WHITE PAPER

VULNERABILITY MANAGEMENT PRIMER

OCT 2024

TABLE OF CONTENTS

INTRODUCTION

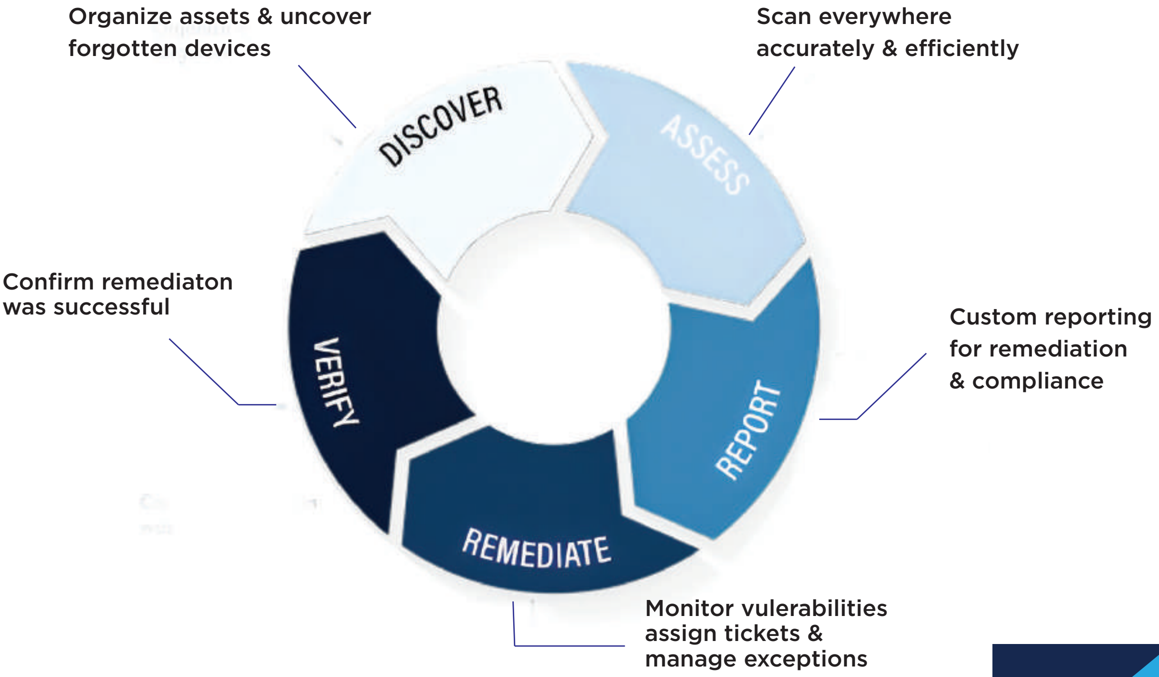
Digital technologies lie at the heart of nearly every industry today, including banking. The automation and greater connectedness they afford have revolutionised the world's economic and financial institutions — but they've also brought risk in the form of cyberattacks.

These cyberattacks pose numerous challenges — increasingly persistent and devious threat actors, a daily flood of data full of extraneous information and false alarms across multiple, unconnected security systems, and a serious shortage of skilled professionals.

VULNERABILITY MANAGEMENT

Vulnerability management is the practice of proactively identifying, analysing, and addressing potential weaknesses in hardware or software that could serve as an attack vector. The basic goal is to apply these fixes before an attacker can use them to cause a cybersecurity breach.

"It is the process of staying on top of vulnerabilities so the fixes can be more frequent and effective." — CSO Online


Organize assets & uncover forgotten devices
Scan everywhere accurately & efficiently
DISCOVER
ASSESS
Confirm remediaton was successful
VERIFY
REPORT
Custom reporting for remediation & compliance
REMEDIATE
Monitor vulerabilities assign tickets & manage exceptions

CURRENT CHALLENGES

There are two major sets of factors that impact an organisation's ability to effectively protect themselves against cyber threats. The first set relates to the growing frequency, reach, and sophistication of threats and their risk to each organisational unit. The second set is operational complexities that make it difficult for an organisation to know what vulnerabilities are exploitable, how they map to its asset criticality footprint, and what other factors achieve cyber hygiene.

