

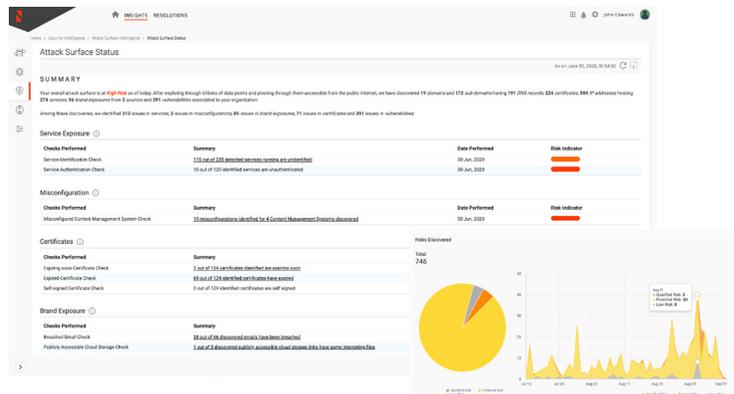
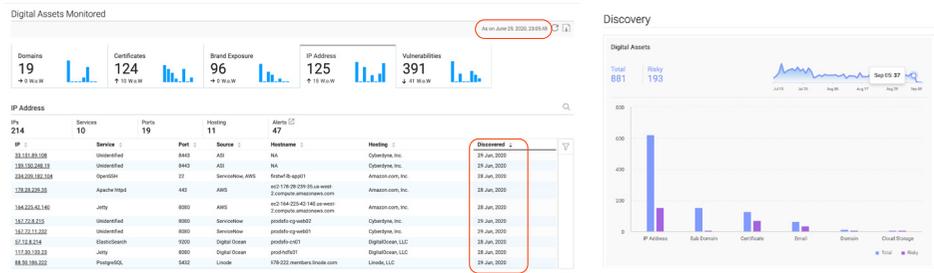
Attack Surface Intelligence

Protect your brand with continuous, outside-in views of your attack surface and fixes to the most critical risks in real-time.

Security beyond the perimeter is tricky for the most sophisticated SecOps teams with billions to spend and a workbench of several security products. ASI helps start-ups, mid-markets, and enterprises, too, demystify security beyond the perimeter with enterprise-grade outside-in security delivered via our human-machine outcomes platform.

Know first to act faster than the speed of bad.

Discover your entire digital footprint be it exposed cloud assets, storage, or domains and certificates, then correlate such public exposures to known risks and exploits that hackers are using right now to target you.



Fix the most critical risks now and let those that can wait, wait.

Prioritize risks basis the likelihood of attacks and the potential impact to your business. Get automated risk criticalities and drill down into categories of risks that have the highest scores. See vetted risk factors from our own global threat intel plus recommended fixes, all in real-time.

Speed up remediation with on-demand access to our cybersecurity experts.

Augment your IT and Security teams with our experts to speed up remediation. Our bench of cybersecurity experts with deep expertise in fixing risks beyond the perimeter help bridge skill gaps and address the most critical threats immediately while recommending steps for long-term protection.

Attack Surface Intelligence

Qualified

Open

Alert

35831

35598

35533

Potential malicious misuse of infrastructure using 91.219.237.36 (ed-cg-web01)

Historic Sandbox Sighting - 1 sighting(s)

Most recent reference Hybrid Analysis result for 'http://91.219.237.36/'

Most recent link: <https://www.hybrid-analysis.com/sample/1e51ed7278e7a12288a19e14792024c0d79530842e1a8034fb0b8d330?sep2ef5909bc8816d8db5>

Entities

IP: 91.219.237.36

Impact

An organizations domain or IP appearing in our threat intelligence indicates potential malicious activity originating from that IP asset. The compromised asset could then be used to attack both internal as well as external systems. Data residing on the system could also have been breached.

Description

Recommendation

1. Identify the indicator of compromise for which the association has been made
2. Identify other IPs and domains used by the same threat actor and verify if they belong to the organization. Identify if the affected asset has communicated with other associated indicators belonging to the same threat actor.
3. Identify malware samples used by the threat actors and search for them across the organization.
4. Clean the infected machines (if any). Deploy signatures for detecting the malware used by the threat actors.
5. Investigate the affected system for the root cause of the compromise and perform necessary remediations.

Your WordPress installation has put you at risk to brute force and denial of service attacks.

AFFECTED ENTRY

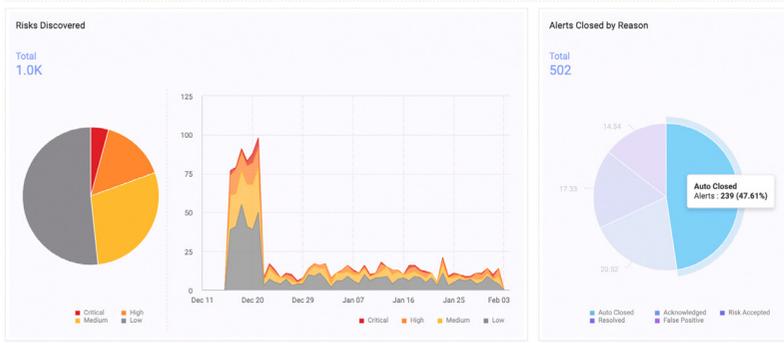
<https://wordpress.com/wordpress.php>

This entry has been reported to the WordPress community as a security issue. This indicates that the entry is a security issue. The entry is a security issue. The entry is a security issue.

Attackers can hijack your brand trust to infect your customers or take complete control of your site.

More Than 100,000 WordPress Sites Used for Distributed Denial of Service Attacks

report generated on 09 Mar 2020 | cyberhygiene systems | NetworkIQ, Inc.



Measurably reduce your attack surface over time.

Quickly see your overall risk score in the moment, then drill down into trends data for the last sixty days. Get rid of manual checks with **ASI's automatic updates** to your overall risk score by fixed and open risks within twenty-four hours of your acting on them.

I Why ASI from Netenrich



Zero-effort onboarding

Start with just your e-mail address to see your attack surface in near-real-time. Bring in your CMDB data, plug in your cloud instances, and ensure you are always ahead of hackers in watching---**and managing**---your attack surface.



Continuous, always-on coverage

ASI continuously and non-intrusively scans your attack surface to discover publicly exposed digital footprint, unlike point-in-time exercises like pen tests and Red Teams, and bubbles up those that need your immediate attention.



Proprietary threat intelligence

Leverage our global threat intelligence, **built ground up** to work natively with our security products and solutions like ASI and ISOC, to prioritize risks and stay ahead of threat actors in your industry and geography.



Collaborative risk mitigation

Fix risks right now with our bench of cybersec experts via chat, e-mail, and phone. Put effective controls in place and scale your Security Operations with our ISOC solution at a fraction of the cost to run your own.

To experience the advantage of continuous coverage, try Netenrich ASI free for 30 days.

You'll receive an attack surface scan, access to the intelligence portal and dashboards, and expert analyst insights to address your most critical risks first.

Sign up at <https://security.netenrich.com/attack-surface-intelligence-free-trial>