Datasheet: Portfolio Security

On-PAR (Preparedness, Assurance, and Response)

Private Equity Portfolio Security Assessments

RKON's Security Assessment Methodology is designed to maximize budget and results. Our Security Assessment provides private equity and mid-market organizations with insights into active security threats and breaches that may be impacting their IT environment. These security threats include phishing attempts, malware, ransomware, insider threats, IOT, social engineering, and more.

WHY IT MATTERS

Hacking attempts and security breaches in private equity continue to increase drastically. An estimated 10% of PE portfolio companies have been compromised. A standard security approach will often take months to plan and execute, time that hackers can take advantage of. An On-PAR Security Assessment gives your team security visibility and reduces costs absorbed by portfolio leadership.

10%

of PE portfolio companies have been compromised

Security Environment

RKON analyzes dark web activity to determine if a Portco is targeted. We analyze portfolios from the hacker point of view, instead of simply scanning your environment.

Security Team

RKON's Private Equity Portfolio Security Assessment doesn't require any involvement from the portfolio IT team, who normally need a few months to fully respond and engage in a traditional audit. Let RKON be an extension of your IT team.

HOW IT WORKS

Private Equity Portfolio Risk and Security Methodology

Baseline Analysis

Phase one establishes an **actionable baseline** by combining two things:

1. A high-level review of client's security controls and effectiveness performed through survey.
2. By performing a dark web site audit to ascertain recent security breaches or activities in a passive, non-intrusive scan.

This allows RKON to develop a high-level score card per Portco to identify areas of risk in the portfolio.

Focused Assessment

For organizations that want to drive a more comprehensive approach, phase two performs a detailed **risk analysis** uncovered during the baseline phase where risks and gaps are quantified in detail. This information is taken to develop a comprehensive remediation program.

Private Equity Portfolio Baseline Analysis Dashboard

Remediation Program

Phase three provides thorough security remediation solutions. Proactively protect against cyber threats with a review of current and future state security architecture findings and recommendations. Our Jump-Start Security Maturity programs are offered in three levels: Foundation, Essential, and Advanced. Talk with a security expert today to **get started.**

Deliverables

- Three-Year IT Security Roadmap
- List of recommended projects, solutions, timelines, and budget
- Project Tracking in Online Security Project Dashboard
- Capital and Operating Expenditure Analysis
- RKON Professional and Managed Services Catalog
- Risks listed in IT Risk Register
- Summary of findings presented in Online Security and Risk Dashboard

Our approach solves the problem of expensive, one-size fits all security analysis that takes months to perform and results in an expansive remediation to do list that is handed back to an already overwhelmed IT staff.

RKON Risk
Advisory Team

WHY RKON

Get Tailored Security Advisory Solutions

Founded in 1998 in Chicago, RKON has grown to become one of the nation's leading IT advisory practices. Our comprehensive understanding of execution strategies, technology, business processes, operations analytics, risk and compliance, and planning and integration supports hundreds of organizations. Recognizing that no two companies have the same IT challenges, RKON takes a truly customized approach. We serve as trusted advisors to our customers, providing strategic guidance, technical resources, and honest assessments to address competitive challenges and meet long-term goals. Need to protect your portfolio from cyberattacks? **Let's talk.**