Cognizant's Cyber Threat Defense: AI-driven, Automation-led Cybersecurity for Modern Enterprises

In an era defined by escalating cyber threats and the unsustainable burden of traditional security, organizations face unprecedented risk. Cognizant's Cyber Threat Defense, powered by Microsoft Sentinel, delivers the decisive edge you need. This comprehensive, AI-driven, and automation-led security operations framework transforms your defenses, ensuring unmatched resilience, stringent compliance, and optimal operational efficiency across your complex hybrid and multi-cloud environment.

Strategic Value: Built for Modern Security Operations

Cognizant's Cyber Threat Defense, powered by Microsoft Sentinel, equips your organization with a proactive and decisive advantage against the complexities of the modern cyber threat landscape. Built on industry-standard frameworks such as

- MITRE ATT&CK and NIST, it provides robust and adaptable security architecture.

- Unified visibility across IT and OT environments enables real-time threat detection and rapid response across workplace, workload, cloud, infra and applications

- AI-powered anomaly detection and User & Entity Behavior Analytics (UEBA) reduce alert fatigue and enhance incident prioritization. Integration with Microsoft Defender Threat Intelligence enriches security insights, providing actionable context in real-time.: Intelligent Threat Detection

- Achieve interoperability and a unified defense posture through seamless integration with Microsoft Purview, Defender XDR, and Entra: Cohesive Defense Strategy
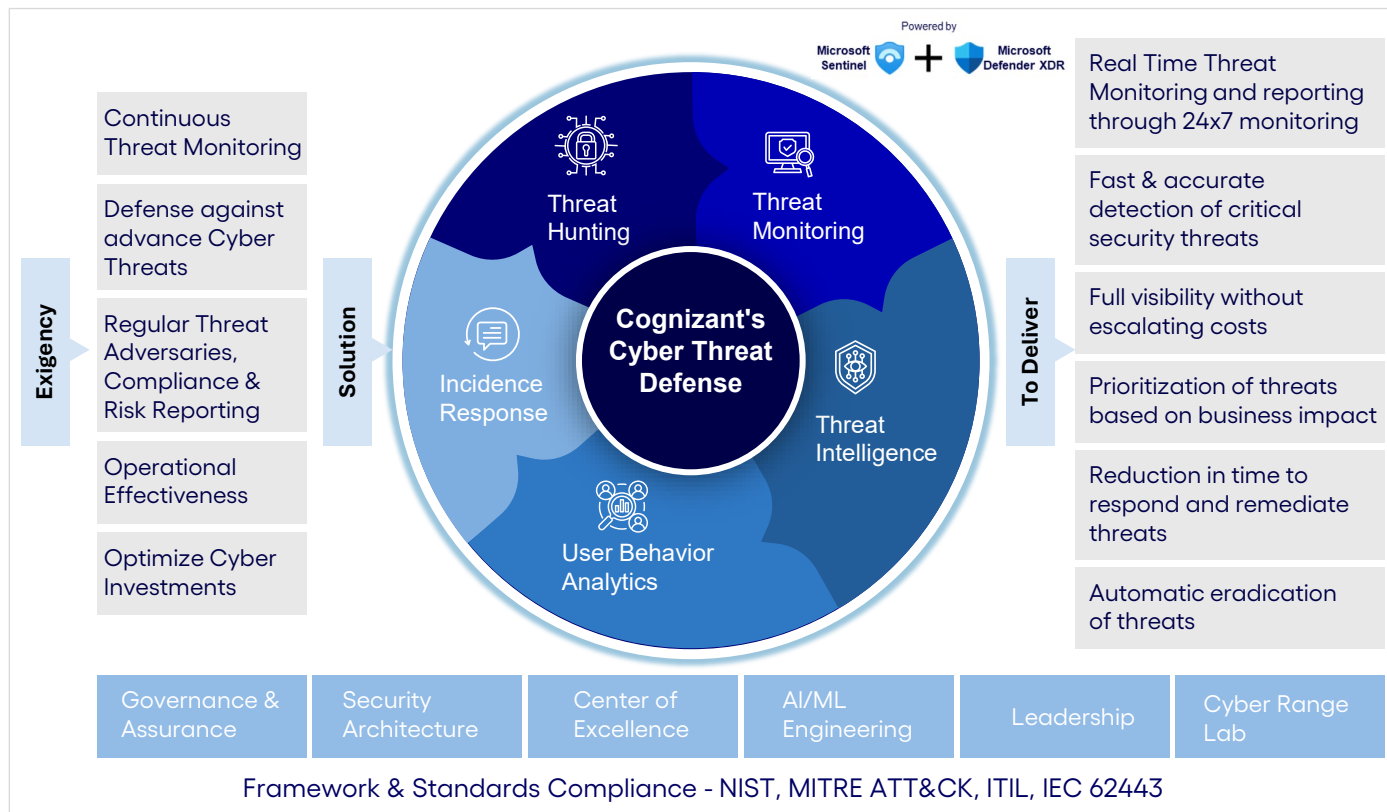
Core Capabilities: Protecting Your Enterprise 24x7x365

Cognizant's Global Cyber Defense Centers (CDCs) delivery centers provide continuous monitoring and response to threats, ensuring uninterrupted protection.

