WHEN TO LOOK FOR AN EXTERNAL SOC

By Sachin Bhardwaj, director, Marketing and Business Development, eHosting DataFort

A security operations centre (SOC) is an external control room that houses a team responsible for monitoring and analysing an organisation's security profile on a continuous basis. The team's goal is to detect, analyse and respond to cybersecurity incidents using a blend of their skills, technology solutions and a set of well-established processes.

Without exception, security operations centres work closely with an organisation's incident response teams to ensure incidents detected are addressed and controlled without delay. The security operations centre tracks anomalous activity on endpoints, networks, servers, databases, applications and websites, and is responsible for identifying, analysing, defending and reporting such threat incidents.

An external security operations centre focuses on the day to day operational component of enterprise information security. This allows the in-house security and IT teams to focus on developing and improving security strategy, designing the security architecture, and implementing latest protective measures. However, security operations centres can also provide advanced services such as forensic analysis and reverse malware engineering to analyse the source, points of intrusion, and modus operandi of threat incidents.

Integrating the role and services of an external security operations centre requires getting the right balance in preventive, detective and reactive security roles as well as access to its threat intelligence capabilities. This can be driven by an objective and proactive assessment and audit procedure or through the experience of painful and damaging historical incidents, including breaches and compromises.

An important step in integrating the services of an external security operations centre is to identify business specific goals and include senior management and business heads as well, in the build-up process. Incorporating the role of an external security operations centre requires an internal gap analysis, detailing a list of milestones to be achieved based on the gap analysis, and an incremental budget spending approach as well.

The security operations centre will also need to communicate and coordinate with internal points of administrative control, such as first responders, public relations, and other identified points of control.

An external security operations centre can provide services built through integration of threat intelligence, security monitoring, incident response, security analytics, to manage advanced persistent threats on the network, endpoint threat detection and data exfiltration. Security operations centres typically blend skilled people resources into processes and use the latest technologies to provide business focused compliance and service level agreements.

A key benefit from the services of an external security operations centre is its uninterrupted and round the clock ability to build up a baseline profile of normal activity by monitoring users, applications, infrastructure, network and other supporting systems. The inability to establish such a normal baseline of activity is a common obstacle that enterprises face in being able to issue credible alerts over false positives.