NeoSOFT®

Capabilities

CyberSecurity

About Us

Great Place To Work. Certified INDIA

25+ YEARS OF EXCELLENCE

CMMIDEV/5

Overview

4000+ Employees

10 Global Offices

9 Development Centers

Office Space **1,00,000+** Sq.ft.

Clientele

1500+ Clients

50+ Countries

85% Clients Retention

Industry Verticals **22+**

Achievements

2000+ Products Engineered

1500+ Applications Developed

12+ Awards

20+ Million Development Hours

Partners

aws

SAP

Microsoft

Google Cloud

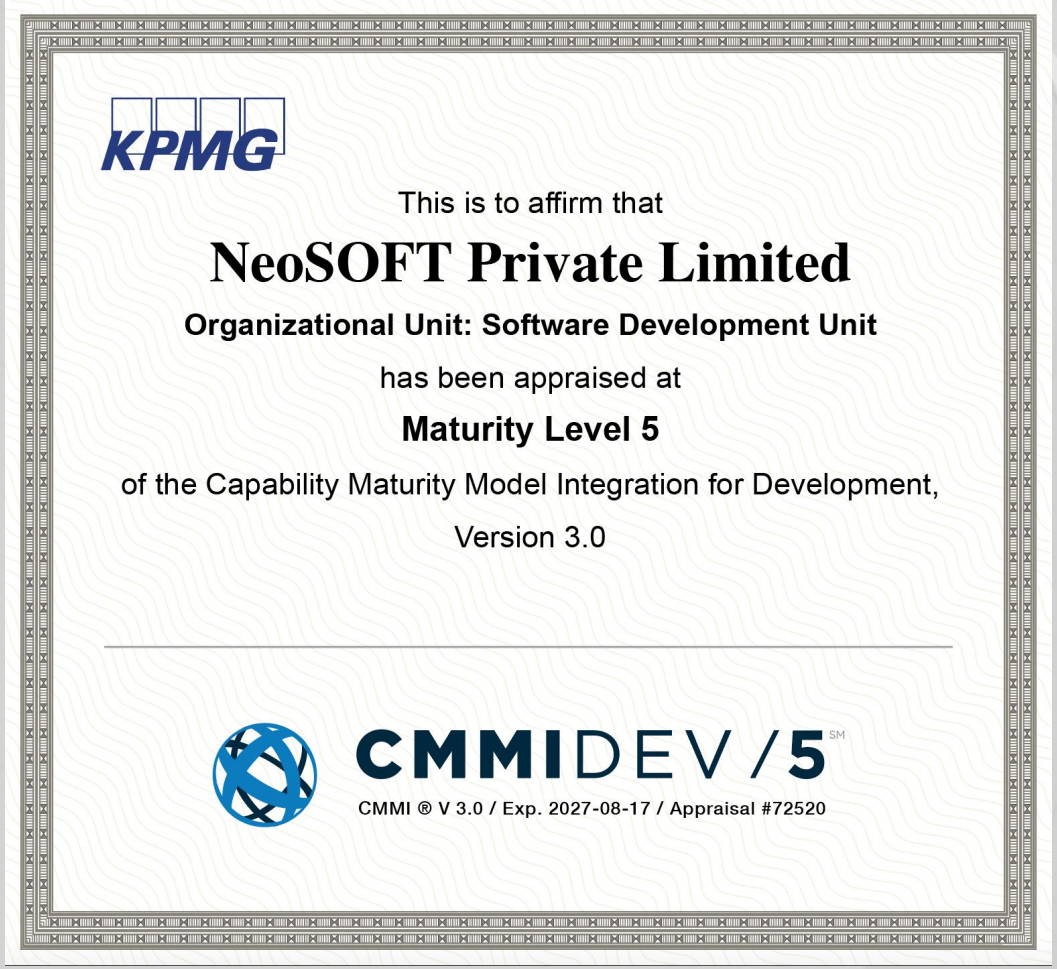
Magento

shopify

WOO COMMERCE

Certified To Deliver Quality

Great Place To Work. Certified INDIA



ISO
9001:2015
Quality Management

ISO
27001:2013
Information Security

ISO
20000-1:2011
IT Management

ISO
22301:2012
Business Continuity Management

What We Do

Team Augmentation

A team of 4000+ Battle Tested engineers across 100+ Different Stacks.

