Security Management Center

Why Your Security Operations Need this Productized Service

Get a consolidated view comprising of risk, reliability and efficiency of the infrastructure to understand your security posture

Traditionally, security infrastructure and components are managed using a hierarchical support model, with engineers and service desk team performing pre-defined set of activities. They are responsible for the upkeep of the infrastructure, management of the devices, handling of service requests, and reporting of service status as part of regular review with the stakeholders.

Various commercial tools and platforms are used to help in the operations. These are tools to monitor device availability or performance, scripts to automate generic tasks, along with service management platforms for ticket and workflow management in the operations process.

With the increase in the number of security products and the associated complexity, enterprises and service providers have started using orchestrators and compliance management tools to reduce the effort of managing these products, and to improve compliance of the infrastructure.

Despite the presence of these security tools and technologies, enterprises face cyber-attacks, and malware infections.

The main reason for the security gap is missing "security hygiene" of the infrastructure and limited visibility of infrastructure and associated service effectiveness.

A proactive and cohesive approach to security

Effective security service requires standardized infrastructure and components. It also stipulates the use of a platform that can provide the required set of services, yet be flexible enough to cater to any new or complex requirement. Hence, the concept of productized services is highly effective in ensuring service effectiveness and filling the gaps in traditional security operations.

Wipro's state-of-the-art Security Management Center (SMC), built on the principle of "Beat Before Beaten", has an integrated approach combining Predictive, Preventive and Proactive activities based on automation and analytics, which ensures a 360-degree business-oriented view of security operations and thus,

Eliminates any threat or vulnerability before it manifests

Increases ROI on the security infrastructure

Facilitates decision making at every level of the organizational hierarchy

SMC is a purpose-built security operations and orchestration product to help deliver managed security services. It offers operational insights, prioritization of risks, pre-integrated tools, short deployment time, reusable use cases, etc. to help enterprises attain operational maturity, thereby greatly reducing time-to-market.

Its unique proactive approach to provide insights into the security infrastructure gives organizations visibility into their security posture. Wipro uses Security Management Center to visualize the security infrastructure, holistically to view its customer's security posture.

The consolidated view comprises of risk, reliability and efficiency posture of the infrastructure. It delivers the richness of correlated data, aggregated information, and transparency related to the offered services.

Consolidated Security Posture	Insights into Security Ops.	Gather & Provide Evidence	Continuous View Of Compliance	Identify & Fix Persistent Issues
• Visualization of security operations & efficacy • Detailed view of security posture, risk, people awareness & process • Views for CISO, Risk Officers, Security Directors & Engineers	• Views to help for faster decision making & driving actions • Provide a detailed view of the security services & technologies • Meaningful reports which help understand the issues and risks	• Identify the issue with configuration of a device or system • Find the root cause of issue • Analyze & report repeated issues leveraging stored data collected over time • Offline reports in form of summary	• Repository of risks & prioritization based on the relevance • Compliance scores for regulatory standards, frameworks and baseline of customer • View of process adherence and closure of NCRs	• Trend of historical data to understand the improvement of a service, device or systems • Orchestrate use cases to derive relationships & identify possible fixes • Leverage bots integrated with use cases to remediate issues

Figure 1: Effective security operations with Security Management Center

SMC provides a unified view translating individual tool views/ reports into meaningful dashboards to stakeholders within the enterprise hierarchy. For instance, an executive view for the CISO shows whether any risks are manifesting due to ineffective or inconsistent application of security controls or if configurations are not meeting the baselines. Similarly, it provides an operational view to Operations Manager and a technology view to Analysts and Engineers.

