VISIONET
Innovation. Simplified.

Security Operations

Capabilities

www.visionet.com

We are transforming from a Cloud First to AI-First Company

VISIONET

1 **Cloud Consulting**

2 **Cloud Migration / Modernization**

Infra / Apps / Data / Security

3 **Platform Engineering**

Infra Platform / Data Platform / Cloud Native Platform / ML Platform Gen AI Platform

4 **Cyber Security**

Infra / Apps / Data / Integration / Gen AI

5 **Cloud Operations**

Infra / Apps / Data / Integration / Gen AI

Our **Cloud Capabilities**

VISIONET

Cloud Consulting	Migration / Modernization	Platform Engineering	Cyber Security	Cloud Operations
• Cloud Strategy • Cloud architecture review • Cloud cost optimization • Security Posture • DevOps Assessment	• Application & Data Modernization • PaaS service adoption • Migration to managed Kubernetes • Cloud native architecture • Containerization and hybrid cloud	• Digital Platforms & Products • Cloud Native • IT Modernization • Enterprise Agility • Mobility • DevSecOps Adoption	• Governance, Risk & Compliance (GRC) • Threat & Vulnerability Management • Cloud Native Security • Security Operations Center (SOC) • App Security	• DevSecOps • DataOps • FinOps • Cloud Automation

visionet CloudStudio

Visionet's framework to enable

- FinOps
- AI Ops
- Sec Ops
- Data Ops
- DevOps
- Mig / Modernization
- Managed Kubernetes

Did you know that Visionet is an "Azure AMMP Partner"?

Out of the 400,000+ partners that Microsoft officially works with, there are only about 500 partners worldwide, that are AMMP certified

Microsoft Solutions Partner
Infrastructure
Azure
Specialist
Infra and Database Migration

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Data & AI
Azure

aws partner network
Advanced Consulting Partner

Google Cloud
Partner

DATADOG

orca security

Prometheus

paloalto NETWORKS

Visionet's SOC Offerings

Service Offerings

- Advisory and Implementation Services
- Audit Management
- Assessment Services
- 24x7 monitoring and management
- Privacy and Compliance
- V-CISO & V-DPO

Features of Visionet's Security Practice:

- Platform based
- Automation enabled
- Advanced technologies – SOAR, DFIR, Threat Intelligence etc.

Visionet SOC Tools & Technology (SIEM, SOAR, TIP, XDR)

- Sentinel
- QRadar
- Splunk
- Resilient
- MISP
- CTM 360
- Microsoft Defender
- Cortex
- Trend Micro

Key Facts

- **30+** Projects Delivered
- **150+** Security SMEs
- **50,000+** Devices monitored & managed
- **20+** GRC Audit projects completed

Tools & Technology Expertise

Visionet SOC Service Catalog

VISIONET

Monitoring

- Security alarms real time notification
- Periodical reports for misconfigurations and low severity security evidences
- Tuning process support
- First level analysis and support in security incidents
- Managed Endpoint Detection & Response

Device Management

- Security policy advisory and review
- Change management
- Software patching and maintenance
- Maintenance and management of Firewall and Security Web Gateway

System Management

- Log sources integration and management
- Log parsing and correlation
- On-prem and Cloud Security platforms change management
- Design and implementation of deception scenarios
- Data Loss Prevention
- Cloud Access Security Management

Threat Intelligence

- Periodic event based threat intelligence reports
- Tailored investigation reports on Solix's request
- Black market monitoring
- Fraud detection
- Data breach
- Anti-phishing

Service Delivery Management

- Incident management
- Change management
- Problem management
- Identity & access management
- SOP / Run book

Crisis Management, training and security awareness

- Security training and courses
- Cyber exercise report
- Cyber Training & Security Awareness
- Cyber Crisis Management

Security Incident Response

- Artifacts analysis and reports
- Containment and mitigation activities
- Incident response reports
- Remediation and restoration technical support
- Security evidences and artifacts
- Compromise assessment report
- Malware Analysis

Governance & Reporting

- Operational reporting
- Cloud security status
- Documentation
- Continuous feedback and improvement

Illustrative Enhanced Features

VISIONET

Enhanced SOAR

- Multiple play books to enrich incident response and remediation
- Incident Diagnosis
- Log Source Health Monitoring
- Ticket triage notification
- Email notification

Use Case

- Reconnaissance
- Weaponization
- Network Security
- Access/Authentication
- Delivery
- Exploitation
- Installation
- Command & Control
- Data Exfiltration
- Others

Threat Hunting

- Identifying previously unknown threats
- Identifying ongoing non-remediated threats
- Threat Hunting using MITTRE Framework tactic and Techniques.

