NTT Communications
Transform Transcend

netmagic®
An NTT Communications Company

SECURITY OPERATIONS CENTER

TO BUILD OR OUTSOURCE?

Rishikesh Kamat
Associate Vice President
Products & Services, Netmagic

Is your security strategy similar to the 'whack-a-mole' game? Threats pop up in one hole and once you've addressed them, they pop up somewhere else. If so, how can your organization shore up its defenses and build a resilient security practice?

A Security Operations Center (SOC) helps organizations stay abreast of the ever-changing threat landscape while safeguarding them against unauthorized malicious activity in real time.

A SOC is made up of an organized and specialized team that constantly monitors and bolsters the security posture of an organization while preventing, detecting, analyzing, and responding to cyber security incidents. This is enabled with the help of technology and well-articulated processes and procedures. Built on the pillars of people, process, and technology, a SOC is evidently a prudent step that organizations can take for maintaining a strong security posture.

If building a captive SOC is on your agenda, you need to invest in specialized resources over a long-term period, which means huge investments in building up infrastructure and hiring specialists. Hence, the bigger question organizations now face is whether to build on their own or outsource it to the experts with access to a deep and wide talent pool in security.

BUILD OR OUTSOURCE

Most CIOs face this question for most of their IT decisions. However, the domain of security adds its own layer of complexities when it boils down to such decision-making. Like most of the other technology decisions, selecting the right model for SOC is no different. The decision to opt for any of the SOC models – in-house, outsourced (as a Service) or hybrid – is a tough one.

Needless to say, it requires a well thought out strategy and a judicious planning. CIOs need to arrive at a decision, keeping in mind their organization's specific requirements.

Let's understand what each decision entails.

IN-HOUSE SOC

An in-house SOC model is usually adopted by organizations that have compliance issues with respect to outsourcing or see outsourcing as a perceived risk that could affect the integrity and functioning of their business.

An immediate advantage of building your own SOC is the realization of the expertise of your in-house staff and the very fact that they know the organization and its environment much better than a third-party security service provider. They are aware of the interdependencies between the different departments and their requirements and can address highly specific requirements efficiently. To have a robust security infrastructure, it is the responsibility of the CISO to hire a team of experienced solutions architects, then build out an operations team and deploy technology experts.

The downside to this approach is that the up-front expenditure of building a SOC in-house is considerably high as compared to an outsourced or shared one. It will take years for an organization to realize the RoI on the CapEx with respect to licensing of SIEM tool, threat intelligence and setting up the infrastructure. Moreover, finding experienced SOC analysts or managers to man the SOC will be difficult as these professionals are not easy to find. Security is a domain where constant knowledge sharing is one of the key levers to successfully prevent attacks. A captive SOC performs like an island in itself. Even if the organization has been able to deploy the best of people and technologies, the inability to connect with a larger ecosystem can lead to a serious knowledge gap.

That said, today, third party security providers are engaging with organizations as consultants and helping them build in-house SOC. These consultants take care of the framework, technology selection, process, and skill sets thus making a captive SOC implementation easier.

However, any organization seeking to build its own SOC from scratch must answer whether it has the appropriate in-house skills and knowledge to man and operate the SOC, to begin with.

OUTSOURCED SOC

Building an in-house SOC can prove to be a cost-prohibitive proposition. It involves setting up of the infrastructure grounds up. Besides, hiring security experts to manage it can be an onerous task. That's primarily the reason an organization considers taking the help of a Managed Security Service Provider (MSSP).

In an MSSP model, the service provider provides the infrastructure, intelligence and other capabilities. An experienced service provider has a state-of-the-art security infrastructure (core competency) that provides rich threat intelligence to detect real time sophisticated and targeted attacks. They already have a team of trained and experienced security analysts who are well conversant with most of the security threats that an organization may face. And, by the virtue of their engagements with multiple clients, they are equipped with state-of-the-art tools, as well as, a sound knowledge about possible security threats and incidents (both current and evolving). Hence, the costs are lower than an in-house solution.

One of such progressive technology solutions is Netmagic's Comprehensive Network Attack Monitoring (CNAM) tool, which is a real-time monitoring solution that fortifies IT infrastructure from security threats and vulnerabilities. It is a fully managed SIEM solution with a SOC team that manages the operations round the clock. Available as a SaaS model, CNAM collates information from multiple devices and applies intelligence to identify suspicious activity across the spectrum. CNAM allows for intelligent sharing of threats across multiple customers without divulging any customer specific information.

Besides CNAM, the Automated VAPT (Vulnerability Assessment and Penetration Testing) is a hybrid solution which blends automated testing with security expert analysis. This blended model provides the best quality test coverage while accelerating the test time. The unique technology identifies all possible attack vectors.

Another important advantage of opting for an MSSP is the time factor. Typically, an MSSP takes a shorter time to get the SOC operational. With the experience of working with multiple clients, an MSSP is experienced to onboard new clients and customizing the solution offering quickly and reliably for their needs.

