happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

AUTOMATING CYBER RISK DETECTION AND PROTECTION WITH SOC 2.0

CONTENTS

INTRODUCTION

Digitalization has transformed the way business's function. With the evolution of technologies, attackers are also evolving. They are finding innovative and more invasive ways to attack organizations. Due to this, the organization's security operations center (SOC) is expected to be more agile and dynamic in detecting and responding to attacks. Most organizations' security operations and incident response teams are overworked due to high volumes of security threats and alerts that they need to manage every day. Often, tools & technologies employed are not efficient enough to isolate true positives, rather adding to the workload. As enterprises increasingly shift to cloud and hybrid environments with digital adaptation, SOCs need to be empowered with the right tools and strategies to address complex cyberattacks efficiently. They should be able to focus on priority initiatives with the help of technology. SOC and security incident response teams (SIRT) should look for ways to reduce time spent on repetitive, low-priority activities. They should build artificial intelligence and machine learning capabilities to become more efficient in handling security incidents.

KEY CHALLENGES FACED BY CYBER SECURITY MONITORING AND RESPONSE TEAMS

Managing the complex threat landscape with multiple security solutions can be overwhelming. Today, SOCs face a multitude of challenges.

INCREASED THREAT LANDSCAPE

The complexity of cyber threats and attacks in the form of malware, ransomware, phishing, and distributed denial of service (DDoS) is witnessing a significant rise. Effective, round-the-clock security monitoring becomes imperative, a challenge for many organizations.

SHORTAGE OF SKILLS

Having the right skills to identify and counter attacks is as important as deploying the right tools. While the demand for skilled staff is on the rise, organizations are facing a shortage of analysts with expertise in managing cyber threats and attacks. The number of unfilled positions continues to increase, and enterprises constantly struggle to hire the right people to maintain the balance of skill and technology.

INSUFFICIENT CYBERSECURITY BUDGET ALLOCATION

As most cybersecurity solutions help protect the organization and its stakeholders from the impact of cybersecurity breaches and attacks, justifying the budget and returns on investment (ROI) often becomes a challenge for security officers. In many organizations, budget allocations are made after experiencing a security breach.

COMPLEXITY IN REGULATORY COMPLIANCE

Organizations engage with multiple service providers or vendors to fulfill their cybersecurity requirements. However, they can face challenges linked to regulatory compliance. For example, a Europe-based organization may want specific information within the European Union, but this could be challenging if the service provider is US-based. Similarly, they may also have to meet other regulatory requirements like the GDPR, PCI, HIPA, etc., this again limits the organization's security teams in choosing the right service providers.

