RADAR Service Description
Hosted Vulnerability Management

INGRAM MICRO CLOUD MARKET PLACE

Last Updated: March 2021

RADAR Service Description

Overview

In today's rapidly evolving technology landscape, traditional antivirus measures and firewalls are no longer sufficient defence from malicious actors. RADAR is a key component of a holistic cybersecurity program. RADAR is a Hosted Vulnerability Management service that allows organizations to identify vulnerable servers as well as missing patches in the environment, which are two of the most common attack vectors used by intruders. RADAR identifies the vulnerabilities in an environment by using the same methods hackers employ. Once vulnerabilities are identified, we integrate with the client's risk management team to recommend solutions and assess their success.

Our Approach

There are 2 components to RADAR:

1. **External vulnerability scanner:** This is ISA's vulnerability scanner located in the cloud that will be used to scan the client's perimeter externally.
2. **Virtual internal vulnerability scanner**: The vulnerability scanner(s) that ISA will help the client install on their premises. This is used to run internal vulnerability scans based on ISA's predefined policies. The cloud console will connect to the scanner to schedule scans and retrieve any identified vulnerability data.

ISA uses the following methodology when approaching vulnerability management:

- Scan preparation: Scheduling when assets will be scanned, creating custom policies, and organizing scan assets.
- Discovery: Gathering information on the scan assets, including which assets are live in the environment from a provided IP address range, determining which services are running, and identifying which operating systems are running.
- Vulnerability Scans: Using pre-defined policies, internal and external scans are conducted to determine what vulnerabilities are present on each host.
  - *Internal scans:* Identify vulnerabilities present within the client's environment that could allow threat actors to move laterally within the environment after gaining access and cause additional damage.
  - *External scans:* Identify vulnerabilities present at the client's perimeter that could allow threat actors to gain unauthorized access to the client's environment.
- Reporting: Generating an automated report that communicates the vulnerabilities found, the potential risks that each vulnerability poses to the client's environment and the remediation actions for these vulnerabilities.

Deliverables and Outcomes

RADAR will:

- Help install and configure on-premises vulnerability scanner software
- Conduct ongoing external and internal scans of your environment
- Identify current and emerging vulnerabilities using plugins updated daily as new vulnerabilities are discovered
- Deliver a Vulnerability Assessment Report listing vulnerabilities present and how to remediate those vulnerabilities
- Provide prioritized recommendations on which identified vulnerabilities need to be remediated first.
- Shorten the time to remediation for identified vulnerabilities

Partner & Client Involvement

A resource will be required to perform the following tasks:

- VPN tunnel between Client and CIOC network
- Setup VM on Client side to install Scanner Agent
- Integrate Risk management process with ISA CIOC team

Industry Trend

According to Verizon's 2019 data breach report[1], most breaches happen due to exploitation of vulnerabilities and misconfigurations.

Most cybersecurity standards, including PCI, SOX, NIST 800-53 and ISO27001, recommend the presence of a vulnerability management tool to ensure visibility and mitigation over security issues.

---

[1] https://enterprise.verizon.com/resources/reports/dbir/

RADAR Features and Deliverables

RADAR comes with a set of enterprise-grade features to provide a world-class vulnerability management service:

Features & Deliverables[2]	RADAR	Partner support required?
Onboarding Process		
Project Manager support	✓	Yes
Client to provide list of hosts in scope for scanning, incl. test host	✓	Yes
Deployment of virtual scanner	✓	Yes
Scanning policy selection (conservative to aggressive)	✓	
Discovery scan	✓	
Architecture		
Firewall policy enablement	✓	Yes
Service available as a Cloud Service	✓	
Policy tuning as required	✓	
Grouping and custom scanning policies	Add-on	
Source code & open-source code scanning	Add-on	
Monitoring & Reporting		
Detection & alerting if scanner port is unreachable	✓	
Access to ISA ticketing portal	✓	
Creating tickets in ISA ticketing system	✓	
Email escalation (one)	✓	
Automated email report after scanning	✓	
24/7 by 365 ISA CIOC Support	✓	
Vulnerability Management		
Remote scanning	✓	
Internal host scanning	✓	
Deployment of multiple scanners as needed	✓	
New asset discovery	✓	
Identification of business-critical assets and scanning accordingly	✓	
Updates on remediation actions	✓	

---

[2] Non-exhaustive list, subject to change

RADAR Pricelist

RADAR is priced monthly, per IP that needs to be scanned. For details, see the Ingram Micro Cloud Market Place.

ISA Difference

RADAR, ISA's Hosted Vulnerability Management Service, provides organizations with a proactive approach to identifying and remediating identified vulnerabilities. Using a suite of custom ISA solutions, we identify security gaps others might miss, and help prioritize and shorten remediation efforts. This allows you to improve your security posture and focus on your core business. ISA can provide a degree of customization tailored to your specific assets that best fit your environment or reporting needs.

THIS SERVICE DESCRIPTION DOCUMENT, INCL. THE PRICELIST IS INTENDED EXCLUSIVELY FOR INFINITY PARTNERS, INFINITY PARTNERS CAN PRICE THE SERVICE FOR END CLIENTS AT THEIR DISCRETION