SATISNET VULNERABILITY MANAGEMENT SERVICE (SVMS)

VULNERABILITY MANAGEMENT IS A TIME CONSUMING EXERCISE, LET US MANAGE IT

RELIABLE VULNERABILITY MANAGEMENT

Satisnet Vulnerability Management Service, powered by Tenable Network Security, performs highly accurate internal and external scan audits across network devices, servers, web applications, databases, and other assets in on-premise and cloud environments.

The scanning technology is fully managed and maintained by our dedicated vulnerability management team, eliminating administration and maintenance burdens so you can better focus on protecting your assets and reducing business risk.

KEY BENEFITS OF SVMS

- Continuous 'always on' scanning using Tenable's passive scanner(s)
- Identify exploitable vulnerabilities with the largest knowledgebase of vulnerability checks in the industry
- Dedicated team of experts: Virtually eliminate false positives with expert operational support
- Satisfy regulatory compliance requirements
- Track remediation workflow across the infrastructure
- Automation with other security tooling
- Correlation with threat intelligence and other alerting systems
- Integration with existing ticketing systems

SERVICE SETUP

The service is quick to setup, with Satisnet's SOC having secure VPN tunnel access to a customer's network to access the Tenable SecurityCenter console. All customer data remains 'in-house'.

satisnet streamlining security management

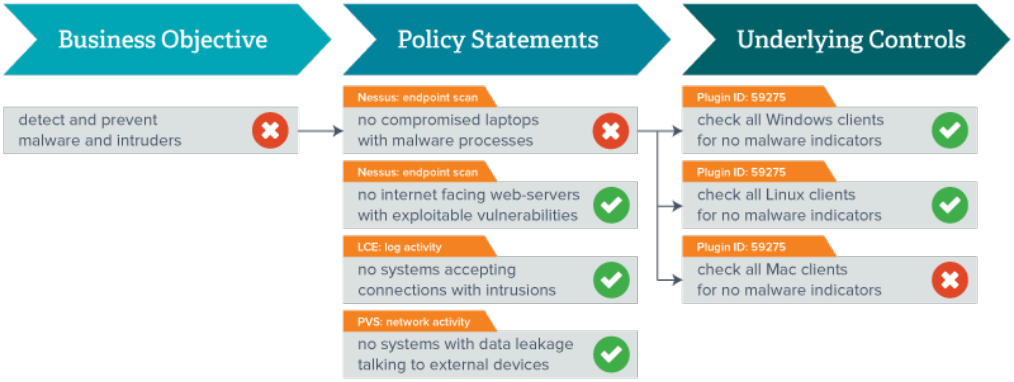
tenable network security

WWW.SATISNET.CO.UK

SERVICE DELIVERABLES

- Creation and maintenance of policies to be used for the scanning of devices internally or externally, based on customer requirements
- Creation and maintenance of automated scan schedules with the inclusion of ad-hoc scanning based on customer requirements
- Creation and maintenance of assets based on customer requirements and best practices
- Automatic reporting of critical or exploitable vulnerabilities at the time of discovery

Assurance Report Cards



- A weekly breakdown of the hosts scanned and the vulnerabilities discovered in order of severity (this can be overridden by a customer's criticality choice – e.g. servers in a particular range or asset group are more critical to the business and thus higher in severity)
- Offering of custom reports and alerts for all customers based on their internal metrics
- Creation and reporting on Assurance Report Cards (ARCs) either from templates or custom created for individual customers/users
- Maintenance of Log Correlation Engine policies and clients
- Updates for all components of SecurityCenter
- SecurityCenter Console
- Nessus Scanners
- Passive Vulnerability Scanners
- Log Correlation Engine Server
- Incident response
- Cyber Run-Books - Workflows and SLA's
- Automations
- Weekly/monthly review meetings

FLOWLANES

Personalised Run-Books detailing best practices and next steps for all detected incidents

INCIDENT DASHBOARD

Realtime Threat Landscape

Key Performance Indicators

Targeted Reports