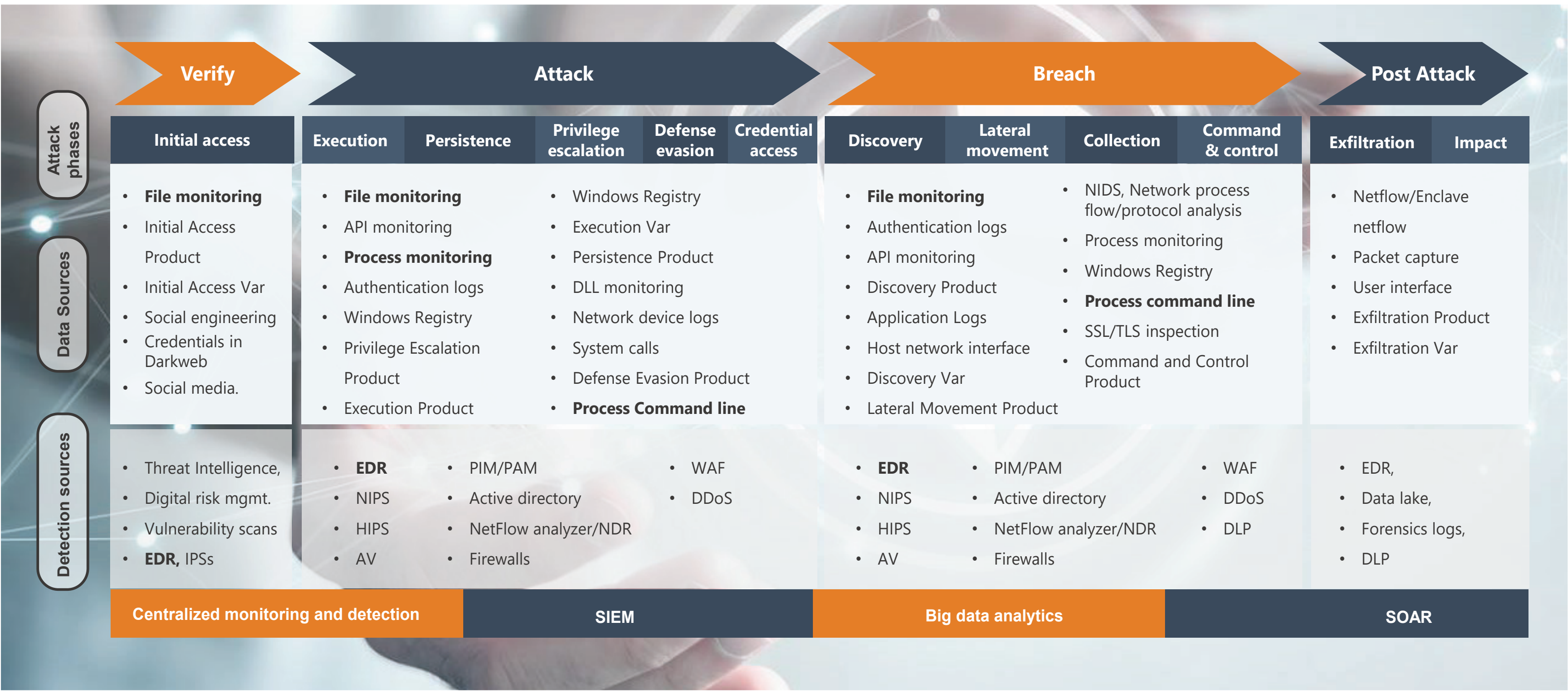
UNAWARE EMPLOYEES AND INSIDER THREATS

Many a time, there isn't enough awareness among employees about cybersecurity. There are multiple instances of employees becoming victims of phishing scams, virus attacks, etc., which affect the entire organization. These could have been avoided if they were more aware. Despite training programs, organizations are finding it challenging to drive situational awareness among their staff.

CLOUDIFICATION

With faster time to market or elasticity to accommodate business needs, the adoption of cloud technology has increased. Organizations are embracing different platforms such as Azure AWS etc., and SaaS platforms are also gaining popularity. Most enterprises are running a hybrid model. While keeping track of the digital footprint is a challenge, choosing security monitoring solutions that can seamlessly integrate with the hybrid environment and provide comprehensive coverage is another challenge.

