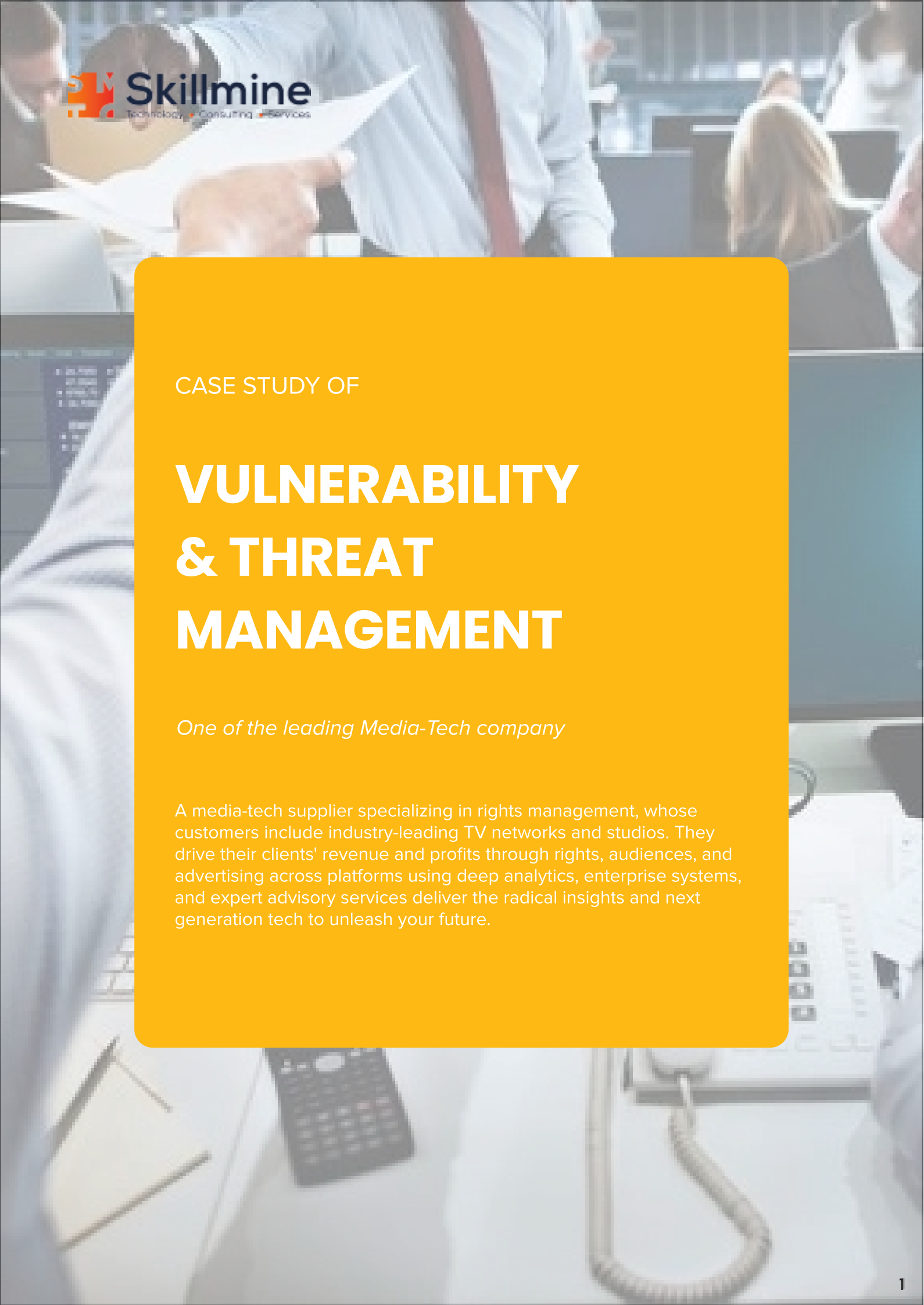

Skillmine
Technology • Consulting • Services

CASE STUDY OF

VULNERABILITY & THREAT MANAGEMENT

One of the leading Media-Tech company

A media-tech supplier specializing in rights management, whose customers include industry-leading TV networks and studios. They drive their clients' revenue and profits through rights, audiences, and advertising across platforms using deep analytics, enterprise systems, and expert advisory services deliver the radical insights and next generation tech to unleash your future.