We are your Digital Factory, dedicated teams to supercharge your development throughput.

0 Operational Overheads.

Agile & On Demand.

Fixed Scope

We offer meticulously crafted project specifications and timelines for cutting-edge development, seamless integrations and feature-rich solutions.

The NeoSOFT approach ensures your projects are delivered with precision and excellence.

Managed Services

Our IMS services helps enterprises to run Business as usual.

With strong SLA driven services, 24x7 Support, Governance and Technology expertise, we help to optimize processes and costs.

Secure. Compliant. Resilient.

End-to-End Cybersecurity Solutions for Enterprises : In today's digital landscape, cybersecurity is not an option— it's a necessity. We offer a comprehensive cybersecurity suite.

Managed Security Services

Endpoint Security
Protecting devices

Cloud Security
Securing cloud environments

Network Security
Protecting Networks

Cybersecurity Process

1. Access – identifies Gap
2. Protect – Implement safeguards
3. Detect – Monitor threats
4. Respond – Mitigate incidents

Industry Specific Solutions

1. BFSI
2. Telecom
3. Pharma

Tailored security for various industries.

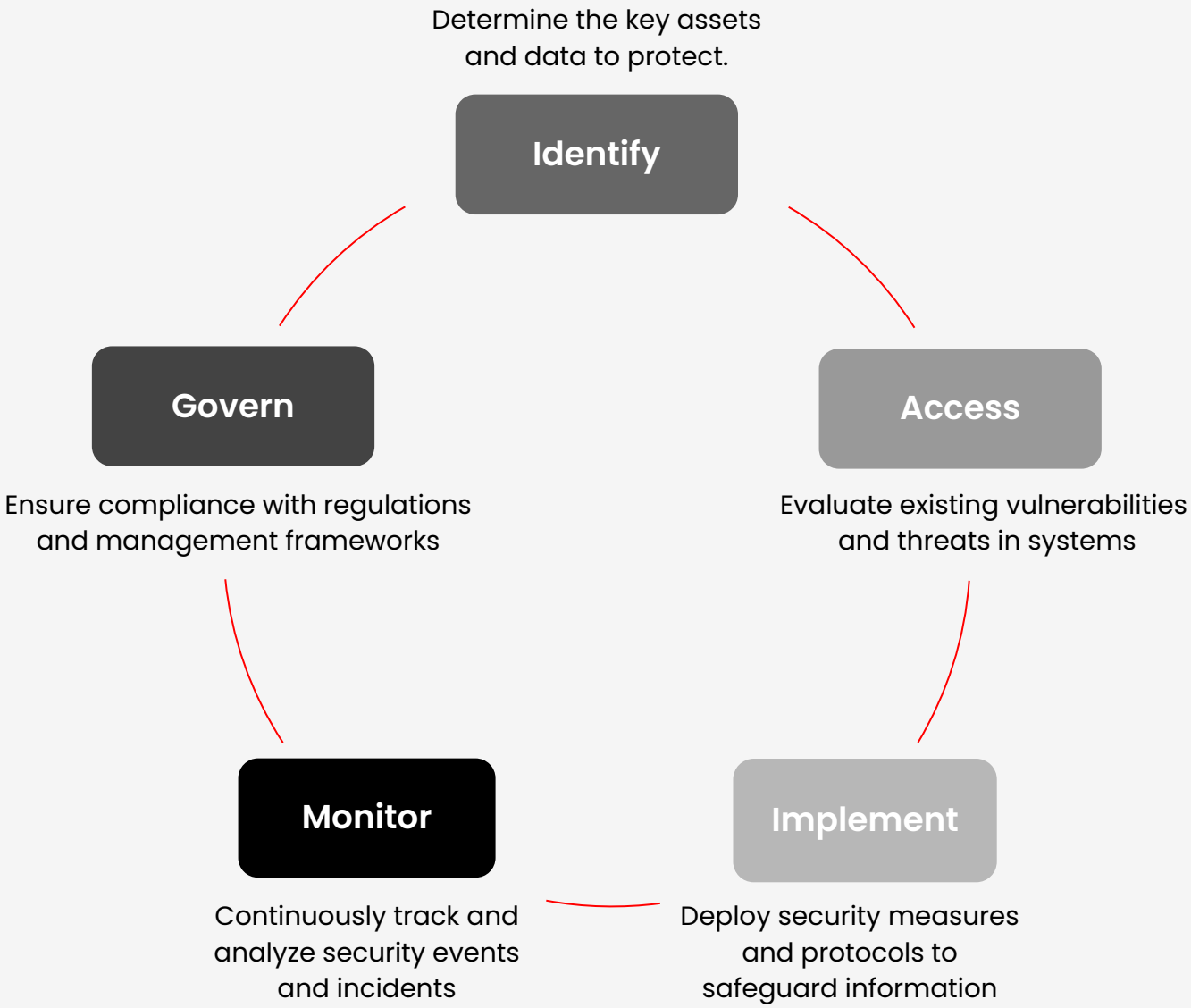
Why Choose Us ?

