Infosys®
Navigate your next

THREAT DETECTION AND RESPONSE

Enterprises must accelerate threat detection and response in order to quickly identify and remediate the loss from cyber attacks thereby ensuring business continuity. This entails developing niche skills for cyber forensics, threat intelligence, and incident management to assure cybersecurity posture.

Client Challenges

- Unable to realize value from current investment due to ineffective cybersecurity program
- Keeping pace with evolving threat landscape in alignment with business needs due to escalating volume of alerts
- Lack of effective integration of Threat Detection and Response (TDR) initiative with the IT and security stack
- Unstructured and reactive approach to security incident response
- Limited access to industry's best practices restricting the ability for a quick response

Infosys Offerings

"We help our clients to strengthen their ability to detect and manage security incidents with a robust and integrated architecture and automated process."

Detection and Analytics

We assess and architect security detection and analytics requirements, suggest recommendations and enhancements, plan, design, deploy and configure SIEM, UEBA and deception toolset. Integrate log sources creating relevant content. Perform integration with other security tools. Define SOC framework.

Orchestration

We plan, deploy, configure and integrate with security tools and SOC solutions such as SIEM & CTI. Define workflows and create playbooks for orchestration and automation services for response activities.

Monitoring and Response

We defend, provide steady state monitoring and SOC operational services including threat detection, response, reporting and tracking of security incidents. Administration of SOC tools (maintenance, user access, patching) and content configuration & management.

Intelligence

We plan, design, deploy and operate threat intelligence platform. Integration with SOC platform and other security tools for ingestion of threat intel.

SWAT

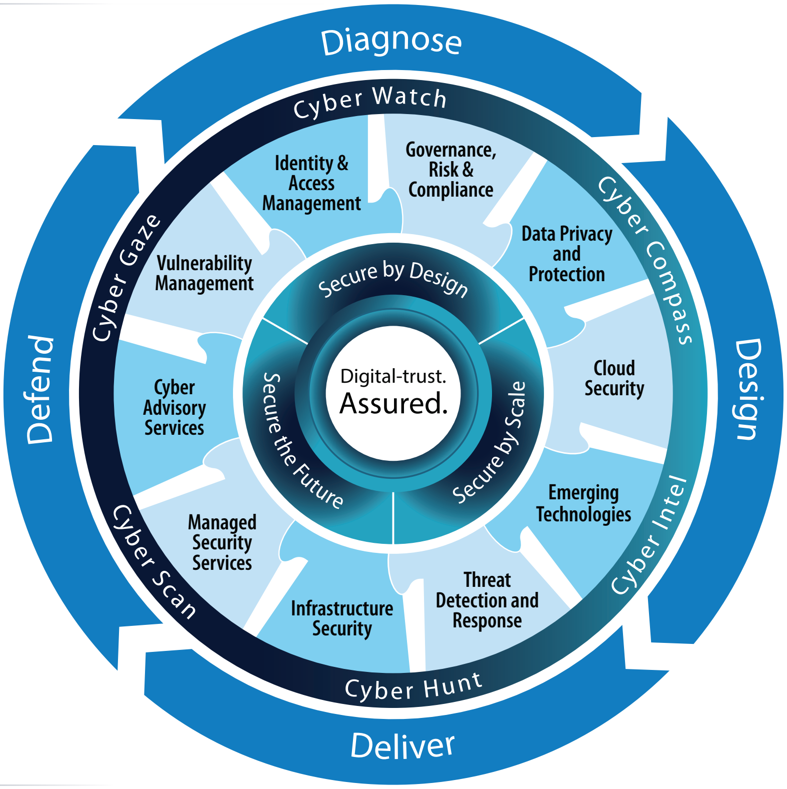
We assess the people, process and technology aspects of the organization's readiness to handle major security incidents. Provide IR and forensic investigation services.

Infosys Credentials

UK BASED COMPANY IN HEALTH & HYGIENE SECTOR	*Facilitated proactive response to cybersecurity incidents with the aid of technology and well defined processes and procedures*	Assured security posture for operations spread around 60 countries Secure by Scale – Deliver Secure the Future – Defend
LARGE BEVERAGES COMPANY	*Enhanced the security posture of the organization by building a suitable capability to centrally monitor and manage the security incidents across the organization spread globally*	Operationalized the processes to cover multiple locations/countries for threat detection and response Secure by Scale – Deliver Secure the Future – Defend

With Infosys CyberSecurity, you have

Digital-trust. Assured.



For more information, contact askus@infosys.com

Infosys®
Navigate your next

© 2020 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.