- Rapid and seamless integration of diverse data sources into the SOC ecosystem.

- Efficiencies through enhanced identification and analysis of security incidents with reduced false positives.

- Benefit from proactive threat hunting, real-time incident response, and comprehensive case management to address threats swiftly and thoroughly.: Proactive & Responsive

- Drive security maturity with SLA/KPI tracking, historical reporting, and post-incident analysis. This iterative approach ensures defenses are constantly evolving.: Continuous Improvement

- Comprehensive enterprise grade coverage for threat monitoring with 1000+ detection usecases and adcanced playbooks for automated threat detection and mitigqtion.

- Maintain stringent compliance standards while optimizing operations through AI/ML engineering, safeguarding regulatory posture and reducing potential penalties.: Governance & Compliance

Transformation Journey: Your Path to a Mature Security Posture

From Reactive to Predictive & Adaptive Security

Exigency
- Continuous Threat Monitoring
- Defense against advance Cyber Threats
- Regular Threat Adversaries, Compliance & Risk Reporting
- Operational Effectiveness
- Optimize Cyber Investments

Solution

Powered by
Microsoft Sentinel + Microsoft Defender XDR

Cognizant's Cyber Threat Defense
- Threat Hunting
- Threat Monitoring
- Incidence Response
- Threat Intelligence
- User Behavior Analytics

To Deliver
- Real Time Threat Monitoring and reporting through 24x7 monitoring
- Fast & accurate detection of critical security threats
- Full visibility without escalating costs
- Prioritization of threats based on business impact
- Reduction in time to respond and remediate threats
- Automatic eradication of threats

Governance & Assurance	Security Architecture	Center of Excellence	AI/ML Engineering	Leadership	Cyber Range Lab

Framework & Standards Compliance - NIST, MITRE ATT&CK, ITIL, IEC 62443

Cognizant's Cyber Threat Defense is built to help enterprises shift from reactive security postures to predictive and adaptive models. This transformation is essential to counter today's sophisticated threats and meet evolving compliance demands. By integrating continuous threat monitoring, real-time intelligence, and automated response, Cognizant empowers organizations to proactively defend their digital assets and reduce risk exposure.

Cognizant's phased transformation approach ensures a smooth and effective transition to a highly mature security operations model tailored to your specific needs.

- Gain a deep understanding of the current security posture, identify critical assets, assess existing tools and processes, and uncover gaps for strategic improvement.

- Define a clear SOC vision aligned with business goals, design robust technical architecture, integrate existing workflows, and establish KPIs for measurable performance.

- Seamlessly activate Microsoft Sentinel, integrate Defender XDR for unified detection, deploy custom security content, and rigorously validate readiness through testing.

- Deliver continuous protection with 24/7 monitoring, expert incident triage, and real-time performance tracking to ensure ongoing security

- Implement SOAR playbooks and leverage AI/ML for smarter threat detection. Continuously refine operations and reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) for peak efficiency.

Tangible Benefits: The Impact of Intelligent Security

Cognizant's SOC-as-a-Service delivers clear and quantifiable advantages across your organization.

Centralized visibility and control across hybrid and multi-cloud environments. Scalable architecture supports agile business growth. Reduced risk of breaches through proactive threat defense. Enhanced productivity via automation and streamlined workflows.

Rapid deployment with minimal disruption to your operations. Proven SOC model built on best practices and compliance alignment. Ready-to-use playbooks and use-case libraries for faster security maturity.

Lower total cost of ownership (TCO) with a flexible pay-as-you-go model. Improved compliance reduces the risk of regulatory penalties. Consolidated tools and processes enhance overall security ROI.

Why Choose Cognizant? Your Trusted Partner in Cybersecurity

Cognizant is a trusted partner committed to future-ready security operations.

With over 450 Microsoft Security Certified Professionals, Cognizant offers unmatched expertise and a proven track record in delivering scalable and secure SOC services.

Our methodology combines compliance-driven estate management, standardized processes, and predictive analytics to significantly enhance your security posture.

Through dedicated Centers of Excellence and automation-led operations, Cognizant ensures efficient, business-aligned security services meticulously tailored to mission-critical environments.

Let Cognizant be your strategic partner in cybersecurity transformation. Reach out today to schedule a personalized consultation and discover how we can elevate your security operations.

Primary Contact – cybersecuritypulse@cognizant.com

cognizant®

Cognizant helps engineer modern businesses by helping to modernize technology, reimagine processes and transform experiences so they can stay ahead in our fast-changing world. To see how Cognizant is improving everyday life, visit them at **www.cognizant.com** or across their socials **@cognizant**.

World Headquarters

300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

280 Bishopsgate
London
EC2M 4RB England
Tel: +44 (01) 020 7297 7600

India Operations Headquarters

5/535, Okkiam Thoraipakkam,
Old Mahabalipuram Road,
Chennai 600 096
Tel: 1-800-208-6999
Fax: +91 (01) 44 4209 6060

APAC Headquarters

1 Fusionopolis Link, Level 5
NEXUS@One-North, North Tower
Singapore 138542
Tel: +65 6812 4000