Expertise

Cost-Driven

AI Driven

Cybersecurity – IT Operations & GRC



Cybersecurity – IT Operations & GRC

Threat Mitigation

Implement advanced threat detection systems to proactively identify and respond to security threats in real-time, as the rise in sophisticated cyberattacks demands robust and timely defense strategies

Compliance Assurance

Establish automated compliance checks to ensure consistent adherence to regulations and industry standards, enabling organizations to effectively navigate evolving frameworks and maintain robust compliance

Risk Management

Develop an automated risk assessment framework to identify vulnerabilities and prioritize remediation efforts, ensuring that risk management gaps are effectively addressed to strengthen overall cybersecurity posture and resilience

Integrated Approach

Foster synergy between IT Security Operations and Governance, Risk, and Compliance (GRC) to streamline processes and enhance the overall cybersecurity posture, ensuring a more cohesive and proactive defense strategy

Key Tools

- SIEM (Security Information and Event Management) systems
- SOAR (Security Orchestration, Automation, and Response) platforms
- Intrusion Detection/Prevention Systems (IDS/IPS)
- Firewalls and network security appliances

Cybersecurity – IT Operations & GRC

Core Responsibilities of IT Security Operations

- Monitoring & Detection
- Incidence Response
- Vulnerability Management
- Threat Intelligence
- Endpoint protection
- Identity & Access Management

Compliance Assurance

- Governance
- Risk Management
- Compliance

Integration of SecOps and GRC : Effective integration between SecOps & GRC framework helps SecOps activities. SecOps help to take operations decisions & strategic governance

Key Tools

- SIEM (Security Information and Event Management) systems
- SOAR (Security Orchestration, Automation, and Response) platforms
- Intrusion Detection/Prevention Systems (IDS/IPS)
- Firewalls and network security appliances

Our Services

Cybersecurity Services Landscape

Security Operations

- SIEM
- SOC (24x7)
- DLP
- EDR
- XDR Email Security (Phishing/DLP)
- Threat Hunting

Vulnerability Mgmt

- VAPT (Nessus, Qualys)
- Patch Management

Network Security

- WAF
- Next-Gen Firewall
- Proxy
- DNS Filtering

Cloud Security

- Secure Cloud Configurations
- Cloud Workload Protection

Endpoint Protection

- UEM
- MDM
- Antivirus
- EDR

Identity & Access Mgmt

- PAM
- MFA
- AD Monitoring
- Identity Federation

GRC & Compliance

- Risk Assessments
- ISO 27001
- RBI/IRDA/SEBI audits support

Incident Management

- IR Plans
- RCA
- Threat Intel
- Tabletop Exercises

Key Challenges, Benefits & Solutions

Threat Mitigation

Implement advanced threat detection systems to proactively identify and respond to security threats in real-time, as the rise in sophisticated cyberattacks demands robust and timely defense strategies.

Compliance Assurance

Establish automated compliance checks to ensure consistent adherence to regulations and industry standards, enabling organizations to effectively navigate evolving frameworks and maintain robust compliance.

Risk Management

Develop an automated risk assessment framework to identify vulnerabilities and prioritize remediation efforts, ensuring that risk management gaps are effectively addressed to strengthen overall cybersecurity posture and resilience.

Integrated Approach

Foster synergy between IT Security Operations and Governance, Risk, and Compliance (GRC) to streamline processes and enhance the overall cybersecurity posture, ensuring a more cohesive and proactive defense strategy.