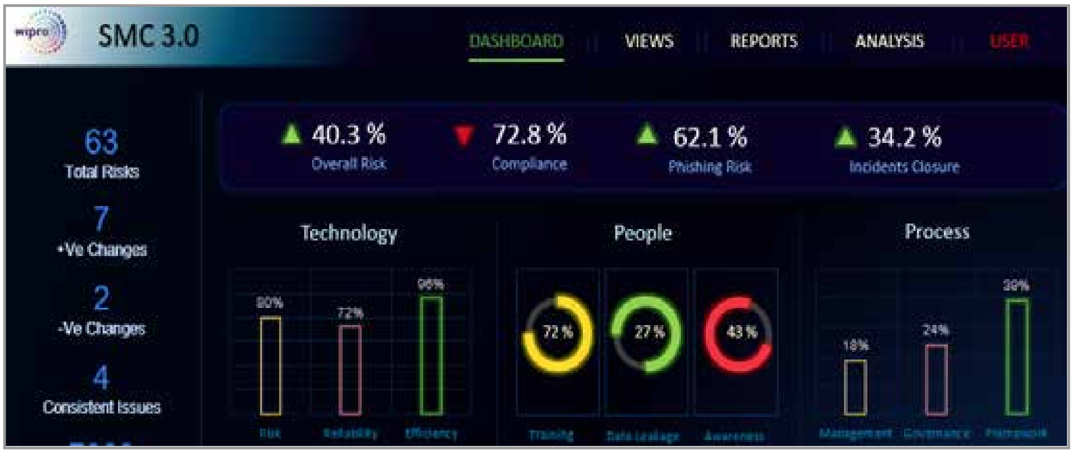
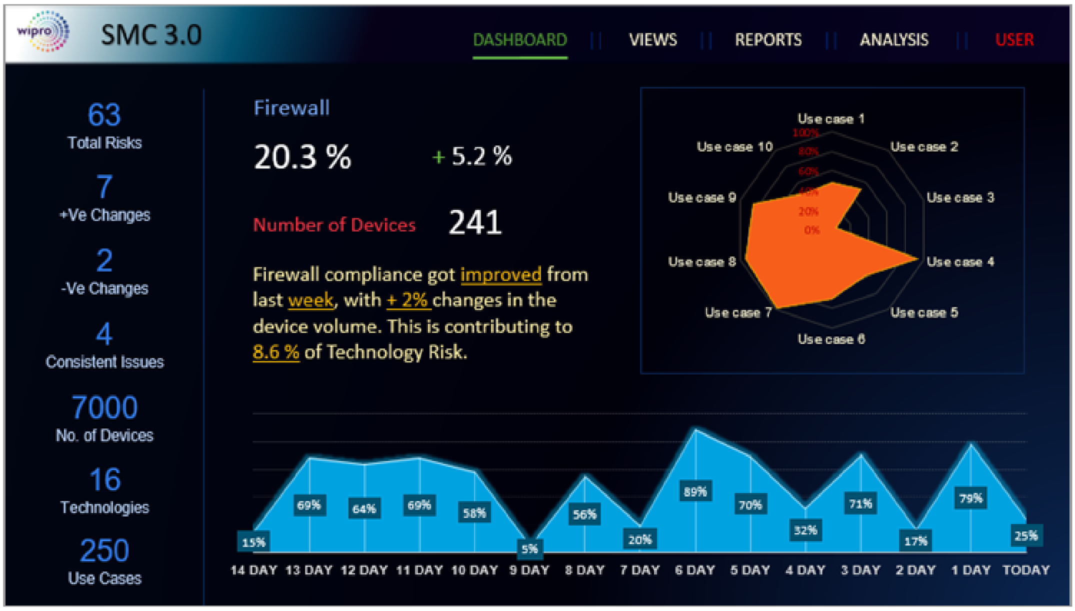