Building and executing a vulnerability management program can be a daunting task. With the number of vulnerabilities growing by the day, many organisations continue to struggle to wrap their arms around such a gigantic task. Discovering the vulnerabilities isn't necessarily the biggest pain point but dealing with the amount of vulnerabilities that organisations are finding. Having the ability to manage the sheer volume of vulnerabilities, correctly prioritise them, and track the organisation's progress in mitigating them are the largest concerns experienced today.

Moreover, the successful management of vulnerabilities requires not just comprehsive insight into the evolving field of vulnerbilties and threats, but also the means to effectively prioritise activities by enterprise risks.

It is one thing to say that an organisation must adopt a risk-based approach to cybersecurity that includes continuous compliance controls and closed loop management of threats and vulnerabilities. It is quite another thing to do it. The current technology environment is becoming increasingly complex, both in terms of the organisation's internal and cloud infrastructure and in terms of the threats looming overhead.

Seeking answers to following questions will give you a far better understanding and insight of where your vulnerability management program stands and where it should be:

- How can you get a handle on the large number of vulnerabilities that plague your operations?
- What is happening around the world? Which vulnerabilities are most exploited? Have there been any attacks in your industry? Who is targeting your organisation, and from where?
- Is your vulnerability management program driven only based on the vulnerability's severity scores provided by the vulnerability assessment tools?
- Can you really afford to prioritise a High severity vulnerability on a receptionist PC over a Medium severity vulnerability on a mission critical server?
- Is there an automated mechanism to conduct follow-up assessments?
- Are you leveraging the all-important Risk Assessment reports/Risk Registers produced by your GRC team?
- Is Asset Register and asset score taken into consideration?
- How about the alerts from your SIEM or other security technologies?

RISK-BASED VULNERABILITY MANAGEMENT

A proper, integrated, automated, and risk-based vulnerability management program enables you to remediate vulnerabilities at scale.

Some of the things to consider while building a vulnerability management program are:

THREAT SCORING

Go beyond the traditional product-based (High, Medium, Low) severity scoring of vulnerabilities. Make use of contextual data like alerts from SIEM and organitional risks from the GRC team, for better prioritistion and scoring. This contextualised information helps in better prioritisation of vulnerabilities that should be patched first.

