RISKSENSE

RiskSense Penetration Testing

Attack Surface Validation & Risk Exposure

© 2019 RiskSense, Inc.

Exposing Cyber Risk Layer by Layer

> ***"RiskSense is our go-to partner for cybersecurity. Excellent partner for consulting and work."***
>
> *– CIO, Arizona State University*

Comprehensive Atack Surface Coverage

Intelligence-Driven Risk Analytics

Time-to-Value

Shorten Time-to-Remediation

Traditional penetration testing is a snapshot in time and the most common strategy used to validate known vulnerabilities and a few readily available exploits on Metasploit or Kali distros. Worse still, most pen test firms are incapable of developing their own exploits as an attacker would.

Don't be satisfied with these results. Standard pen tests are not continuous and deliver a report that is not actionable or risk-centric. The report is often nothing more than re-formatted vulnerability scan data outlining vulnerabilities and not necessarily the exploits utilized. A few firms promise more but cannot scale. RiskSense delivers in all key areas – assessment time, delivery time, validation time, elapsed time to demonstrate lateral attack, and remediation time.

While traditional penetration testing is performed for a fixed period of time, RiskSense focuses on complete attack surface coverage rather than measuring time in engagement hours. RiskSense Penetration Testing services have validated over 3,000 exploits, allowing us to ensure coverage of all assets and exploitable vulnerabilities.

RiskSense penetration testers are security researchers and exploit writers who identify infiltration vectors up through potential lateral attacks, going beyond known exploits to cover the attack surface at all layers.

The delivery of results and findings has been thoroughly modernized. Both are delivered in near real-time through the RiskSense platform as the penetration test progresses. You are able to follow along and interact with the security analysts while the assessment is underway. Now, remediation activities can begin immediately thus avoiding any unnecessary latency that traditional pen tests introduce.

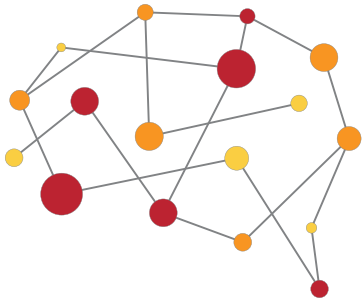
RiskSense value is not found in secret attack techniques, but rather in transparently providing information and helping you understanding your overall security posture. Findings are presented in easy to understand yet detailed formats so that your team can reproduce issues and in turn use the RiskSense platform to validate remediation.

All exploits are performed using freely available tools or custom-developed scripts, with provided screenshots making it easy to replicate RiskSense findings and attack paths.

The RiskSense Advantage

RiskSense Methodology and Team Provide Foundational Strength

First and foremost, RiskSense has built a team of deep security analyst experience. Exploit writers and researchers look at attack vectors and multi-phase approaches that could expose your business. Our proven methodology provides clients the most effective approach, leveraging focused subject-matter expertise as needed. Transparency and access to RiskSense analysts, daily touch-point meetings, and ad hoc discussions of current findings are always available.



Human Intelligence

Unique Tools

Synchronous Delivery

RiskSense-Developed Tools Enhance Penetration Testing Effectiveness

RiskSense cybersecurity professionals have created a number unique, industry-leading tools. For example, DA Bomb and Koadic allow RiskSense to replicate and scale the behavior of sophisticated attackers. DA Bomb eliminates known repeatable attack techniques from manual testing processes, and Koadic rapidly replicates sophisticated post-exploitation techniques across large scale networks. We've even open sourced Koadic to help further state-of-the-art pen testing techniques.

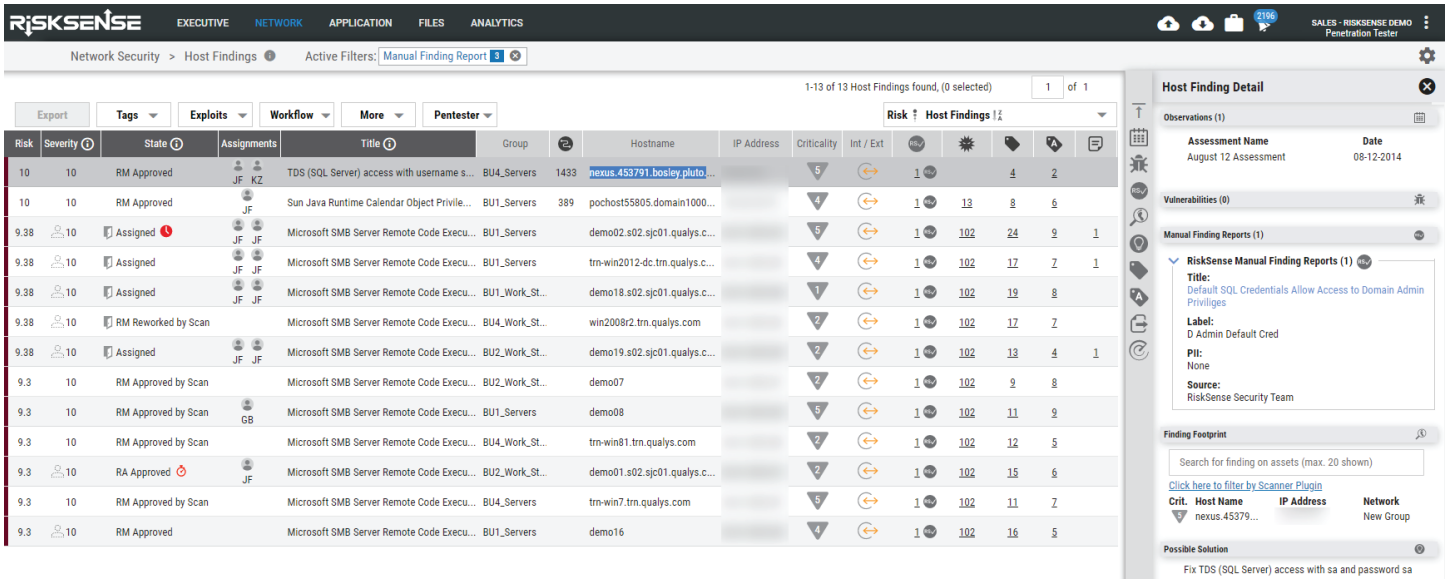
Immediate Visibility with Near Real-Time Delivery of Assessment Results