UEBA

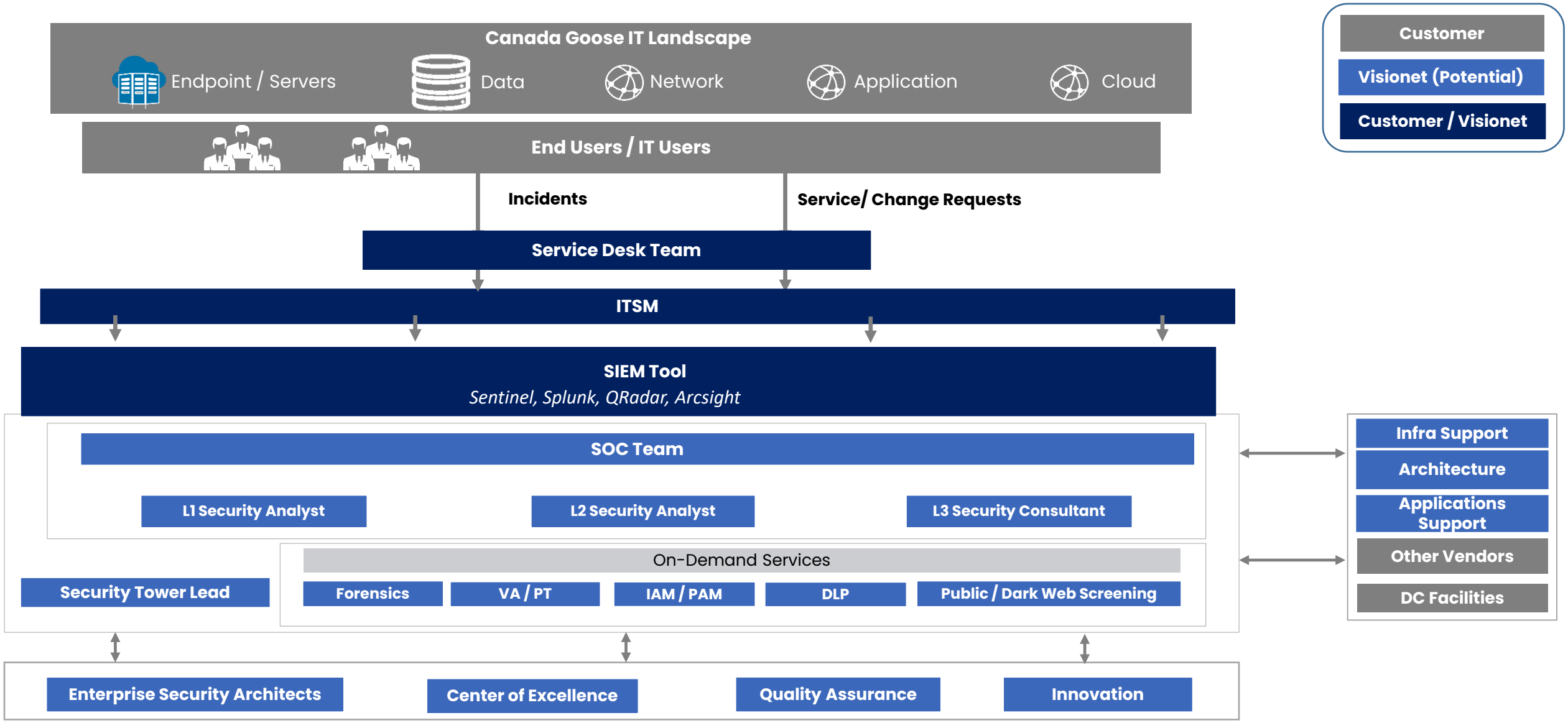
- Based on Machine learning and AIML modules.
- Search Host activities
- Search User Activities

Threat Intelligence

- Periodic event based threat intelligence reports
- Tailored investigation reports on Canada Goose's request
- Black market monitoring
- Fraud detection
- Data breach
- Anti-phishing

Our Approach of Managing SOC

VISIONET



SOC Incident Response (Monitor Network Security, Identify vulnerabilities & Threats)

VISIONET

SIEM

Prioritized Security Insights from Network Logs, Flows, Vulns, User, Config Data etc.