ASSET VALUES

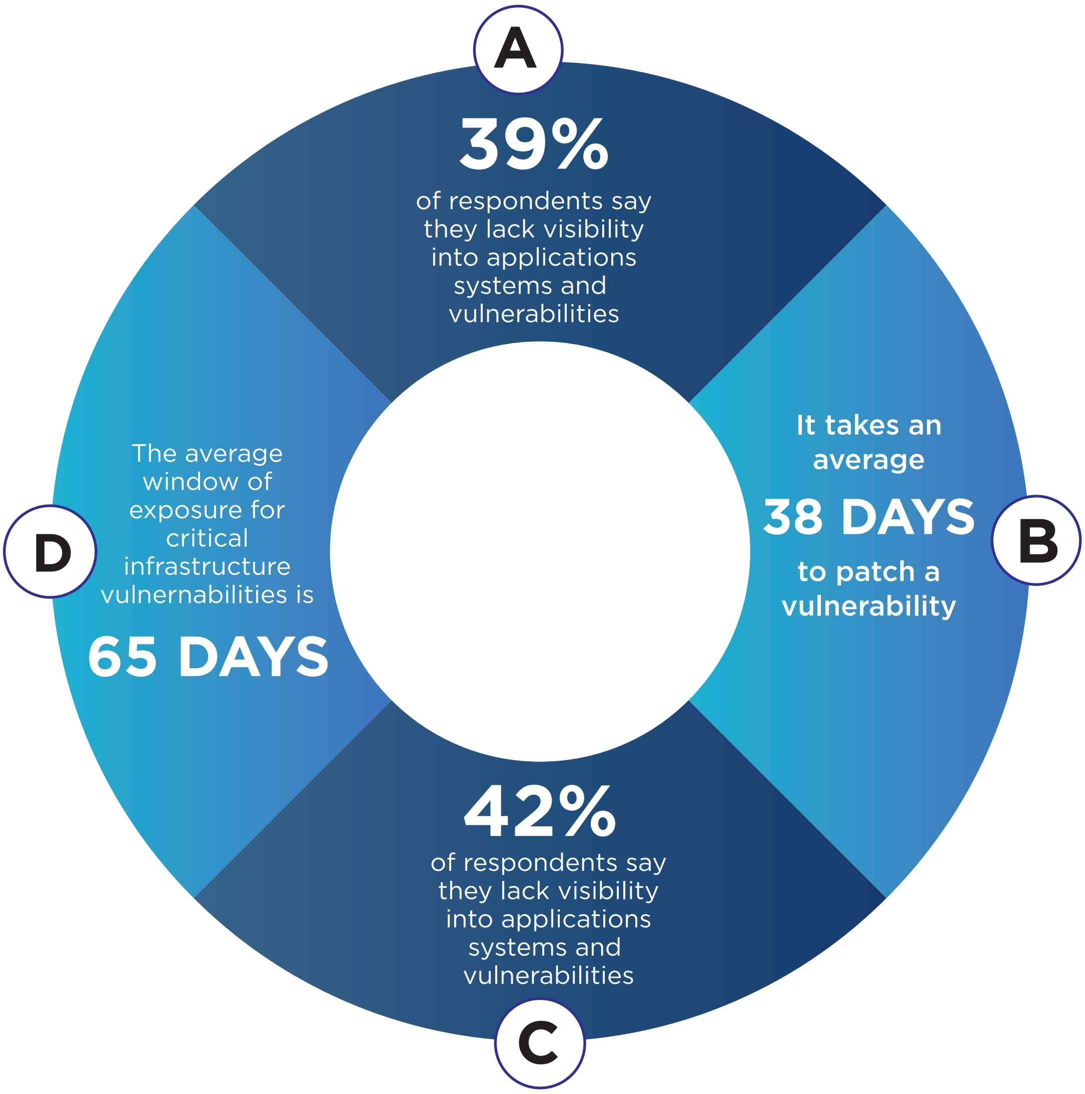
Make use of your Asset register and individual asset's value i.e. how important an asset is to the organisation. Because you may want to fix a medium severity vulnerability on a server before fixing a high severity vulnerability on a help desk laptop.

Go for a one window solution to get reports from different security technologies at one place. Establish integrations with help desk systems and patch management systems. This allows you to establish a communication and remediation channel with other departments. Assign tasks to other departments and asset owners from the same platform.

AUTOMATION

Vulnerability management is an ongoing process. Every scan requires a follow-up scan after a round of patching and fixing. Capability to automate these assessment activities can dramatically reduce time to identify and remediate the vulnerabilities. With automation, you can schedule follow-up scans or execute them

SOAR solutions derive several key benefits when connected to automated vulnerability management.



A

39%

of respondents say they lack visibility into applications systems and vulnerabilities

B

It takes an average

38 DAYS

to patch a vulnerability

C

42%

of respondents say they lack visibility into applications systems and vulnerabilities

D

The average window of exposure for critical infrastructure vulnernabilities is

65 DAYS

TRADITIONAL VULNERABILITY MANAGEMENT	VS	VULNERABILITY MANAGEMENT WITH SIRP
High false positives		Near zero false positives
Lack of prioritization		Automated priotization based on risk level
Lack of contextualization		Context-aware vulnerability management
Limited visibility		Full visibility of security operations
No automation and orchestration		Comprehensive automation and archestration
Lack of communication and coordination		Comprehensive case management