CYBERATTACK AND DETECTION: ATTACK STAGES AND DETECTION TECHNIQUES

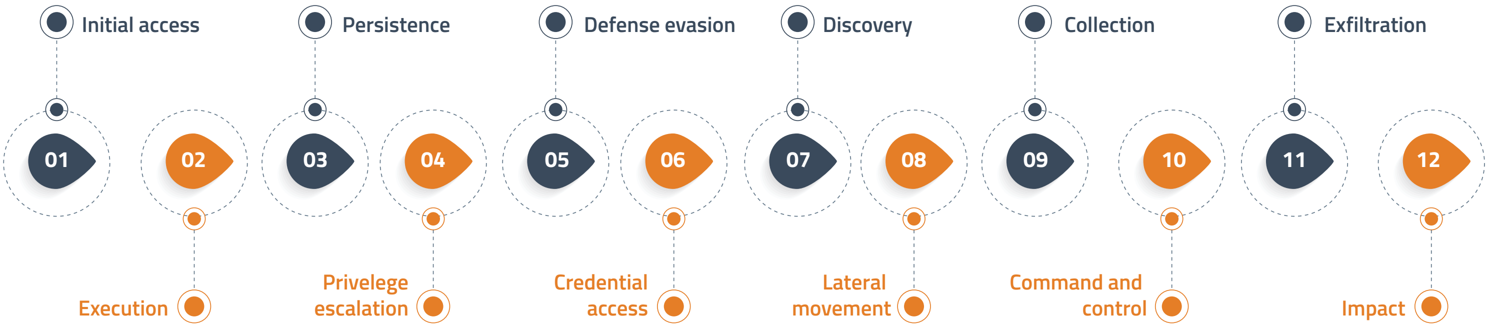


	Verify	Attack	Breach	Post Attack
Attack phases	Initial access	Execution Persistence Privilege escalation Defense evasion Credential access	Discovery Lateral movement Collection Command & control	Exfiltration Impact
Data Sources	**File monitoring** Initial Access Product Initial Access Var Social engineering Credentials in Darkweb Social media.	**File monitoring** API monitoring **Process monitoring** Authentication logs Windows Registry Privilege Escalation Product Execution Product Windows Registry Execution Var Persistence Product DLL monitoring Network device logs System calls Defense Evasion Product **Process Command line**	**File monitoring** Authentication logs API monitoring Discovery Product Application Logs Host network interface Discovery Var Lateral Movement Product NIDS, Network process flow/protocol analysis Process monitoring Windows Registry **Process command line** SSL/TLS inspection Command and Control Product	Netflow/Enclave netflow Packet capture User interface Exfiltration Product Exfiltration Var
Detection sources	Threat Intelligence, Digital risk mgmt. Vulnerability scans **EDR,** IPSs	**EDR** NIPS HIPS AV PIM/PAM Active directory NetFlow analyzer/NDR Firewalls WAF DDoS	**EDR** NIPS HIPS AV PIM/PAM Active directory NetFlow analyzer/NDR Firewalls WAF DDoS DLP	EDR, Data lake, Forensics logs, DLP
	Centralized monitoring and detection	SIEM	Big data analytics	SOAR

As per MITRE ATT&CK framework there are about ~200 techniques out of which 157 techniques use Process monitoring 90 use File monitoring, and 87 used by Process command line parameters

Cybercriminals utilize the latest tools and techniques to launch attacks on enterprises. To understand how attackers work, it is important to first understand the different stages involved in an attack and various techniques that will help detect the attacks. The MITRE ATT&CK framework contains exhaustive details of tactics and techniques used by cybercriminals to get into a network. The framework lists multiple phases involved in a cyberattack.

Organizations need to have the required data sources/toolsets to identify suspicious activity/ behavior at different stages, which help detect security incidents efficiently. Most organizations may not have an exhaustive list of data sources to identify an attack in every phase. Still, It's important to identify what solutions or tools in your environment can help you do that and establish a road map to bring those technologies that could enhance your detection capability.



For example, the team may fail to detect the initial access phase, where a user clicks on a link that installs a program on the user's machine. However, as the attack progresses and there's a lateral movement where the machine is trying to communicate with another machine, the SOC team may detect suspicious behavior and the possibility of an attack based on the available data sources.

Another example could be, under process monitoring, if new .exe or any other new file gets installed on a system, an additional process gets added to the overall processes list. An alert is generated so the team can monitor if it is a required process.

Attack phases	Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Command & control	Exfiltration	Impact
Data Sources	• **File monitoring** • Initial Access Product • Initial Access Var • Social engineering • Credentials in Darkweb • Social media.	• **File monitoring** • API monitoring • **Process monitoring** • Authentication logs • Windows Registry • Privilege Escalation Product • Execution Product		• Windows Registry • Execution Var • Persistence Product • DLL monitoring • Network device logs • System calls • Defense Evasion Product • **Process Command line**			• **File monitoring** • Authentication logs • API monitoring • Discovery Product • Application Logs • Host network interface • Discovery Var • Lateral Movement Product		• NIDS, Network process flow/protocol analysis • Process monitoring • Windows Registry • **Process command line** • SSL/TLS inspection • Command and Control Product		• Netflow/Enclave netflow • Packet capture • User interface • Exfiltration Product • Exfiltration Var	

Now, for the SOC team to detect such incidents, they will need appropriate information in their central security monitoring tool. They will need technologies that can identify such occurrences either on the system or in the infrastructure and forward them to the SOC platforms, so they can be acted upon.

WHAT TOOLS HELP IDENTIFY CYBERATTACKS EFFICIENTLY?

