Coalfire Continues Penetration Risk Research, 5th Annual Report Highlights Evolution in Offensive Security

Continuous, intelligence-driven testing moves industry from point-in-time to all-the-time adversarial operations

GREENWOOD VILLAGE, CO – September 12, 2023 – Today Coalfire released its 5th annual Securealities Penetration Risk Report, validating a significant advancement in offensive security practices. Drawing on five years of penetration testing and vulnerability research, this year's report findings emphasize the urgency of moving from traditional point-in-time testing towards a threat-informed defense strategy driving adversarial-risk prioritization and more continuous testing. This industry transformation is spotlighted in the report foreword by MITRE Engenuity.

In the report, Coalfire analyzed over 11,000 penetration tests and nearly 500,000 hours of testing. The offensive security team examined 20,000 individual findings over the last five years from web, cloud, API, wireless, network, IoT hardware, and mobile tests, in addition to over 7,000 mobile app findings from NowSecure's analysis. The research takes a deep dive into industry vertical trends in technology, financial services, healthcare, and retail, along with a unique view into major cloud service providers.

Key risk findings include:

- **Many organizations are aggressively moving to the cloud without mastering cloud security fundamentals.** There is a shift in high-risk cloud vulnerabilities, with 79% of those surveyed reporting security misconfiguration as the top risk, followed by injection and encryption issues, a clear indication that companies are not practicing basic cyber hygiene.

- **The rise in high-risk vulnerabilities stems from an unclear view of the attack surface.** After a three-year decline, high-risk external vulnerabilities increased by 7% in 2023, with phishing attacks as the top technique used to gain initial breach access, followed by the exploitation of internet-facing systems.

- **Mobile apps are becoming core risk factors across the attack surface.** Often the primary point of customer and employee data access, mobile app risk continues to rise, with 88% of retail apps showing weak crypto issues– leaving a huge exploitable gap for millions of users.

- **The human factor continues to hamper security efforts.** Social engineering is the favored adversarial technique, given its high effectiveness in gaining an initial foothold in an organization. This year, the Coalfire pen testing team increased successful human element exploits by 8% over the previous year.

- **Software misconfiguration is the highest application security risk.** Top-five OWASP findings include security misconfiguration (31%), cryptographic failures (22%), vulnerable and outdated components (20%), identification and authentication (15%), and injection (8%).

- **Retail and healthcare sectors struggle the most with high-severity external exposure.** Retail led all industries with 28% high-risk external vulnerabilities, nearly doubling findings from 2022.

After three years of decline, high risks are up by 7% in healthcare. Social engineering scenarios continue to expose external attack vectors.

“Penetration testing is quickly progressing from an ancillary validation exercise for annual compliance audits to a continuous operational discipline that improves the ability to defend, detect, and respond to today’s Gen-AI equipped adversaries,” said Mark Carney, executive vice president at Coalfire. “The recognition of rising sophistication of adversaries amongst cybersecurity leadership is forcing a new mindset to routinely validate against relevant real-world scenarios for their organizations.”

"By applying the fundamental principles of a threat-informed defense, we can effectively address the challenges revealed in 2023 Penetration Risk Report,” said Jon Baker, director of the Center for Threat-Informed Defense at MITRE Engenuity, and author of the report foreword. “In alliance with Coalfire, a benefactor in our global R&D program, we're uniting the world's top security teams to innovate solutions for today's cyber defenders. Together, we're driving open-source adversary emulation capabilities that are turning the tables on our adversaries, injecting uncertainty into their next move."

About Coalfire
The world’s leading organizations – including the top five cloud service providers and leaders in financial services, healthcare, and retail – trust Coalfire to elevate their cyber programs and secure the future of their business. Number one in cloud penetrating testing, Coalfire is the world’s largest firm dedicated to cybersecurity services, providing unparalleled technology-enabled professional and managed services. To learn more, visit Coalfire.com.

###

For media inquiries:
Mike Gallo
(212) 239-8594
luminacoalfire@luminapr.com