Ongoing penetration test findings and results are delivered in near real-time through the RiskSense platform, preventing the introduction of additional latency that traditional pen testing injects while waiting for a test to complete and a report to be issued. Our risk-based vulnerability management platform continuously ingests massive amounts of vulnerability and threat data, giving our clients access to the details and recommendations needed to fix critical vulnerabilities, allowing them to quickly understand and address their cybersecurity risk exposure without waiting for an engagement to conclude. We utilize a modern pen test methodology, continuously improving the experience we provide our clients.

Traditional Versus RiskSense Pen Tests

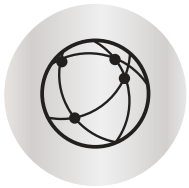
	Traditional Pen Tests	RiskSense Pen Tests
Resources	Typically 1 or 2 people	Team approach with over 150+ curated threat sources
Location	Can be onsite	Onsite and remote options
Coverage	Hours-based	100% scope of coverage
Better For	Vulnerabilities	Vulnerabilities, exploits, attack paths
Time to Test	Based on hours purchased	100% coverage typically achieved in 2-3 weeks
Results	High volume of unactionable vulnerabilities	Uncover critical vulnerabilities and exploits with actionable remediation guidance
Industry Contributions	Minimal	Exploit tools, conference talks, and notable published research
Costs	Fixed hours	Fixed coverage
Deliverables	PDFs and spreadsheets	Near real-time delivery of findings via the RiskSense platform with remediation workflows and progress tracking; PDFs
Criticality / Scoring	Industry-based (CVSS)	Contextually analyzed using risk potential, escalating or waning threat scenarios, and human-intel from RiskSense analysts and researchers
Impact	Data overload; must digest findings and then determine action	Actionable, prioritized remediation recommendations

RiskSence Pen Test Findings



RiskSense Testing Services

Security testing requires focusing on your entire attack surface and the vulnerabilities that allow cyber criminals to exploit them and conduct malicious activity.



Network | Applications | IoT | Vulnerability Discovery

Web Application Attack Surface Validation

RiskSense provides a deep security evaluation of a web application in a customized approach that looks at the target web application's development components, features, and business functionality. We use a proprietary framework to discover multiple attack vectors by passing or inputting data to user interfaces, network interfaces, application programming interfaces (APIs), and other places where inputs are processed. As part of the dynamic testing, our team determines the areas of the code that are critical to application security. The core functionality areas include authentication, role/privilege management, information passing, storage encryption/decryption, and input/output filtering. RiskSense security analysts review these areas to ensure they conform to industry best practices for secure software development.

Network Attack Surface Validation

RiskSense provides a comprehensive evaluation of target network(s), systems, and computing environments using best practice methods to identify vulnerabilities, enumerate attack surface exposure, and validate key infiltration vectors. The assessment is performed using a multi-scanner approach based on 100% coverage of every device within target scope and is combined with manual testing to determine susceptibility to compromise.

IoT Attack Surface Validation

A growing focus, this evaluation investigates the IoT device and all of its interactive components to identify vulnerabilities that adversaries can exploit. Beyond the IoT devices themselves, RiskSense evaluates the development, code, environments, and processes used from end-to-end. Interconnected networks, vendors, platforms, programmable interfaces, and protocols all potentially introduce vulnerabilities within IoT systems creating double exposure risk.