Security - Managed Services

- 24/7 Security Monitoring
- Threat Detection & Incident Response
- Security Event Correlation & Analysis
- Endpoint Detection & Response (EDR)
- Extended Detection & Response (XDR)
- Vulnerability Management & Patch Advisory
- Email security solutions
- Web Application Firewall (WAF)
- Threat Intelligence & Hunting
- Security Orchestration, Automation & Response (SOAR)
- Compliance & Regulatory Reporting
- Cloud Security Monitoring
- Phishing Detection & Response
- Insider Threat Monitoring
- Incident Investigation & Digital Forensics
- DevOps & DevSecOps
- Cloud Security Posture Management (CSPM)

Product /Solution		
SIEM	Q-RADAR	ARCSIGHT
VM	QUALYS	NESSUS
DAM	AVDF	GUARDIUM
ENDPOINT SECURITY	TREND MICRO	SYMANTEC
DLP	SYMANTEC	FORCEPOINT
PAM	AARCON	CYBERARK
CYBER ANALYTIC	SKYBOX	MDR
HSM	GEMALTO	DFIR

SOC Managed Services - Service Catalogue

24/7 Security Monitoring

- Continuous real-time security monitoring
- SIEM (Security Information & Event Management) integration
- Log collection & analysis

Threat Detection & Incident Response

- Advanced threat intelligence & analysis
- AI-driven anomaly detection
- Rapid incident detection & response

Security Event Correlation & Analysis

- Correlation of security events across endpoints, networks & cloud
- Behavioral analytics to detect abnormal activities
- Automated security alerts

Endpoint Detection & Response (EDR)

- Advanced endpoint protection against malware & ransomware
- Automated response to endpoint threats
- Forensic analysis of endpoint breaches

Vulnerability Management & Patch Advisory

- Regular vulnerability scanning & assessment
- Patch management recommendations
- Threat exposure reduction strategies

Threat Intelligence & Hunting

- Continuous proactive threat hunting
- Dark web monitoring for leaked credentials
- Tactics, Techniques, and Procedures (TTPs) analysis

Security Orchestration, Automation & Response (SOAR)

- Automated incident response workflows
- Integration with existing security tools
- Playbook-based remediation

Compliance & Regulatory Reporting

- Compliance with ISO 27001, NIST, GDPR, PCI-DSS, HIPAA
- Audit logs & forensic investigations
- Real-time & scheduled compliance reports

Cloud Security Monitoring

- Cloud-based workload security (AWS, Azure, Google Cloud)
- Cloud Access Security Broker (CASB) integration
- Cloud Identity & Access Management (IAM) monitoring

Phishing Detection & Response

- Email threat analysis & mitigation
- User awareness & phishing simulation training
- Real-time phishing attack response

