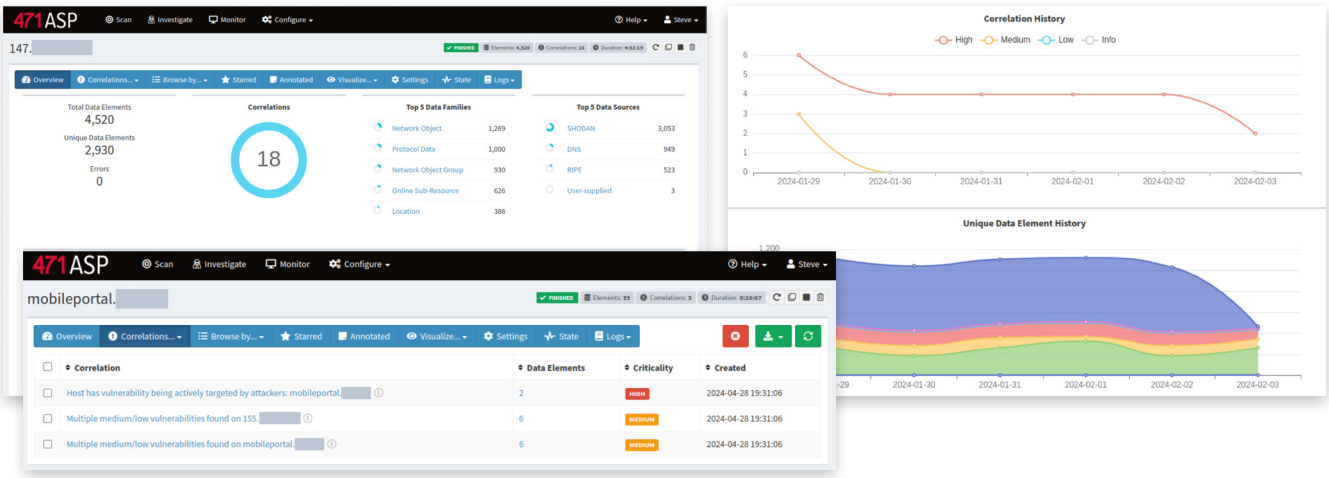
471 ATTACK SURFACE PROTECTION

Your external attack surface is continually evolving, which makes it challenging to maintain up-to-date visibility of every asset and new exposure. This lack of visibility increases the probability of unpatched vulnerabilities and misconfigured settings being exploited and resulting in data theft and ransomware attacks.

While threat actors are constantly probing attack surfaces for weaknesses, you need greater visibility of your constituent assets and their issues. 471 Attack Surface Protection answers this need, giving you the ability to discover your external-facing assets and awareness of emerging threats to your external attack surface and your digital supply chain.

Intel 471's timely cyber threat intelligence (CTI) from across the cyber underground, forums, open web sources and more is the key difference between 471 Attack Surface Protection and other ASM solutions. Intel 471's timely, accurate and relevant CTI helps your security team take a risk-based approach to digital threats. It assists you in prioritizing what exposures to remediate as new threats emerge, as well as manage unsanctioned internet-facing assets, including application servers, web hosts, non-production and production environments, exposed remote desktops, and cloud resources such as storage buckets and databases.



THE DIFFERENCE: TIMELY, ACCURATE, RELEVANT CTI DATA

Intel 471 intelligence — Know when exploits for exposures (CVEs) affecting your external assets are being sought, researched or traded in underground or public forums, and what malware families are communicating with your IP addresses and domains by leveraging Intel 471 Vulnerability Intelligence and Malware Intelligence capabilities. 471 Attack Surface Protection also integrates with over 200 OSINT sources for publicly available threat intelligence.

Continuous scans — Conduct continuous monitoring and alerting for new exposures and threats in your digital footprint. Regular, automated and repeated scanning of your attack surface provides ongoing monitoring and immediate alerting to any changes or new vulnerabilities and other issues or data exposures identified.

