Threat Detection and Response Services

Attain Industry benchmark maturity on Threat Detection through Correlation & Contextualized Threat Intelligence

Introduction

With the ever-evolving attack vectors and the related impact on business, cyber defense has become a cornerstone to delivering business resilience. Wipro's Threat Detection and Response services provide Security Monitoring and Incident Response support, as a subscription-based service to AWS customers across the globe. Wipro monitors network, API, and host-level threats of AWS account(s) and triage security alerts and suppresses false positives. Security events are regularly delivered with AWS metadata of affected resources. AWS customers receive high-priority security event alerts, recommended remediation actions, or guided response support 24/7/365.

Key takeaways/ benefits

Threat detection and response empowers cyber defense which strengthens business resilience

Protecting business against latest and newer threats

High availability of Service Layers

Real-time, actionable security intelligence through analytics

Customizable to applicable regulations, guidelines, and standards

Solution

The key to Wipro's effectiveness in detected cyber-attacks is our **Threat Detection, Analysis and Response** framework.

Wipro leverages a unique use-case framework that defines indicators of threat and compromise that must be monitored and investigated. A rich repository of indicators is maintained by the Content management team and deployed for various customers to deliver security intelligence around malware, user behavior, vulnerability, network anomalies, and security operations. This repository contains a combination of more than 150 attack indicators and indicator groups that help identify:

- Infiltration via Attempts to exploit vulnerabilities
- Data Exfiltration via covert channels
- DoS / DDoS Attacks on networks and applications
- Zero day attacks
- Outbound Traffic Anomalies
- Suspicious Privilege Users on critical assets
- User behavior analytics
- Policy Violations by internal users
- Reconnaissance Attempts by external threat actors
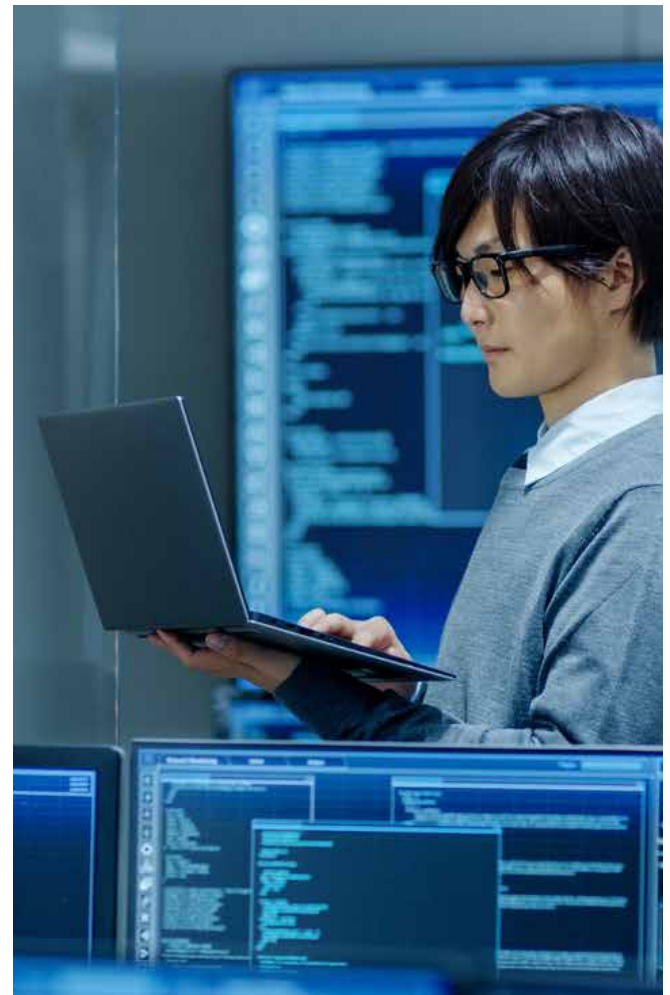
Threat Detection and Response Architecture
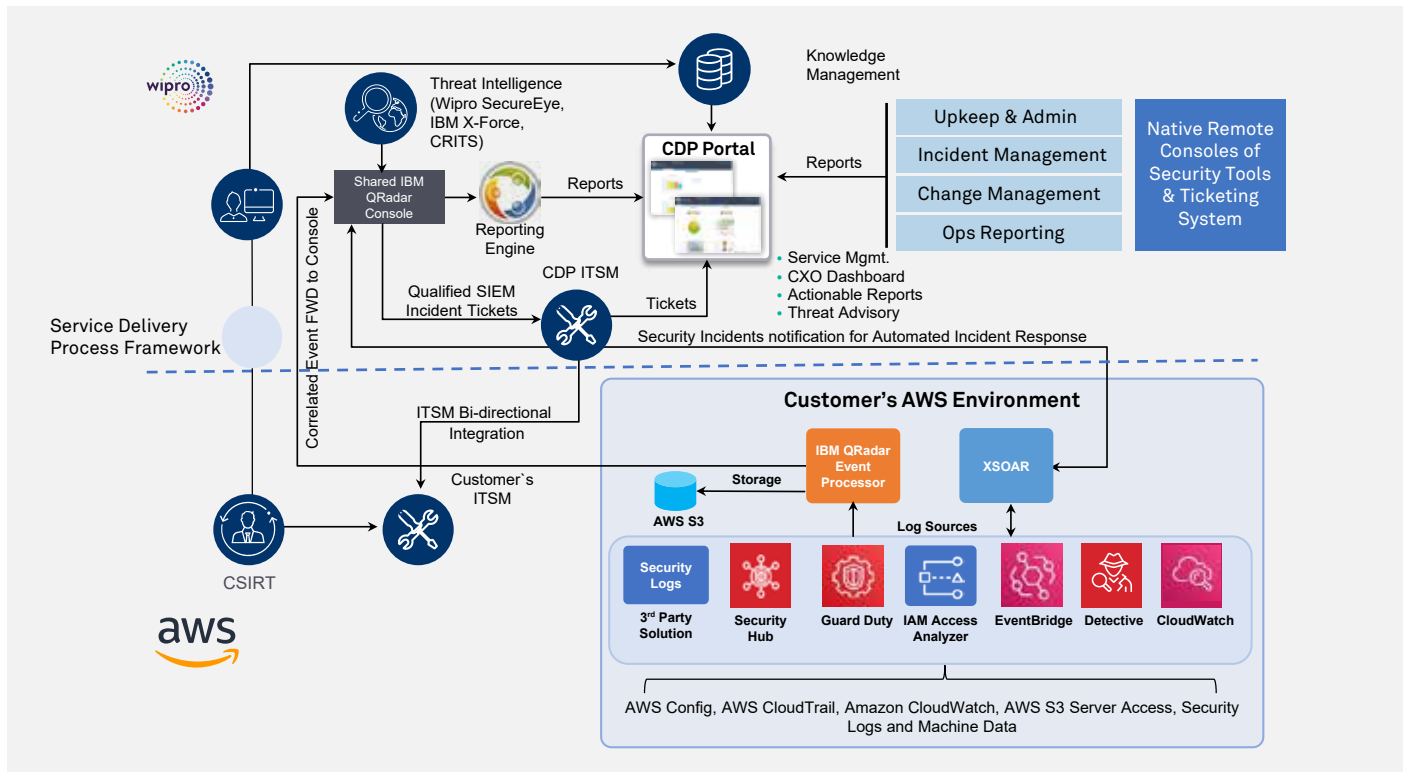
Features of Wipro's Threat Detection and Response

Security Data acquisition and retention on premises: Collection of security data of interest including security events, flows, and one or more types of security context data (network flows, vulnerability data, asset models and identities) from the AWS estate. This data is retained at customer's premises.

Incident Detection, Analysis, and Reporting that delivers:

- Comprehensive security log and flow collection, monitoring, and correlation using a shared Security Information and Event Management (SIEM) platform
- Near real-time alerting of critical attack indicators
- Indicator qualification through context-based enrichment
- Analytical correlation of indicators to detect advanced threats/attacks
- Rapid security incident escalation and reporting
- Security incident kill-chain and causal analysis

Integrated Cyber Threat Intelligence that helps in identification and reporting of threats based on new indicators of compromises and threats.

Cyber Defense Portal delivers Security intelligence using an advanced reporting and visualization platform.

Periodic service maturity assessments that help in continuously assessing the service.

Wipro Limited
Doddakannelli, Sarjapur
Road,
Bangalore-560 035, India
Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 180,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,
please write to us at **info@wipro.com**