INFOSYS CYBER WATCH

Infosys®
Navigate your next

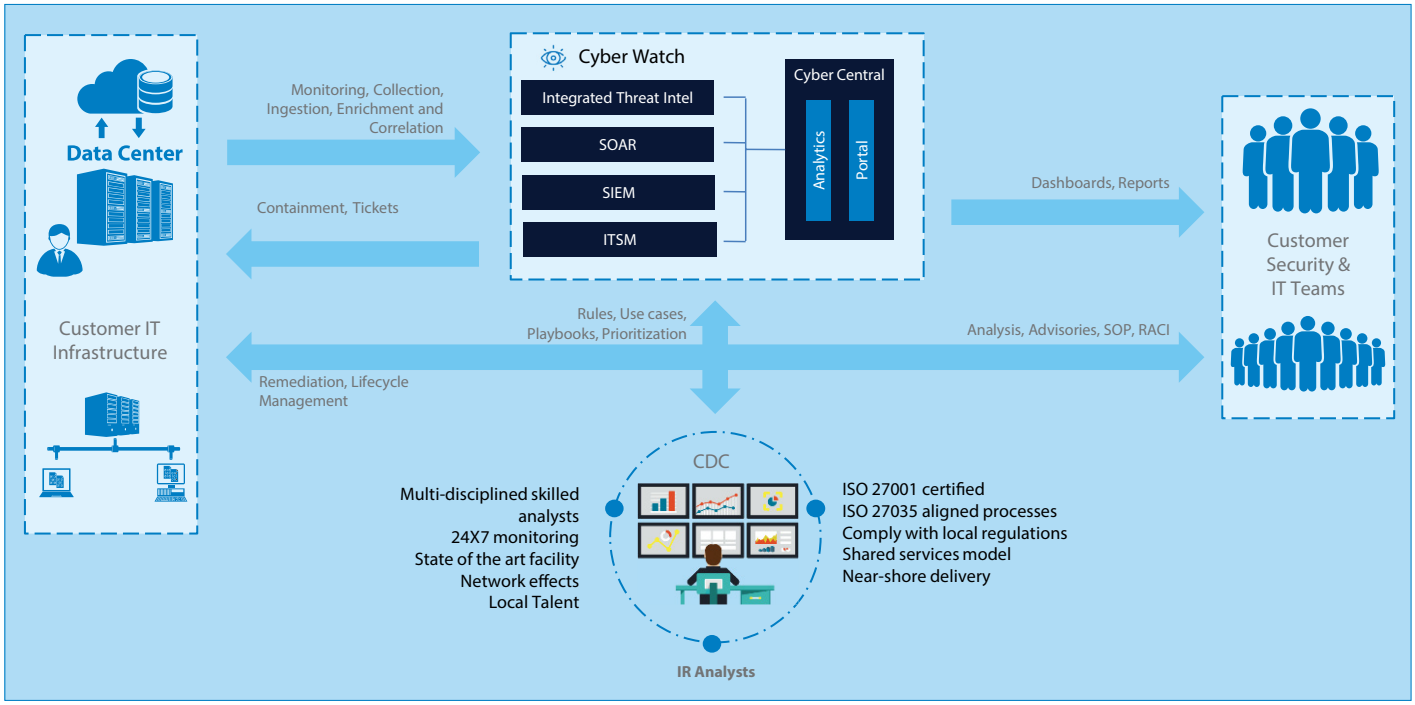
As businesses across the world become increasingly reliant on information technology, and with the rapid rise of digitization, it is imperative to have a robust solution that can constantly and incessantly monitor the IT infrastructure for security incidents, detect them in real-time and contain them immediately. In case of a cyber incident, quick response is required to contain and mitigate damage else it could lead to devastating consequences such as financial or reputational losses, legal implications, or operational downtime.

Maintaining a 24x7 SOC is an expensive proposition for many enterprises. Due to the ever-changing threat landscape, it requires a constant upskilling of the SOC analysts. Additionally, organizations today may suffer from alert fatigue caused by a flood of security alerts due to misconfigured detection rules. This is further leading to high detection and response times.

Infosys Cyber Watch

Infosys Cyber Watch is a managed incident detection and response service, delivered as a comprehensive package from our state of the art Cyber Defense Centers. It is a ready-to-use solution that is consumed by global enterprise customers. It comes with a large library of built-in use cases and log source integrations, that provide deep visibility, automation, end-to-end lifecycle management, risk-based prioritization and orchestrated remediation, and containment responses to security incidents.