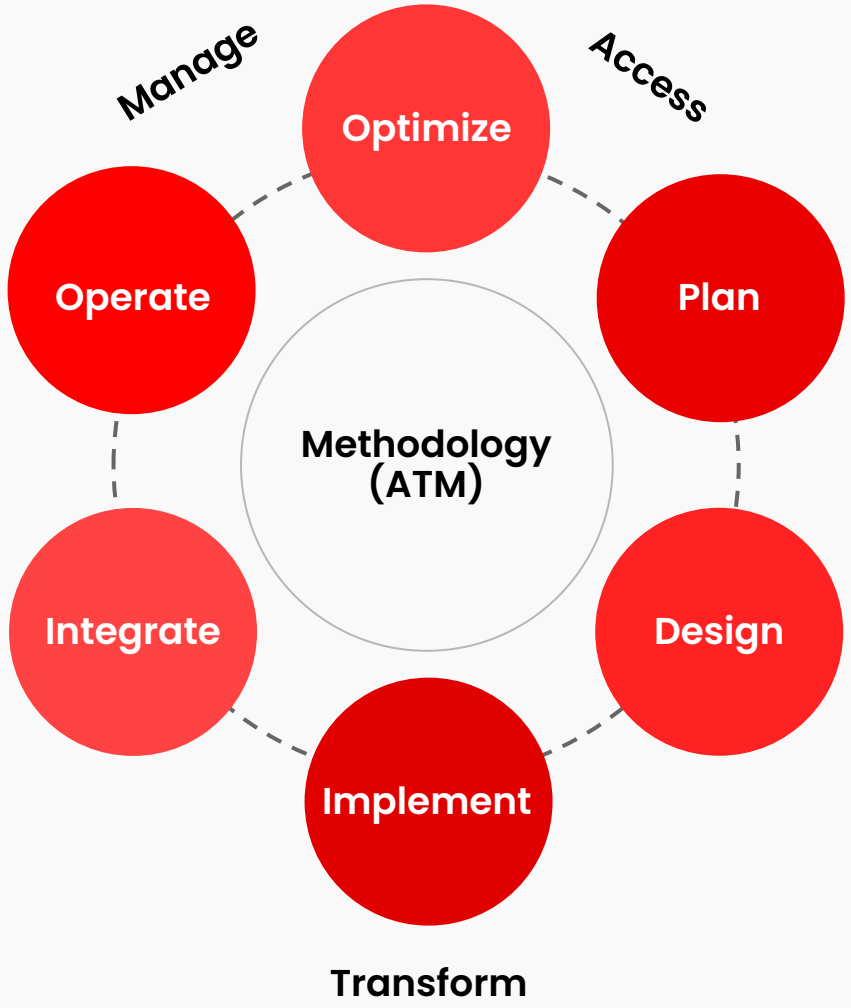
Insider Threat Monitoring

- Behavioral analysis for suspicious insider activities
- Privileged Access Monitoring (PAM)
- Policy enforcement & zero-trust framework implementation

Incident Investigation & Digital Forensics

- Deep-dive forensic investigations of cyber incidents
- Data breach root cause analysis
- Incident containment & recovery strategies

Security Consulting Methodology & Services Portfolio



- Governance Risk & Compliance
- BCP
- Mobile Security
- Infrastructure & Network Security
- Cloud Security
- Security Information & Event Management (SIEM)
- Identity & Access Management / Single Sign-On
- Security Posture Assessment (VA-PT)
- Security Operations Center (SOC)
- End-Point Security
- Data Loss Prevention (DLP)
- Web Security & Mail Security

Core Duties and Responsibilities

L1

- **Monitoring & Alerting –** First line of defense, continuously monitoring security systems and network traffic.
- **Alert Triage –** Analyzes security alerts to determine escalation needs.
- **Basic Incident Handling –** Performs initial response, including system isolation and data gathering.
- **Escalation –** Transfers critical incidents to L2 analysts for in-depth investigation.
- **Security Tools –** Proficient in SIEM, IDS/IPS, and fundamental security technologies.

L2

- **In-Depth Investigation –** Analyzes and investigates escalated security incidents.
- **Threat Analysis –** Identifies attack vectors and vulnerabilities.
- **Incident Response –** Implements containment, eradication, and recovery measures.
- **Reporting –** Documents findings with root cause analysis and recommendations.
- **Advanced Tools –** Utilizes security tools, network traffic, and malware analysis.