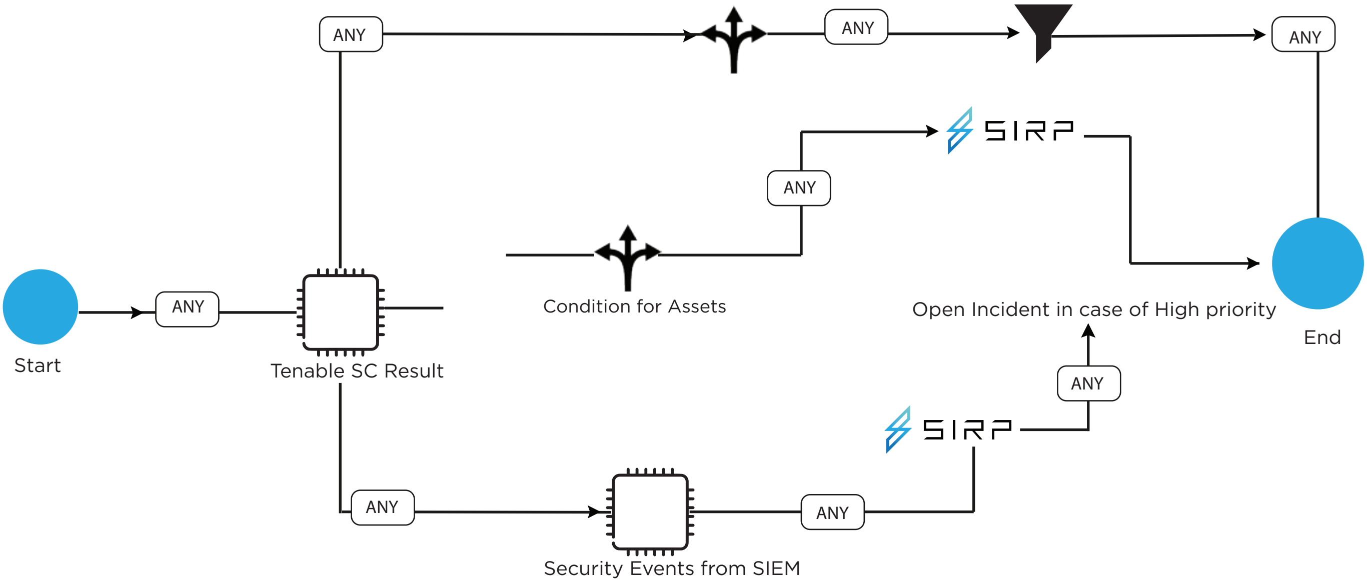
USE CASES

An organisation has developed their operational plan on how they would like to triage their vulnerability scanning results. They gathered input from all departments who would be responsible for helping to mitigate their vulnerabilities and created their action plan.

When a new vulnerability is detected by the Tenable Security Centre, SIRP playbook for Vulnerability Management is executed automatically.

The Vulnerability Management playbook will start off by identifying what vulnerability has been detected. Depending on the priority, it will take one of three paths to confirm its true priority and alert the necessary teams for mitigation. Once the vulnerability is parsed from the event, the plabook will pull information regarding the involved asset including its system information.

Once this information is gathered, SIRP will come to its first set of conditional statements which look to see if the involved asset is a high priority.



If the asset is considered a high priority target, the playbook will elevate its priority to critical if it is already a high priority vulnerability. If it is a medium or low priority vulnerability it will be upgraded to a higher priority incident. Once this information is gathered, SIRP will come to its second set of conditional statements which evaluate whether there were any additional security events targeting the asset. If there were additional security events a user choice selection will temporarily pause the playbook and alert an analyst for manual review of the case.

If the analyst finds that the events were targeting the vulnerability reported by the asset, the priority is again adjusted and a case is created in the SIRP for the responsible parties, which include the change asset owners, change management team, and patch management team to plan for appropriate patch and mitigation activities If additional security events are not

observed, the playbook will conclude by opening a case in the for the appropriate parties to review the vulnerabilities by vulnerability priority and plan for patching and remediation

USE CASE #2 - Automated Vulnerability Ingestion, Enrichment and Response

CHALLENGE:

Constantly evolving threats keep security teams perpetually behind the eight-ball trying to identify and patch vulnerabilities before they are exploited.