The most common security tools are firewalls, anti-virus, IPS, etc, detecting security alerts and also offering a layer of protection. In some cases, the logs from the active directories or servers are also collected on the SOC platform to report certain anomalies. But clearly, they are not sufficient to handle sophisticated present-day attacks. It is important to cover all data sources and address attacks with a modern security framework, SOC 2.0.

In addition to all capabilities of a traditional SOC, Happiest Minds' SOC 2.0 includes different types of technologies essential for security monitoring. While security information and event management (SIEM) and security orchestration and automation (SOAR) continue to be the central aggregation and correlation platforms, there are other solutions to facilitate effective security monitoring:

An endpoint detection and response (EDR) tool, is now one of the essential components in the overall security detection and monitoring architecture

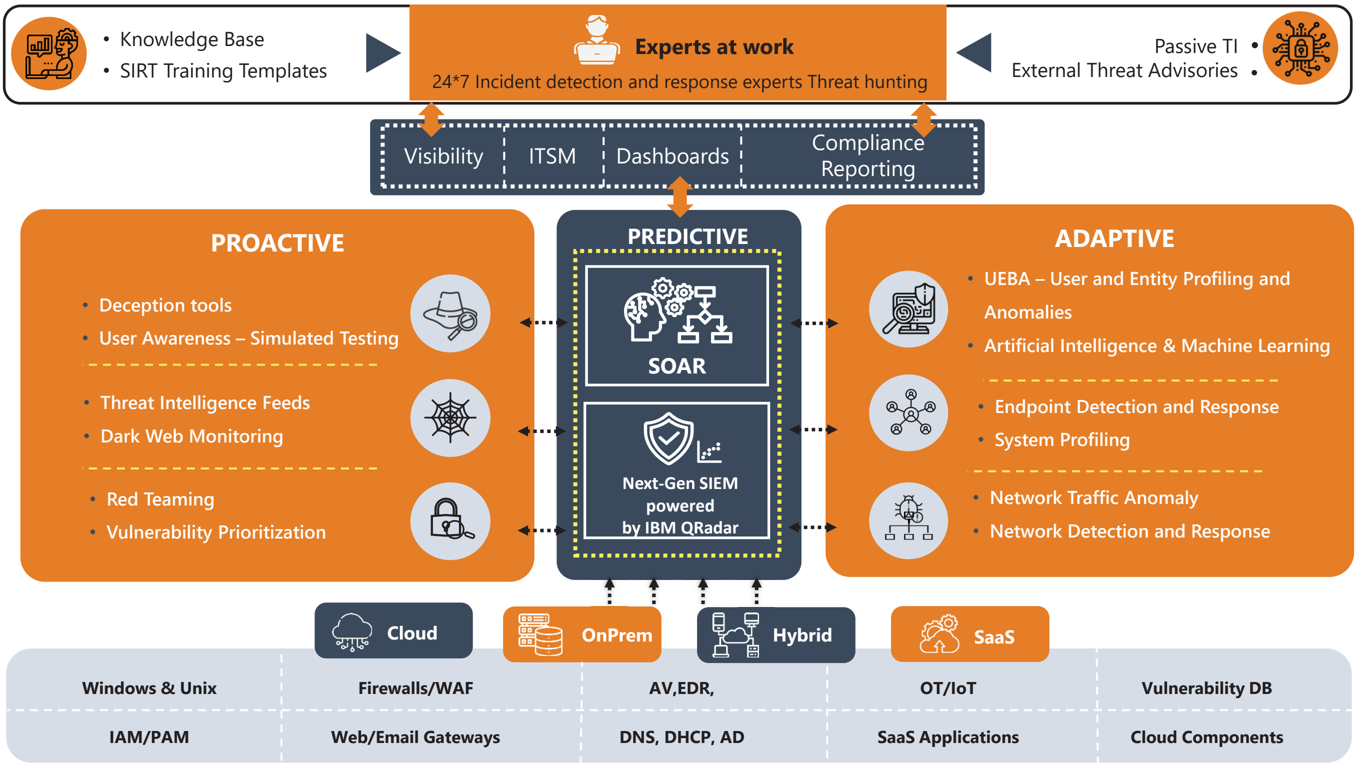
A network detection and response (NDR) solution to tap flow data and traffic patterns on the network and detect anomalies