L3

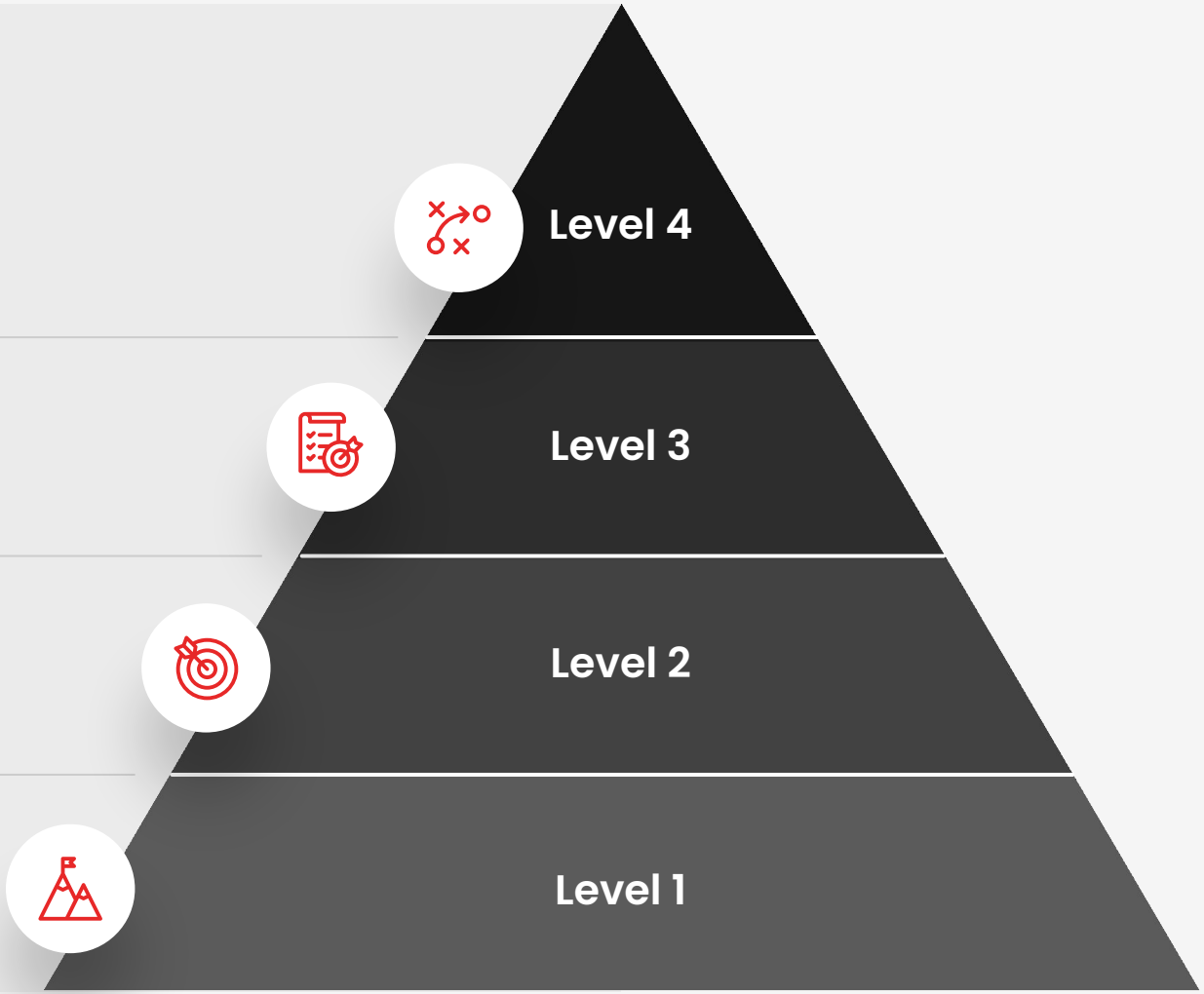
- **Advanced Threat Hunting –** Identifies hidden threats and vulnerabilities through proactive analysis
- **Threat Intelligence –** Monitors emerging threats and leverages intelligence feeds to enhance security.
- **Security Architecture & Design –** Contributes to security solutions, frameworks, and policies.
- **Incident Response –** Develops and optimizes response strategies for swift threat mitigation.
- **Expertise & Training –** Acts as a cybersecurity SME and trains SOC analysts.
- **Advanced Tools –** Specializes in network forensics, DLP, and insider threat detection.

Program / Project Manager

SME / L3 Support

Technical Support / L2

Monitoring Team / L1



Service Offering in Network Technology Managed services

01
24*7 Network surveillance

02
Performance monitoring

03
Trouble ticket management

04
Event management

05
Incident Management

06
Problem Management

07
Service level Management

08
Quality assurance

09
Change Management

10
Hardening & Compliance

11
Service Improvement plan for resource & performance Optimization

12
Network Security

13
Asset Management

14
Resources as per industry standards(Certified on Cisco, Checkpoint, Palo alto etc.)

15
SDWAN implementation & monitoring

Network Managed Services - Service Catalogue

Network Monitoring & Performance Management

- 24/7 real-time network monitoring
- Traffic analysis & bandwidth optimization
- Network health reporting & analytics
- Proactive issue detection & resolution

Security & Threat Management

- Firewall management & configuration
- Intrusion Detection & Prevention (IDP)
- Threat intelligence & vulnerability assessments
- Endpoint & perimeter security

Incident Management & Troubleshooting

- Rapid response to network incidents
- Root cause analysis & resolution
- Automated alerts & escalation procedures
- Onsite & remote troubleshooting

Cloud & Hybrid Network Support

- Secure cloud connectivity & VPN management
- Hybrid network integration (On-prem & Cloud)
- Multi-cloud security & compliance
- SD-WAN deployment & management

