It typically takes 229 days for an Enterprise to detect a resident Advanced Persistent Threat?

Enterprises going digital has hastened the shift to cloud computing, made access through mobile devices ubiquitous and increased the adoption of Internet of Things (IoT). These developments have led to the attack surface being broadened significantly and defense becoming more complex. When you combine a massively distributed fleet of autonomous devices that are capable of making decisions and directly affecting the physical state of people and things, you have a considerable risk to manage. This is not a scenario that most enterprises are familiar with managing. To add to these problems, it has been consistently seen that around 50% of cyber breaches are caused by deliberate malicious actions or mistakes inadvertently made by internal employees and partners. Other issues like regulatory compliance pressure and the problems associated with hiring and retaining appropriately skilled engineers makes managing these cyber security challenges more difficult.

In order to maintain a constant vigil of clients’ applications, networks and systems and to protect them from the ever-changing threat landscape, Infosys offers Cyber Next - Platform-Powered Service Ecosystem. Cyber Next is a modern stack of commercial and open source technologies powered by in-house, home grown research and well tested IP and use cases. It is a suite of integrated ready-to-consume hosted platforms, supported by proprietary use cases, reporting and analytics. Our MSS allow customers to attain swift maturity in their cybersecurity posture enabling compliance, effectiveness, resilience and time-to-value. It presents an effective and efficient management of assets, incidents, threats, vulnerabilities and risks with a unified view for quick decision making.

With Cyber Next, we bring the power of technology and cybersecurity excellence to our customers to fulfil the promise of securing their future.
Component - Cyber Next Platforms

These platforms ensure comprehensive security at any given point in time and are handled and deployed by highly skilled security analysts in our niche global distributed Cyber Defense Centre (CDC) network.

Benefits

- Reliable IT infrastructure and systems leading to interruption free business operations for the enterprise
- Access to a range of on-demand SLA based Managed Security Services leading to minimized cybersecurity risks and reduced costs of compliance
- Availability of real time dashboards and reports providing insights on a range of key cybersecurity metrics on a regular basis
- Trusted advisory services to keep the enterprise up to date to prevent cybersecurity breaches
- End to end services handled in a unified manner providing peace of mind to stakeholders

Case Study

Customer Profile:
The client is one of the leading transportation and logistics company of Australia having extensive global logistics network across 1,200 locations in more than 50 countries and Data Centers spread across Australia, China, Singapore and USA. The client wanted to engage with a vendor who could implement a complete security program for them as the current landscape lacked security monitoring and threat detection capabilities leading to higher risks.

Challenges:

- Complex IT environment spread across multiple geographies and transformation of Data Centre happening simultaneously
- Lack of security monitoring and no clear inventory of log sources and security devices

Solution:

- Implemented Cyber Watch based solution - provided deeper analytics capability by examining risks in context and understand behavior
- Enhanced scalability to cater to changes in the scale of infrastructure
- Built a single pane of glass view, enabling decision-support across many job streams
- Aligned team services and provided operational leverage (24x7)
- Defined architecture so data remains within the organization and Geo boundaries

For more information, contact askus@infosys.com