However, a concern with an outsourced SOC model is that the log data and incident data are stored with the MSSP. In a worst-case scenario, this data can be lost or misplaced or misused. Another concern related to an MSSP model is the fact that a third-party is made aware of your network's vulnerabilities. Much depends on the selection of a credible service provider, the non-disclosure agreements that your organization signs with the service provider, the architecture of the tools deployed by the service provider and well-defined Service Level Agreements (SLAs) between you and the service provider.

If you choose to go for an MSSP model, there are a few things that you should consider:

a. The reputation of the service provider for protecting critical assets and the ability to respond swiftly,

b. Technologies/tools/approaches to data protection and the level of security at their SOC,

c. The experience of the staff managing the SOC,

d. Background checks and any reference customers that you may speak with before signing on the dotted line.

HYBRID SOC

In essence, a hybrid SOC is a combination of the above two models. Under this model, the organization, and the MSSP come together and share synergies for technology, processes, expertise, facilities and personnel resulting in substantial cost savings. It is of utmost importance in this kind of an arrangement is to have an overall strategic plan for the operating model, define roles that are tactically delivered by partners, and build capabilities and maturity that leverage the ecosystem. With MSSP, your security moves beyond individual devices to being managed and controlled from a centralized SOC.

Whether your organization is considering investing in a SOC for the first time or seeking to evolve an existing SOC infrastructure, the decision has to be made factoring in all the elements. Choosing the correct model to go for is not about implementing a single solution but implementing the right solution mix for your organization's unique requirements.

The right choice will enable your organization to address any security concerns (based on correlated, contextual data), incidents and breaches in a timely fashion. It also helps you stay a step ahead with a stable and robust platform for risk reduction.

And, it surely helps you experience peace of mind, while enabling you to focus on your core competencies.

About Netmagic (An NTT Communications Company)

Netmagic, an NTT Communications company, is India's leading Managed Hosting and Cloud Service Provider, with 9 carrier-neutral, state-of-the-art data centers and serving more than 1500 enterprises globally. A pioneer in the Indian IT Infrastructure services space - it was the first to launch services such as Cloud Computing, Managed Security, Disaster Recovery-as-a-Service and Software-Defined Storage. Netmagic also delivers Remote Infrastructure Management services to NTT Communications' customers across Americas, Europe and Asia-Pacific region.

Netmagic is India's only IT Infrastructure services provider to be PCI DSS certified for its entire suite of services. It is also the first cloud service provider in India and in the world, to receive the CSA STAR certification for Cloud Capability Maturity Model (CCM) version 3.0.1, an industry benchmark for the specific security requirements of multi-tenant service providers. Besides this, Netmagic is also empanelled as an IT Security Auditing Organization with CERT-In (Indian Computer Emergency Response Team).

Netmagic was chosen by India's CIO community for 6 awards at the recent CIO Choice Awards 2016, across categories for Data Center and Cloud services. Prior to that, it was awarded the 'Data Center Service Provider of the Year' and 'Infrastructure as a Service Provider of the Year' by Frost & Sullivan at India ICT Awards 2015. Netmagic was also mentioned in Gartner's 2015 Magic Quadrant Report for Cloud-Enabled Managed Hosting, Asia/Pacific, where NTT Communications was named in the Leader quadrant. The mention was a result of the analyst firm's assessment of NTT Communications' Cloud services portfolio, which included Netmagic's Cloud services.

To learn more, visit us at: www.netmagicsolutions.com

Netmagic is committed to providing world-class and customized IT Infrastructure solutions that enable our customers to 'Rethink' the way they configure IT.

DATA CENTER SERVICES

• Colocation • Bandwidth
• Remote Hand Support

CLOUD SERVICES

• IaaS-based Public / Private / Hybrid Cloud
• DR On Cloud • Object / Performance
• Tiered Storage (NTSS) • DBaaS

INFRASTRUCTURE APPLICATION

• Exchange • Linux Email
• SAP Basis • Middleware

HOSTED IT INFRASTRUCTURE

• Dedicated Hosting • Pre-provisioned Servers
• Managed Firewall • Load Balancing
• Backup And Storage • Disaster Recovery
• DRaaS • Data Center Consolidation
• Data Center Migration

MANAGED SERVICES

• 24x7 Infrastructure Monitoring
and Management of OS, DB, Network and App
• WebControl • CNAM and VAPT
• Remote DC Management • SecureAT
• MDDoS • SOC • SSL Certification
• Managed IPS/UTM

NETWORK SERVICES

• Domestic MPLS/IP VPN
• Domestic NFV based services
• ILD - VPN, Internet

The 2016 Frost & Sullivan India ICT Awards

'Infrastructure as a Service Provider of the Year'

CIO Choice Awards 2017

Public Cloud | Private Cloud | Hybrid Cloud
Data Center Managed Services Provider | Disaster Recovery as a Service

marketing@netmagicsolutions.com | www.netmagicsolutions.com
Twitter: @netmagic | LinkedIn: @Netmagic Solutions | YouTube: Netmagic Solutions
Facebook: Netmagic Solutions

FOR FURTHER DETAILS PLEASE CONTACT
1800 103 3130