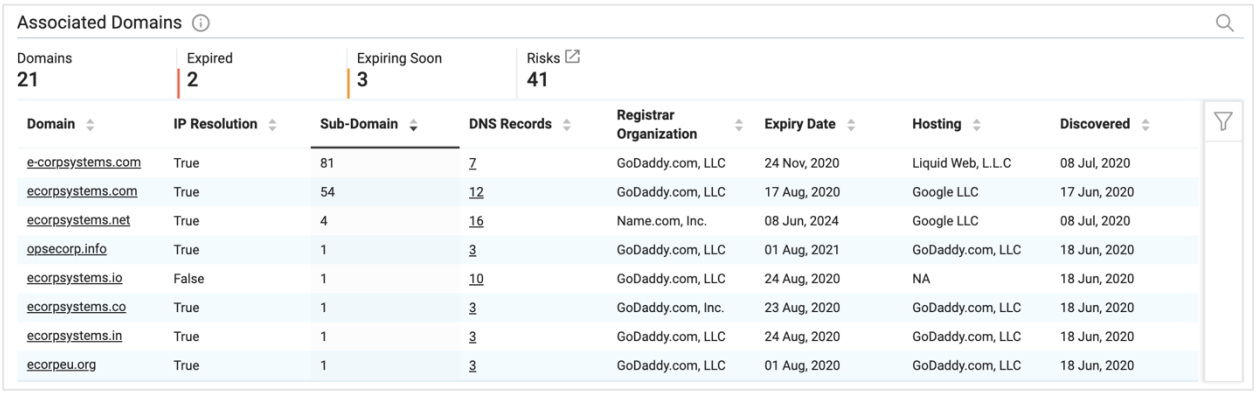


Figure 2. In this use case, a total of 21 domains were discovered as being associated with your brand. For each, discovered sub-domains, DNS records, registrar organization, expiration dates and hosting are shown, along with discovered dates. Each discovery features quick indicators such as how many domains have expired or are about to expire that might impact your organization's brand.

Benefits

- Know first, act faster than the “speed of bad”
- Proactively prevent attacks:
    - Ransomware
    - Command and control
    - DDoS
    - DNS hijacking
    - Brute force
    - Email-based attacks
    - Phishing
    - Typosquatting / lookalike attacks
- Stronger overall security posture
- Risk to brand reduced quickly
- Bridge skills shortages:
    - Intelligence updated automatically
    - Reduce cycles, alert fatigue

Flexible ASI Options

ASI Silver features continuous attack surface assessments and do-it-yourself (DIY) access to the ASI portal and dashboards.

ASI Gold adds monthly reports and four in-depth analyst consultations per year.

ASI Platinum includes automated attack surface scans, access to the ASI portal, monthly reports and in-depth analyst consultations, along with high-priority alert service.

About Netenrich

Netenrich delivers complete Resolution Intelligence to transform digital operations into smarter business outcomes. With 15+ years’ innovation across IT, NetOps and SecOps, Netenrich applies a dynamic mix of machine and expert intelligence through a wide range of products and SaaS-based offerings. More than 6,000 customers and organizations worldwide rely on Netenrich to help drive digital transformation, mitigate brand exposure, increase efficiencies, and bridge skills gaps. Netenrich is based in San Jose, California.