Artificial intelligence and machine learning (AI/ML) to address complex threats and attacks base on behavioral analytics

Proactive usage of the vulnerability database in the client environment for incident prioritization

Dark web monitoring to identify potential leakages (Data, Credentials, Ips, Source codes) which could be weaponized against organizations threat trends in similar industry verticals, information around indicators of compromise(IOC) and common vulnerabilities being exploited by hackers

HAPPIEST MINDS CYBER RISK PROTECTION PLATFORM (CRPP): SOC 2.0 ARCHITECTURE



CRPP offers integrated threat detection and response across multiple layers of enterprise IT, removing a siloed approach to security. The easy plug-and-play methodology has been developed to suit clients' unique business requirements. Happiest Minds' SOC 2.0 architecture comprises three blocks — Proactive, Predictive, and Adaptive.

PROACTIVE

Proactive dark web monitoring helps organizations pre-empt possible attacks. The Proactive block helps detect possible weaponization against a company or its peers early.
Global threat intelligence-based correlation can detect true positives and enable right effort channelization. Threats can be prioritized based on vulnerabilities that organizations may be exposed to. Proactive threat simulation helps check the effectiveness of security controls, detection tools, and the response process. Simulated phishing and vishing techniques help educate and strengthen the weak links within the organization.

Deception: SOC 2.0 uses deception to lure cyber criminals to attack their enterprise network, giving attackers the impression that they have landed and are in a position to attack. This helps detect the possibility of an attack and understand the techniques that attackers are deploying. Based on the learnings, they can deploy preventative controls and countermeasures to mitigate real attacks in the future.

Cyber resiliency and vulnerability assessment prioritization: Most enterprises perform penetration testing, vulnerability assessments, etc., on a monthly or quarterly basis. However, derived insights are utilized only for patching remediation. The information can also be consumed for effective security monitoring. SOC 2.0 collates information from customers and correlates it with Threat intelligence and dark web findings to get an idea of available tools, malware, exploits, etc. An organization could be exposed to and preempt a possible breach. SOC 2.0 can thus help enterprises proactively detect and mitigate attacks at an early stage.

ADAPTIVE

A lot of advanced (and maybe critical) threats deceive existing controls, antivirus, firewalls, IPS, and other such solutions. Quite a few organizations have security controls only for their data centers. These enterprises also trust certain employees with access to critical systems and confidential information in the enterprise environment. However, adaptive, or behavior-based analysis comes into play when such an employee's machine gets compromised without the user's knowledge, a scenario of a potential insider threat. The Adaptive block leverages user and entity behavior analytics (UEBA) to detect and address threats.

For example, an access request for a user based out of a specific location — and operating out of just two locations (office and home location) in a particular city — cannot come in from a different country suddenly. In such instances, the Adaptive block helps identify advanced threats through behavioral analytics. Generally, vendors dealing with antivirus, firewalls, and IPS are unable to identify such persistent threats or a case of zero-day threats. However, the Adaptive block in SOC 2.0 effectively identifies these advanced, zero-day threats that haven't been seen before and do not match any known malware signatures. Solutions like the EDR, NDR, and UEBA help in profiling users, entities, and networks based on their behavior, sending out alerts when there is an anomaly.

Early adoption of artificial intelligence and machine learning techniques helps understand the organization's environment and detect anomalies. UEBA, EDR, and NDR bring these detection capabilities to profile systems, networks, users, and entities to identify zero-day and advanced threats in the environment.

PREDICTIVE

IT security teams rely on logs generated via integration with SIEM platforms. This typically leads to a high volume of alerts, and a lot of time is spent qualifying the alerts into security incidents. Most of the time, SOC teams do not have the bandwidth to address all of the alerts and incidents. Due to this, almost always, a few advanced threats that cause the highest level of damage to organizations get missed out. Also, getting the right level of skills required to address this issue has been an even greater challenge.