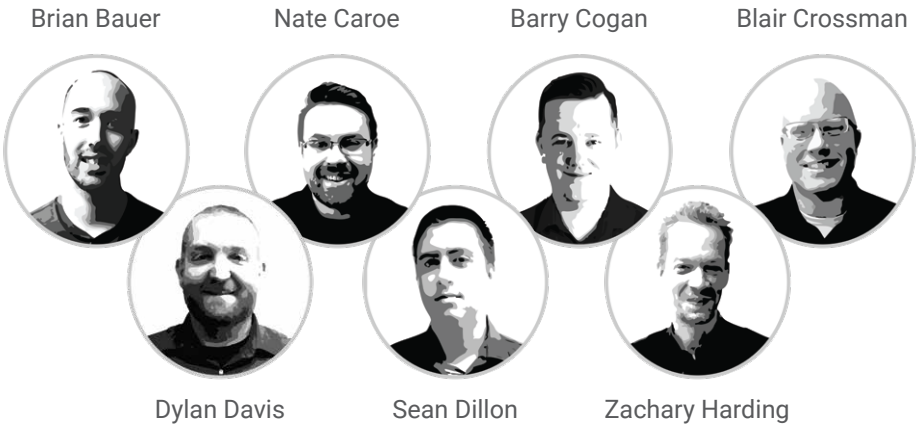
Vulnerability Discovery

RiskSense provides fully managed vulnerability assessments at monthly, quarterly, or annual intervals that swiftly and accurately identify misconfigurations and vulnerabilities on your network. RiskSense can also provide consulting to aid you in setting up your own in-house vulnerability scanning program. We identify the vulnerabilities that are most likely to be used by adversaries to carry out infiltration and utilize post-exploitation techniques to launch successful attacks across the enterprise. Within with the RiskSense platform clients are provided the visibility, prioritization, and actionable remediation recommendations needed to lower their organization's cybersecurity risk.

Introducing the RiskSense Senior Analyst Team

50+ Years Industry Experience

Our security researchers and exploit writers are among the best in the industry; you're getting far more than typical penetration testing. All members of the team have years of experience in defending critical networks against the world's most dangerous cyber adversaries. Many of them regularly speak at industry conferences and frequently release cutting-edge security research.



Each RiskSense team member brings a level of expertise and experience that we align with specific project needs. Our team members complement each other to provide a holistic approach and deep focus to every engagement. Teamwork permeates all project aspects. Our family of analysts collaborate and have a passion for sharing and driving professional excellence in each other. Beyond the team chosen for a given project, additonal staff members act as sounding boards, always eager to explore alternate attack vectors and exploit paths.

Industry-leading time to value with transparency and actionable insights

Since becoming a RiskSense customer, El Paso Electric has accelerated time to remediation and has applied corrective measures to hundreds of vulnerabilities that measurably impacted their cybersecurity risk posture. Working with RiskSense Pen Testing teams and use of the RiskSense platform has given them peace of mind knowing that their existing security and IT resources are able to swiftly deliver maximum value, actively making a measurable difference in their security posture.

"Excellent technical capabilities demonstrated and superb customer service. We will continue to work with RiskSense in the future." – *Rick Bernal, Information Security Manager, El Paso Electric*

History

Cyber resilience is a new market segment that our founding team pioneered and perfected over many years. RiskSense itself came to existence in May 2015. The company was initially founded in 2006 as CAaNES (Computational Analysis and Network Enterprise Solutions) LLC and is a spin-off from the New Mexico Institute of Mining and Technology (New Mexico Tech).

Under the CAaNES label, the team conducted research-as-a-service engagements, which led us to be part of a think tank that advised the U.S. Department of Defense and U.S. Intelligence Community. As part of these engagements, we developed Computational Analysis of Cyber Terrorism Against the U.S. (CACTUS), Support Vectors Intrusion Detection, Behavior Risk Analysis of Vicious Executables (BRAVE), and the Strike Team Program. The team was also the first to create RFID malware and showcased it in the field to prove that RFID was less secure than many had thought.

Over the years, we realized that our findings and expertise could serve a broader set of customers. In turn, we productized our knowledge and created the RiskSense platform, which transforms cyber risk management into a more proactive, collaborative, and real-time discipline across the entire computing stack. After some prototyping, we launched this Software-as-a-Service platform in 2012. The RiskSense platform embodies the expertise and intimate knowledge gained from real-world experience in defending critical networks from the world's most dangerous cyber adversaries.

Today, we're over 100 employees strong, serving more than 150 clients across every major industry segment. We have seen tremendous growth over the years and are proud to have started as a self-funded, profitable company. We are headquartered in Sunnyvale, California with offices in Albuquerque, New Mexico as well as internationally in Chennai and Bangalore (India).

Since its inception, RiskSense has invested heavily in research, leading to a variety of patents that are part of the RiskSense platform DNA. To stay ahead of cyber adversaries, RiskSense employs a deep bench of security researchers and collaborates via its Fellowship Program with leading IT and cybersecurity programs at New Mexico Tech, UC Riverside, and Carnegie Mellon University, among others.

About RiskSense

RiskSense®, Inc. provides vulnerability management and prioritization to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated pen testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness. For more information, visit www.risksense.com or follow us on Twitter at @RiskSense.

RiskSense – the industry's most comprehensive risk-based vulnerability management and prioritization platform

Contact Us Today to Learn More About RiskSense

RiskSense, Inc. | +1 844.234.RISK | +1 505.217.9422 | info@RiskSense.com

CONTACT US | SCHEDULE A DEMO | READ OUR BLOG

© 2019 RiskSense, Inc. All rights reserved. RiskSense and the RiskSense logo are registered trademarks of RiskSense, Inc.

Brochure_PenetrationTest_20190603