Business Challenge

- Five ranges of IP addresses were not managed.
- Obsolete legacy software was being used.
- Web applications were programmed to run only on internet explorer, which is shutting down in 2022.
- The single point of contact from the company didn't understand the severity of the vulnerabilities.
- Business logic vulnerability.
- Full Trust CLR Verification issue Exploiting Passing Reference Types by Reference.
- Insufficient Session-ID Length.
- Unsafe function call from a signal handler.
- Using a broken or risky cryptographic algorithm.
- Unchecked Return Value Missing Check against Null.
- Deserialization of untrusted data.
- Unchecked Error Condition.
- Missing XML Validation.

Skillmine Solution

Risk Classification

Defining, identifying, classifying, and prioritizing vulnerabilities in systems and applications.

Evidence of Vulnerabilities

Clear classification of Vulnerabilities

Issue & Impact Analysis

Impact map of Vulnerabilities.

What could be exploited to what extent.

Classification of Impact and Probability.

Recommendations & Ongoing Assistance

Specific Recommendations for Remediation.

Best Practices on remediation.

Advising for any standards needs to be adopted.

Execution

Skillmine managed all the internal IP's and set up a structure, we internally tested the open vulnerabilities of internal IP addresses that were within the network. Created a subsystem for windows, which was basically a virtual environment for that system and fixed it. Migrated all web applications from internet explorer to Google chrome. We used Burp Suite Professional, it is one of the most popular penetration testing and vulnerability finder tools and is often used for checking web application security.

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. The Nessus Scan Report presents extensive data about vulnerabilities detected on the network. Detailed information about the vulnerabilities detected on every host scanned is included.

Checkmarx is the global leader in software security solutions for modern enterprise software development. Checkmarx provides static and interactive application security testing, software composition analysis, and developer application security awareness and training programs to reduce and remediate risk from software vulnerabilities.

Data Points

- 1,275 devices (IP addresses) that were within the system were managed.
- Q1 – VA & PT Service Initiation, Knowledge Transition, Prerequisites Setup, Scanning.
- As per the Scope Internal IP's- 10.10.21.x,10.10.22.x, 10.10.31.x,10.10.32.x,10.10.33.x, External IP's-16, Web Application- 2 Applications are On Prem applications and 8 Public facing Applications.
- Remediation Exercise (Q1 Results) Working with Action Owners to remediate the identified vulnerabilities.
- In Internal VA 77 vulnerabilities, External Ips, 61 vulnerabilities and Web Application 126 Vulnerabilities were reported.

- In Internal Ip, following are considered as "Out-of-Scope" with remarks, High: 14, Medium:43, Low:04 and vulnerabilities mitigated are, High: 03, Medium:12, Low:01.
- In web app, following are considered as "Out-of-Scope" with remarks, High: 06 Medium:07, Low:41 and vulnerabilities mitigated are, High:17, Medium:38, Low:17.
- In External Ip, following are considered as "Out-of-Scope" with remarks, High: 03, Medium:07, Low:23 and vulnerabilities mitigated are, High: 03, Medium:17, Low:08.
- As per the Scope confirmatory test was not initiated.
- Confirmatory test Scope of work is changed Internal IP's-10.10.21.x,10.10.22.x, 10.10.31.x,10.10.32.x,10.1.60.x, Azure IP's were increased due to RSG Media infrastructure migration to Azure, Web Application- 6 Applications are integrated into 3 On Prem applications and 3 Public facing Applications.
- Q2 VA Results Review with Stakeholders and identify owners against action items in progress.

Capability
& Competency

- Digitization & Robotic Automation
- Analytics
- Mobility
- Social Media
- Cognitive Computing
- Artificial Intelligence
- Endpoint Protection
- Network Monitoring
- Intrusion Detection
- Application Security
- Device Security
- Data Protection & Anti-virus
- Mobile Security
- Threat Intelligence
- Predictive Analytics
- Identity and Access Management
- Log Management
- Firewalls

For more information
Contact: info@skill-mine.com
Visit us: skill-mine.com

Skillmine
Technology • Consulting • Services
India | KSA | UK | USA

Stay connected