Wysetek Cyber Defense Centre

Constant Vigilance, Continuous Protection

Detect, Defend and Respond cyber threats in real time and provide an integrated view with 24x7x365 coverage

The Cyber Defense Centre Advantage

Incident Response

Response process begins with a preparation phase where every asset, identity and network segment are fully prepared to handle an effective incident response

Easy Integration

Works with existing technologies including security systems to deploy advanced threat detection and response tools, and provide real-time threat intelligence and analysis

Increased Coverage and Confidence

Better visibility and detection capabilities into the organization's entire network, including critical infrastructure and IT systems.

SOC Platform Engineering	Managed Security Operations Services	Threat Intelligence & Hunting
· SIEM design and deployment · SOAR orchestration · System integration, parser development and API integration · Log source and event flow tuning	· Cybersecurity toolset management · Alert Monitoring · Triage, containment, and recovery · Incident Response & Management · Time Bound Reports	· Threat feeds ingestion · Threat hunting & Attack discovery · Recon, scanning, and enumeration · Analysis and confirmation · Response coordination

24*7*365 Real-time security monitoring and analysis with Shared-Hybrid-Dedicated Models

Services Offerings

- Application Security Testing-SAST, DAST & Source Code Review
- Logs Normalization, Co-relation, Analysis & Retention
- User & Entity behavioural Monitoring and Analysis (UEBA)
- Incident Response & Management and Alerting
- Vulnerability Assessment & Penetration Testing (VAPT)
- Threat intelligence Feeds & Indicators of Compromise (IOC) reporting
- Dark Web & Brand Monitoring and Takedowns
- Threat Hunting
- Governance, Monthly reporting
- Automated blocking of Ports, URL's and Domain Names

Evaluation of the threat landscape Assessment Services:

- **Threat Landscape Report:** Comprehensive documentation of current and emerging threats relevant to the organization and its industry.
- External and Internal Attack Surface Analysis: Detailed mapping of all potential exposure points and recommendations for reducing them.
- **Risk Assessment Matrix:** Prioritized list of threats and vulnerabilities with impact and likelihood ratings.
- Threat Intelligence: Summary of adversaries, campaigns, and tactics that could impact the organization.
- **Mitigation Recommendations:** Actionable steps to improve security posture, reduce risks, and respond to threats effectively.
- Dark Web Monitoring
- Brand Monitoring +Takedown

Red Teaming:

- Identify potential entry points and vulnerabilities exposed on public-facing infrastructure
- External and Internal Exploitation
- Simulate cyber-attacks both from an external adversary and from within your network
- Breach and Attack Simulation (BAS)
- Adversary Simulation: Mimic actions of cyber adversaries targeting your specific environment
- Ransomware Simulation: Test the resilience of data against ransomware attacks
- Malware Execution: Assess detection and response to malware threats
- Targeted Asset Coverage

Vulnerability Assessment and Penetration Testing:

- Vulnerability Assessment, Scanning and Penetration testing of Web Application, Mobile Application, Network Devices, Servers and Endpoints.
- Publishing of the management and technical report of Vulnerabilities with recommendations.
- Revalidation / Rescan after remediation, publishing and submission of report

Phishing Attacks:

- Customized phishing email templates.
- Simulated phishing campaigns and analysis reports.
- Phishing awareness training materials (presentation decks, videos, job aids).
- Post-training phishing simulation results with trend analysis.
- Comprehensive final report summarizing findings and recommendations.

Trainings:

- On specific issues arising out the gaps and redressal weaknesses observed.
- Phishing Awareness Trainings

Governance:

- Review of Governance platform by way of Policy, Procedure documents.

Regulatory Compliance & Audit Support:

- Assistance in complying to RBI Audits, IS Audits, VA Audits, PT Audits and/or any other security audits.

Move Beyond the SOC...

As cyber threats grow more advanced and frequent, a traditional SOC can't keep up. To stay ahead, businesses need a proactive approach to threat intelligence, detection, and response.

...and Enhance with the Cyber Defense Centre

A Cyber Defense Centre (CDC) is a centralized function that integrates security operations from multiple sources, including security devices, threat intelligence feeds, an incident response program, and global intelligence. The primary goal of a Cyber Defense Centre is to Detect Defend and Respond to cyber threats using an intelligence-driven analysis, Mitre att@ck framework, and tailored incident response process.

Next-Gen Cybersecurity for Digital Transformation

Protecting businesses from newer threats and being compliant requires a strong cybersecurity posture, built on collaboration and advanced technologies. With Wysetek as your trusted partner, you can transition from a traditional SOC to a next-gen Cyber Defense Centre. We help global enterprises navigate cybersecurity challenges with resilience, earning trust from our customers and accolades from the industry.

For More Information Contact: **Peter Dcosta** | Email: **peter.dcosta@wysetek.com** | Call: **+91 98330 86869**

WYSETEK

Wysetek Systems Technologists Private Limited
1701 & 1702, 17th Floor, D-Wing, Lotus Corporate Park,
Graham Firth Compound, Off Western Express Highway,
Goregaon (E), Mumbai - 400063.
+91-22 4918 5900 www.wysetek.com

Branch Offices:
- Ahmedabad
- Bangalore
- Chennai
- Hyderabad
- Kolkata
- New Delhi
- Pune