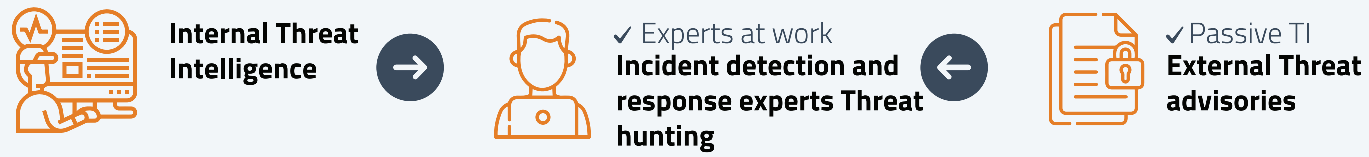
In a traditional SOC, triaging of an incident where an attack is launched from a specific location is detected, the source's credibility will have to be identified. The engineer will need to go to a threat intelligence forum or a threat intelligence platform and validate the authenticity of the threat. If the threat is genuine, the engineer will email the company's IT security team, who will put that IP address to blocklist on the firewall. This is the typical sequence of steps in a security incident triaging and response. The first 20-30 minutes are lost in identifying or qualifying the incident. The next 20 minutes would go into raising a ticket and notifying the security administrator. The security administrator would then raise a change request and wait for a few hours (unless it is an emergency) or days based on the SLA. A lot of precious time is lost. Then, there's the possibility of missing attacks due to manual monitoring, especially when alert volumes are high.

While identifying and qualifying these security incidents is a challenge, responding poses a bigger challenge. It may consume the time of other teams too.

Happiest Minds SOC 2.0's next-gen SIEM seamlessly integrates with on-prem, cloud, SaaS, and hybrid environments. Well-defined MITRE ATT&CK TTP-based alert mapping ensures extended and accurate detection coverage, eliminating many false positives. These are further aggregated and normalized through Happiest Minds' security orchestration and automation (SOAR) platforms. The SOAR platforms address most of the efficiency and skill gaps in the environment. With their ability to integrate with some of the essential infrastructure components, they can mimic the actions of a security analyst at machine speed and help in qualifying a lot of the security incidents. All of the process workflows that security analysts typically follow are eventually converted into standardized workflows. This not only helps in automation but also in standardizing the overall security monitoring and detection process.

These SOAR platforms possess the ability even to send responses back to devices like the EDR, active directory, firewalls, proxies, and email gateways, enabling response at machine speed. SOAR in SOC 2.0 automates the complete workflow. The moment there's an alert from SIEM, SOAR automatically verifies the IP address. If it is listed as a blacklisted IP, it directly goes back to one of the integrated devices (AV, IPS, FW, etc.) and adds to the blocklists there. This collaborative approach forms the managed detection and response service.

CYBER RISK PROTECTION CENTER (CRPC)



Internal Threat Intelligence →

✓ Experts at work
Incident detection and response experts Threat hunting

← ✓ Passive TI
External Threat advisories

The Cyber Risk Protection Center (CRPC) is where Happiest Minds subject matter experts (SMEs) are active or operational. The team constantly accesses the central monitoring /SOAR platform. Once an incident is detected, it will be investigated, and all relevant information required will be gathered to support the investigation and list out possible containment and remediation strategy. For cases that have automation workflows associated, they will also cross-verify the SOAR platform's analysis for accuracy and validation, which may be used to finetune the playbook further.
The team constantly updates and finetunes its use cases and workflows to make the security detection and response as accurate as possible. The shared team works with multiple customers. Hence there is a good understanding of trends across customers which a customer can benefit from. Happiest Minds' SOC 2.0 analysts work with multiple clients across different industry verticals. The shared team benefits from information that it gets through its different customers. Hence, these analysts have wider exposure to security issues and can address them faster and more efficiently. Their vertical knowledge, best practices, and intelligence can benefit customers as the team proactively applies it to all of them. The experts at work also subscribe to multiple threat advisories. They constantly look for new advisories and new kinds of exploits happening across the globe. Hence, the team is well-informed, makes decisions much quicker, and recommends quicker fixes to customers.

Happiest Minds is deeply invested in periodic training and skill enhancement of SMEs. Lessons from the multitude of incidents being addressed are well-documented and used for training. Additionally, Happiest Minds has an internal training academy that focuses on requirement-based skills training through internal and external trainers. A Cybersecurity Centre of Excellence, comprising a team of experts, provides extended platform engineering support, IR retainer service, and periodic internal training.