- Provides 24x7 monitoring of endpoints, workloads, networks and critical infrastructure in public and private clouds as well as third-party hosted SaaS products
- Packages multiple technologies (such as SIEM, SOAR, ITSM) that are pre-integrated and pre-tested, which significantly reduces deployment time
- Offers out-of-box and customized playbooks that encapsulate prior knowledge for consistent and automated response
- Tracks incidents throughout the lifecycle spanning across departmental boundaries with smooth workflow, thus ensuring that no incident is neglected. It comprises of the Infosys technology stack, proprietary content and robust SOC services.
- Provides access to Cyber Central, the integrated customer portal for all Cyber Next platforms thereby enabling customers with security insights through customized incident dashboards, giving details of incidents and alerts, as well as query and raw events.



External Document © 2021 Infosys Limited

Platform Features

- Any log source integration - Cloud, DC, Edge, Workplace, SaaS, OT/IoT etc.
- 700+ Comprehensive detection use case library mapped to MITRE ATT&CK framework
- Large playbooks for automated incident response and containment
- Integrated threat intel feed for contextualization and enrichment
- Dashboards, reports, incident view with cyber central
- Integration with customer ITSM

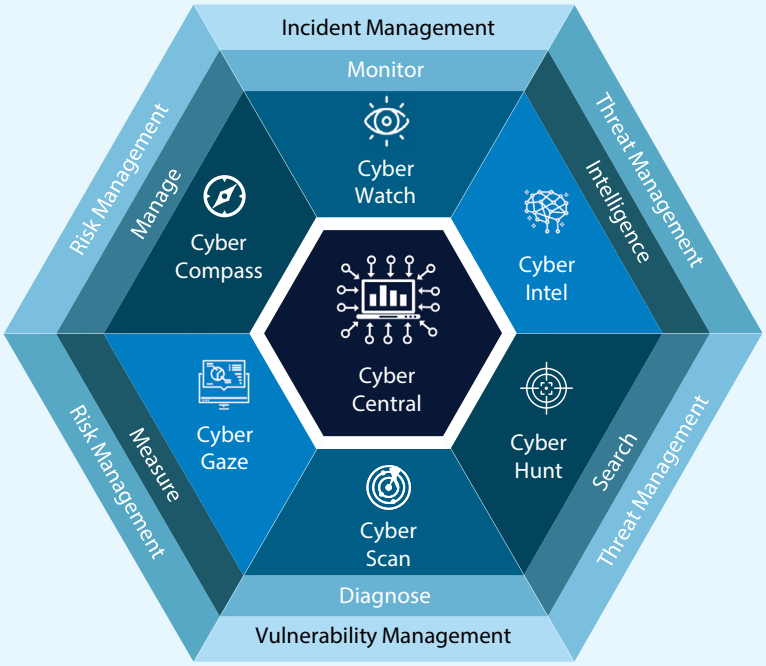
Services

- 24x7 Security event monitoring
- Log collection and analysis
- Security incident investigation and response
- Incident classification and prioritization
- Orchestrated and automated security response powered with playbook library
- Online and periodic reports and dashboards

Service Benefits

- Fast ROI due to quick onboarding, Pre-engineered technology stack, Pre-tested use cases and playbooks
- Reduced detection and response time, Automation playbook
- Subscription-based pricing model, Unit based pricing
- Continued focus on security outcomes, Not just managing security technologies

Cyber Next Suite



CYBER NEXT PLATFORM

Cyber Watch

24x7 Monitoring | Incident Monitoring & Response | Orchestration and Automation | Incident analysis and response

Cyber Intel

Strategic Intel | Threat Landscape Monitoring | Brand Monitoring | Operational Intel | Threat Alerts & Advisories | Threat Feeds

Cyber Hunt

Proactively detecting anomalies | Hypothesis based hunting | Intel and TTP-driven Hunting | Home-grown "data lake"

Cyber Scan

Application Scanning | Infrastructure Scanning | Risk-based Prioritization | Secure by design | DevSecOps | Auto Patching

Cyber Gaze

Metrics Management | CISO Dashboard | NIST Alignment | Automated Integration | Developed "by a CISO for a CISO"

Cyber Compass

Controls Management | Centralized Enterprise Security Architecture | Status of controls and security tools | Identify control gaps

Cyber Central

Integrated View of all Offerings | Fully customizable Dashboards | Data Fusion | Next-gen Interface

External Document © 2021 Infosys Limited

Infosys Cyber Watch is a module of the **Infosys Cyber Next – Platform Powered Services.** Infosys Cyber Next offers a **comprehensive cybersecurity solution** to enterprises that otherwise need to invest in dozens of security technologies and niche skills in order to attain swift security maturity. It provides security-as-a-service in a single package that combines pre-selected and pre-integrated ready-to-use security technologies that are homegrown or from our partners. The ecosystem offers deep visibility, lifecycle management, automation, risk-based prioritization, and the flexibility to scale-up and scale-down solutions as per business and operational requirements.

To know more, please write to us at cybersecurity@infosys.com

For more information, contact askus@infosys.com

Infosys®
Navigate your next

© 2021 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.