SOLUTION:

With SIRP's integration with different VA tools, the vulnerabilities are automatically ingested into the SIRP. Upon ingestion, automated playbooks enrich and add context to these vulnerabilities by utilising threat intelligence data. The playbook then hands-off control to security analysts for further investigation or remediation.

BENEFIT:

The solution helps analysts prioritise vulnerabilities based on severity level and the threat actor behind the attack. This has proven to shorten the time from detection to response from hours to minutes. In addition, a standardised process implemented via automated playbooks can pave the way to more proactive vulnerability management.

USE CASE #3 - Interactive, Real-time Investigation for Complex Threats

CHALLENGE:

While playbooks can automate commonly performed tasks to ease analyst load, an attack investigation usually requires additional tasks such as pivoting from one suspicious indicator to another to gather critical evidence, drawing relations between incidents, and finalising resolution. Running these commands traps analysts in a screen-switching cycle during investigation and a documentation-chasing cycle after investigations end.

SOLUTION:

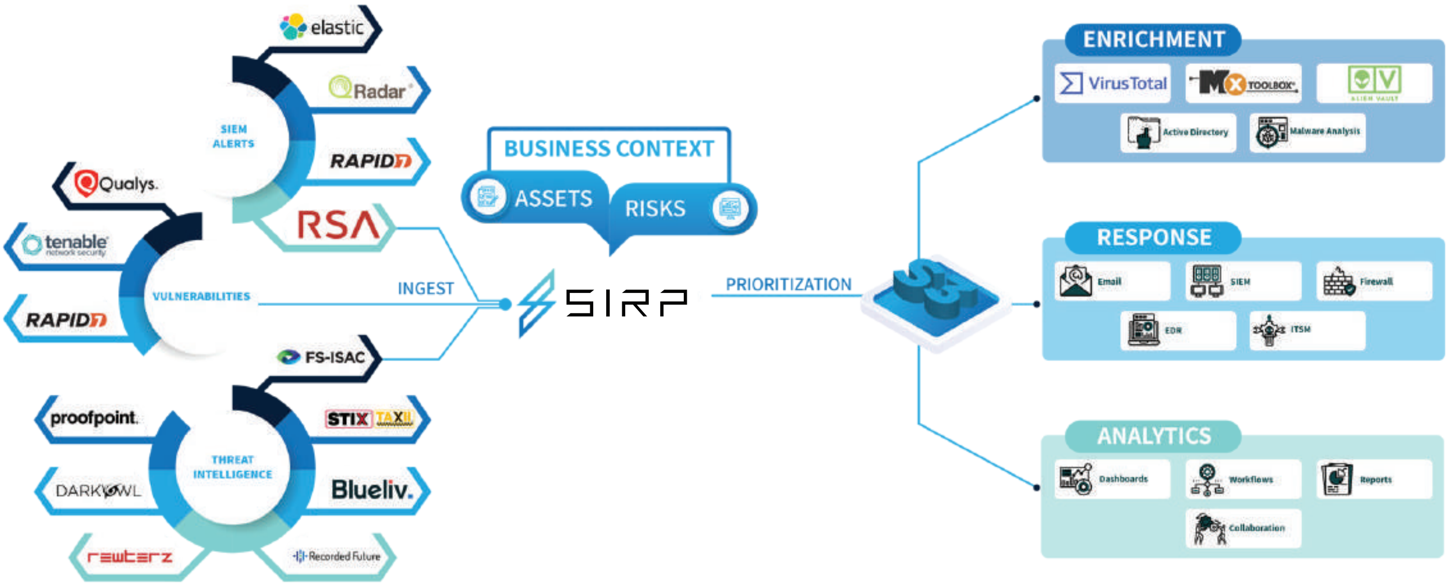
After running enrichment playbooks, analysts can then gain greater visibility and new actionable information about the vulnerability. For example, if playbook results throw up alert details, analysts can retrieve details for a given vulnerability or get specific device information. They can also run actions from other security tools in real-time using the SIRP, ensuring a single-console view for end-to-end investigation.