Extensive data sources

- Cloud
- Security devices
- Servers and mainframes
- Network and virtual activity
- Data activity
- Application activity
- Configuration information
- Vulnerabilities and threats
- Users and identities
- Global threat intelligence

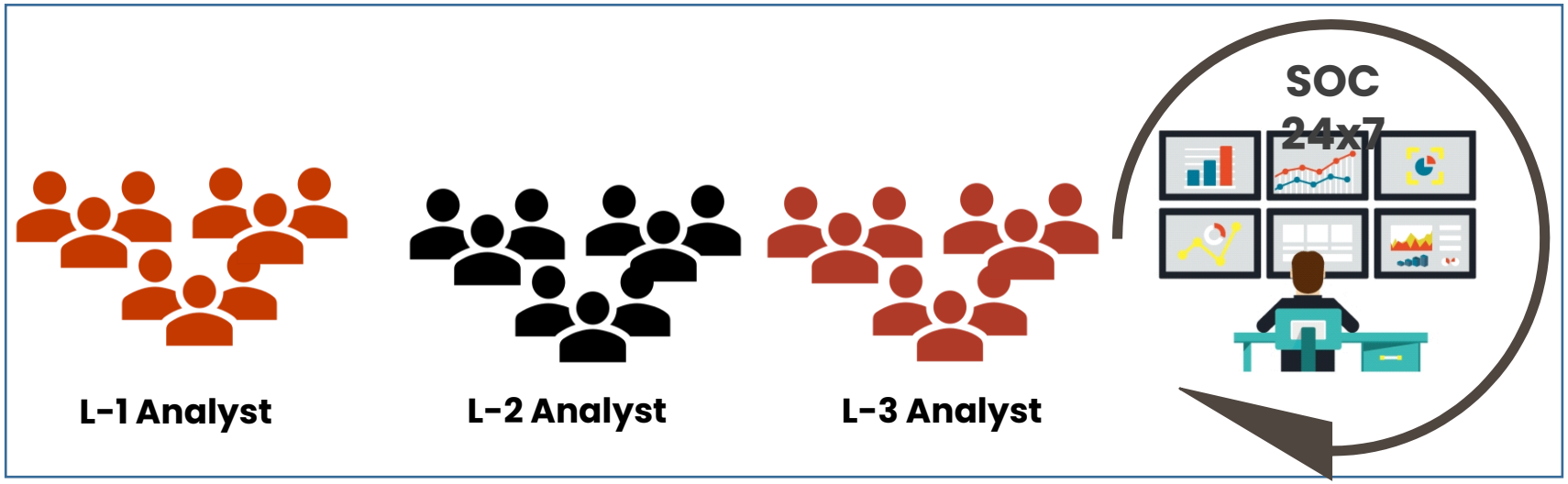
SIEM

- Extensive data collection, storage, and analysis
- Real-time correlation and threat intelligence
- Automatic asset, service and user discovery and profiling
- Activity baselining and anomaly detection

Prioritized incidents

IRP/SOAR

Security Operations for responding to threats, breaches, vulnerabilities



Your Trusted Technology Partner

Visionet is an engineering-led company driven by innovation. In our journey of 27+ years, we've helped over 350 clients across various industries to innovate faster, remain relevant, and build better products and services.

With more than 8,000 people worldwide, across our 14 locations, Visionet provides transformational consulting, technology, and outsourcing services and solutions for a broad range of industries, including Retail & Consumer Goods, Pharmaceutical, Banking and Financial Institutions (BFSI), Insurance, Foods & Beverage, Manufacturing & Distribution, and Apparel & Footwear. With our alliance with global innovators, including Microsoft, Salesforce, Amazon Web Services, and Adobe, we deliver next-generation services and solutions to our clients across Cloud, Digital, Data and AI, and Business Process Management.

Learn more about Visionet at **www.visionet.com**

Headquarters

4 Cedarbrook Drive, Bldg. B
Cranbury, NJ 08512
Tel: +1 609 452 0700
Fax: +1 609 655 5232

VISIONET