Network Infrastructure Management

- Router, switch & access point configuration
- LAN/WAN management & optimization
- Data center network management
- Load balancing & failover management

Compliance & Risk Management

- Adherence to industry standards (ISO, NIST, GDPR, HIPAA)
- Security audits & risk assessments
- Policy enforcement & compliance reporting
- Encryption & data protection

Remote Access & VPN Services

- Secure remote workforce solutions
- VPN setup & management
- Multi-factor authentication (MFA) integration
- Zero Trust Network Access (ZTNA)

Backup & Disaster Recovery

- Network data backup solutions
- Redundancy planning & failover configurations
- Disaster recovery planning & testing
- RTO/RPO optimization

Wi-Fi & Wireless Network Management

- Secure enterprise Wi-Fi setup
- Wireless access point monitoring & optimization
- Guest Wi-Fi & access control
- Performance analytics & reporting

Network Consulting & Advisory Services

- Network architecture design & optimization
- Technology upgrades & migrations
- Custom network solutions tailored to business needs
- Training & cybersecurity awareness programs

Case Studies

Case Study for Client

Client: Life Insurance Provider

Challenges

- Managing and triaging a high volume of security alerts from endpoints and email systems.
- Gaining comprehensive visibility across a distributed and hybrid infrastructure.
- Investigating and responding to complex security incidents.

Solution

- Used **Crowdstrike EDR** for intelligent endpoint alert correlation and **Cisco Email Security** for spam/phishing filtering with rule-based automation.
- Deployed **Zscaler and BluCoat Proxies** to monitor and secure web traffic, and used **Palo Alto Firewalls** for granular traffic inspection and threat prevention.
- Leveraged **OEM support** via integrated platforms **Palo Alto and Cisco**.

Impact & Success

- **Reduced false positives and alert fatigue, ensured faster triage** of real threats due to prioritized and context-aware alerts.
- **Centralized visibility** of all user activity across cloud and on-prem, and **improved detection** of lateral movements and hidden threats.
- Enabled **accurate root cause analysis (RCA)** with evidence-based escalations and quick containment and remediation guided by threat intelligence.

Tech Stack

CROWDSTRIKE | cisco Security | INDUSFACE | paloalto NETWORKS | zscaler | BlueCoat | CITRIX

Case Study for Client

Client: Pension Funds Provider

Challenges

- Managing a high volume of vulnerability alerts.
- Managing cloud misconfigurations and ensuring continuous compliance across multiple cloud services.
- Integrating multiple security tools into a unified monitoring and alerting system.

Solution

- Implemented **Qualys** to automate vulnerability scanning and triaging with custom tagging and risk-based prioritization.
- Utilized **Palo Alto Prisma Cloud** for continuous cloud resource monitoring and policy enforcement.
- Integrated all tools with a **centralized SIEM** for correlation and centralized alert management.

Impact & Success

- **Reduced alert fatigue** and ensured **faster and more accurate remediation** workflows.
- Automatically **identified misconfigurations and non-compliance**, enforcing security as code and reducing human error.
- **Streamlined threat visibility and incident response**, enabling faster decision-making and action.

Tech Stack

CROWDSTRIKE | PRISMA CLOUD BY PALO ALTO NETWORKS | Qualys. | iraje Enterprise Data Security | Akamai

Case Study for Client

Client: Leading Financial Institution

Challenges

- Increased cyber threats targeting financial transactions.
- Existing security operations lacked real-time threat detection.

Solution

- Deployed an advanced **Security Operations Center (SOC)** with L1, L2, and L3 analysts.
- Implemented **SIEM, IDS/IPS, and threat intelligence tools** for proactive monitoring.
- Developed an **automated incident response framework** to minimize manual intervention.

Impact & Success

- **40% reduction in incident response time** through automation.
- **Improved threat detection by 60%,** reducing false positives.
- **Strengthened overall security posture,** preventing major data breaches.

Tech Stack

python, Flask, AngularJS, JS, AJAX, CSS, HTML, Bootstrap, Qlik Sense, QlikView, mongoDB, redis, Windows Server

NeoSOFT® CMMI Level 5

Leading by Passion. Driven by Innovation

4000+	22+	1500+	85%
Professionals	Industries	Clients	Client Retention

Thankyou

022 4050 0600

www.neosofttech.com