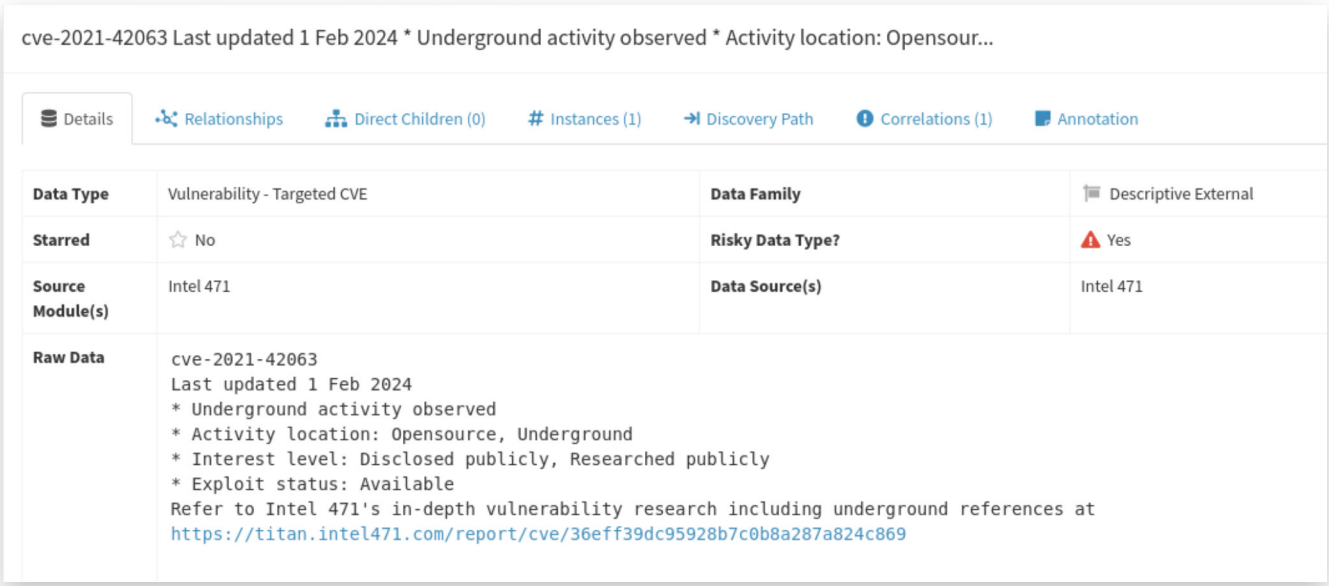
Integration — Easily integrate with SIEMs, SOARs, and other management systems to expedite the communication and remediation of potential vulnerabilities and minimize the amount of time your attack surface is exposed.

Baseline your performance — Save and compare the results of new and previous scans to monitor changes across the attack surface and use metrics to report on KPIs.

Alerting — Automated alerts immediately notify when a relevant change is made to your attack surface. Configuring automated alerts eliminates the need for manual checks for a faster response to issues.

KEY CAPABILITIES:

- Identify and reclaim unknown cloud and on-premises assets, services and unsanctioned IT
- Proactively defend against targeted threats and prioritize remediation
- Independently evaluate third-party vendor, subsidiary and/or M&A attack surface risks
- Monitor departments to improve compliance
- Empower pentesters, red teams, and intelligence teams to improve overall security posture against cyber threats
- Discover internet-exposed hosts, applications, software and identities
- Identify expired digital SSL certificates and weak encryption
- Understand your attack surface visibility using over 200 OSINT sources in addition to active scanning
- Reduce the duration of exposures with automated scans



TAKE YOUR ATTACK SURFACE DEFENSE TO THE NEXT LEVEL

471 Attack Surface Intelligence* extends and improves upon 471 Attack Surface Protection by unlocking full access to Intel 471's TITAN cyber threat intelligence platform, and provides invaluable insights into adversaries, marketplaces, underground forum mentions, detailed and continuously updated intelligence reports and General Intelligence Requirements.

** 471 Attack Surface Intelligence requires a subscription to Intel 471's TITAN cyber intelligence platform.*

ABOUT INTEL 471

Intel 471 arms enterprises and government agencies to win the cybersecurity war using real-time insights from the cyber underground. Organizations leverage our cyber intelligence platform to protect from costly security breaches and cyber incidents by solving real-world use cases, including third-party risk management, security operations, attack surface protection, fraud and more. Learn more at www.intel471.com.

Your Window into the Cyber Underground

SALES@INTEL471.COM