Figure 2: Snapshots of Security Management Center dashboards



63 Total Risks

7 +Ve Changes

2 -Ve Changes

4 Consistent Issues

7000 No. of Devices

16 Technologies

250 Use Cases

Firewall

20.3 % + 5.2 %

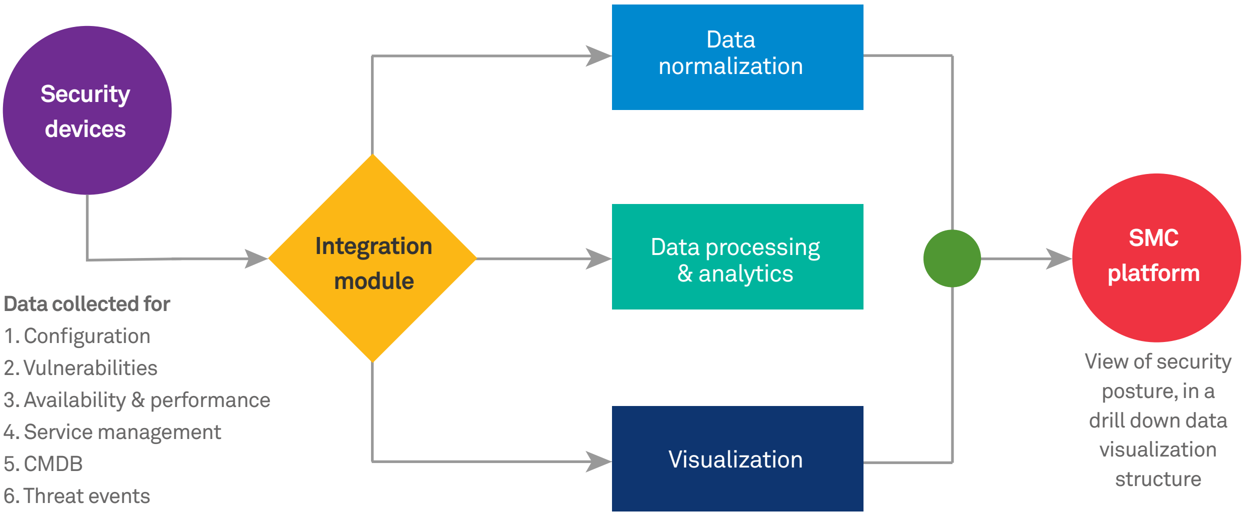
Number of Devices 241

Firewall compliance got improved from last week, with + 2% changes in the device volume. This is contributing to 8.6 % of Technology Risk.

Figure 2: Snapshots of Security Management Center dashboards

Security Management Center: Ensuring integrated visibility

SMC service architecture consists of multiple tools, collector and different data access methods using which the data is captured, correlated and aggregated to create the required views in the portal.



Data collected for
1. Configuration
2. Vulnerabilities
3. Availability & performance
4. Service management
5. CMDB
6. Threat events

View of security posture, in a drill down data visualization structure

Figure 3: Indicative diagram for SMC data flow

The architecture consists of a server hosting SMC platform with the data collection module, with IP connectivity to various security devices available in the infrastructure. The configuration of these security devices, are assessed using set of use cases defined as the baseline criteria. These use cases are derived from security frameworks, regulatory standards, vendor best practices and Wipro's experience. SMC integrates with these security devices using APIs to collect the required information.

The vulnerability management tool deployed at customer infrastructure is integrated to collect relevant information defined by pre-defined use cases. SMC integrates with orchestrator tools deployed at the customer's premise, which integrates with the firewall, load balancer devices to collect the configuration and rule bases, and access Firewall logs to analyze and create meta data content. The meta data is then sent to management server for further analysis. The service management tool hosted at customer data center is integrated with SMC using supported mechanisms and collect security operations ticket data in pre-defined time interval.

The health monitoring tool is hosted in the data center, which monitors the infrastructure security devices including firewall, load balancer, forward proxy, end point security management servers, etc. to collect health and performance related data, for analysis and reporting to SMC. The data gathered from all the above processes are then sent to the database of SMC platform, where it is further correlated and aggregated, to provide integrated visibility towards security infrastructure and security posture. SMC portal shows consolidated view of security posture as operational risk, efficiency and reliability view, with the capability to drill down to individual device status.

About the author

Angshuman Chattopadhyay

Infrastructure Security within Cybersecurity and Risk Services
Wipro

Angshuman Chattopadhyay is the Consulting & Solutions Lead for Infrastructure Security within Cybersecurity and Risk Services at Wipro. He brings extensive experience with over 19 years in IT and cybersecurity across a wide range of global roles.

Angshuman can be reached at angshuman.chattopadhyay1@wipro.com

Security Management Center visualizes service effectiveness and identifies operational security risks, helping prevent more than 70% of threats, along with visualizing ROI.

To know more or for a free demo, connect with us at cybersecurity.services@wipro.com

Wipro Limited
Doddakannelli,
Sarjapur Road,
Bangalore-560 035,
India
Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 180,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,
please write to us at **info@wipro.com**