BENEFIT:

SIRP allows analysts to quickly pivot and run unique actions relevant to vulnerabilities and incidents in their network from a single window. All participating analysts will have full task-level visibility of the process and be able to run and document actions from the same window.

SIRP – RISK-BASED SOAR PLATFORM

SIRP is a Risk-based Security Orchestration, Automation and Response (SOAR) platform that fuses essential cybersecurity information to enable a unified cyber response. Through a single integrated platform, it drives security visibility, so decisions can be better prioritised and response time is dramatically reduced. With SIRP, the entire cybersecurity function works as a single, cohesive unit.



SIRP provides a more dynamic, complete view of incidents, threat intelligence, vulnerabilities, and risks in one place, so you can prioritise and make better decisions faster and respond more effectively. It combines security orchestration, playbook automation and case management capabilities to integrate your team, processes and tools together. SIRP makes security data instantly actionable, provides valuable intelligence and context, and enables adaptive response to complex cyber threats and vulnerabilities.

SIRP provides security teams with instant access to four powerful modules, incident management, threat intelligence, vulnerability management and risk management. SIRP Security Score (S3) module makes security data instantly actionable by fusing information from these modules and assessing the risk to the organisation. S3 uses machine learning algorithms to assess security data relevancy and calculate security score. S3 enables organisations to prioritise risks, make better decisions faster and respond more effectively.

SIRP's modular architecture supports more than 200+ applications with coverage of 1000+ APIs, enabling security teams to connect and coordinate complex workflows across different teams and tools. Powerful abstraction allows security teams to focus on what they want to accomplish, while the platform translates that into tool-specific actions.

SIRP helps organisations implement an intelligence-driven defense by focusing on addressing the fragmentation problem across information, people, technology, and process.

INFORMATION:

For relevant information to be refined into usable intelligence, it must be available to be correlated, enriched, and contextualised. You must remove the silos segmenting relevant data by creating a common source of record for it. SIRP does this by aggregating internal and external information so that it can be refined into intelligence usable for informing decisions. Internally sourced information, details of an IR investigation, notable events from the SOC, or even curated intelligence from an in-house team is often the most valuable part of the feedback loop SIRP enables.

PEOPLE:

Like data, the various functional teams within your security organisation (IR, SOC, Intel, Risk, Executives, etc.) also need the silos taken down from around them. They need access to relevant information from other teams, and intel sharing communities outside your organisation. They also need to be able to work seamlessly together with a dynamic workflow. SIRP facilitates this by allowing teams to provide tips and tasks to each other, create and funnel intelligence to relevant functional organisations, and create reports for executive decision makers based on threats to the organisation.

TECHNOLOGY:

Most organisations today have a very heterogeneous and disconnected set of point defensive technologies. For most, coordinating action across them means coordinating tickets between IT and various facets of the security team. SIRP enables organisations to coordinate intelligence-driven action and automation across our ever-growing library of applications and integrations

PROCESS:

Once you have removed the silos between information, people, and technology, SIRP enables you to streamline your processes with playbooks that leverage both internal and external intelligence to inform action for your teams and your technology as well as learn from past experiences.

VULNERABILITY ASSESSMENT TOOLS INTEGRATIONS

SIRP integrates with all top of the line vulnerability assessment tools to orchestrate and automate your vulnerability management program. SIRP automatically incorporates vulnerability data imported directly from different VA tools via API, delivering real-time cyber threat protection based on up-to-date situational awareness and comprehensive security analytics.

tenable RAPID7

Qualys. netsparker

These types of integrations combine comprehensive vulnerability management capabilities with SOAR to help security teams standardise their response processes, execute repeatable tasks at scale, and accelerate time to identify, analyse, remote, and remediate vulnerabilities.