HOW DOES SOC 2.0 ADDRESS CHALLENGES THAT CUSTOMERS FACE?

Through automation, AI/ML, multi-environment integration, and a shared services framework, SOC 2.0 effectively addresses all challenges related to the increasing threat complexity, dearth of people and skills, cost efficiency, and more.

INCREASING THREAT LANDSCAPE

Happiest Minds SOC 2.0 framework provides a comprehensive solution with extensive coverage of data sources essential for detecting and responding to advanced threats, insider threats, zero-day attacks, etc., at machine speed. This helps customers focus on the actual threats and streamline efforts in addressing true positives.

INSUFFICIENT CYBER SECURITY BUDGET

If all the features and capabilities were to be deployed by an organization, it would require a significant investment. However, as Happiest Minds extends its SOC 2.0 services in a managed security services model, customers can leverage the features and benefits of the platform and shared model at a minimal cost. They can pick tools, components, and modules from the architecture based on their requirements through a SaaS and modular approach. Customers have greater efficiency while saving costs, which helps security officers get budget approvals by sighting its value proposition.

SHORTAGE OF SKILLS

If an organization must set up the SOC 2.0 environment independently and run a 24/7 SOC service, it will need a handful of security analysts. A few more experts would be needed to accomplish the task. However, Happiest Minds' shared services model leverages the efforts of the same set of skilled analysts and experts for multiple engagements. Hence, there's cost efficiency while filling in the gap of having the right skillset. Secondly, any organization having 5-10 cyber security analysts and experts will face challenges when one or more members of the team are unavailable (due to work leaves, resignations, etc.). However, the SOC 2.0 shared model has a larger skilled team with sufficient back-up, and organizations availing these services needn't worry about business continuity and skills shortage.

MULTI-PLATFORM ENVIRONMENT

SOC 2.0 covers the entire ecosystem — gathering information from and securing the cloud, on-premises, SaaS as well as the hybrid environment. All solutions under SOC 2.0 can be deployed on-premises or on the cloud. It is an elastic, highly scalable, cloud-based model.

OTHER BENEFITS:

SOC 2.0 offers a host of other benefits to organizations:

- Regulatory compliance in terms of geography as well as overall log retention requirements
- SOC monitoring with greater maturity from day one with a proven managed security service provider (MSSP) program built and engineered over the years
- Proactive reporting on the organization's information presence in the dark web
- Contextualized threat intelligence with fewer false positives
- Standardization of processes and procedures through automation
- Faster time to detect and respond through orchestration and response automation
- Comprehensive security and management that narrows time to detection and resolution from days, weeks, or months to hours, minutes, or even seconds
- Plug-and-play services to existing SOC — enhancement with automation, SOC enrichment with dark web monitoring feeds, EDR, etc

FINAL THOUGHTS

Organizations must move away from traditional methodologies and become more proactive and adaptive in addressing the ever-evolving threat landscape. They must constantly update and evolve to achieve projected growth and expansion. Security officers must make security an enabler and give confidence to the business. SOC 2.0 provides such an approach that security managers can quickly leverage and enhance their overall security posture while efficiently tackling all the challenges. SOC 2.0 offers efficiency gains and an early ROI. Analysts and experts are freed up from mundane tasks to focus on processes that need their expertise. There is better visibility, faster threat and attack detection, and steady processes and workflows.

AUTHOR BIO

Anand Kumar brings in more than 16+ years of experience in IT Security across multiple domains like Advanced Security Monitoring Services, IOT/OT Security, Data Security, Cloud Security, and Infrastructure Security. Before joining Happiest Minds, Anand has worked with HCL Technologies in different roles/initiatives for its Cyber Security Services, like large Security Transformation, Security T&T head for the UK, Security Solutions Head for EMEA, and more. At Happiest Minds, Anand is working on building new services and business development of Cybersecurity practice. His recent work includes establishing SOC 2.0 services, retail-specific security services, building Security Automation, and Collaborative Threat Intelligence as services for seamless consumption by customers. It is currently focusing on developing Cloud Security Framework and OT Security and its integration with IT. Anand is an Engineering graduate from BIT-Bangalore, India. Anand is very passionate about motorcycles; he loves traveling, cooking, painting, and Netflixing when not working.