MICROLAND®

Making digital happen

Microland Cyber Services

Service Definition Document

Table of Contents

Microland Cyber Services

As the digital world races forward, so do the threats that target it. Businesses must constantly assess their current defenses and adapt their cybersecurity strategies to this ever-changing landscape. By proactively mitigating risks and building robust cyber resilience, enterprises can thrive in this dynamic environment.

Microland's "Cyber Resilient First Approach" is about equipping clients protect their IT systems, data, networks, and perimeter against cybersecurity attacks.

We leverage proven methodologies and intelligent automation to offer cyber defense solutions and offerings to ensure global enterprises can focus on business operations.

Services Portfolio

1. Cyber Advisory Services
2. Cyber Deploy Services
3. Cyber Run Services

Powered by **Intelligeni** – Microland's AI and ML-powered observability platform with predictive analytics and prescriptive solutions integrated with security tools.

Intelligeni® CyberOps extends the core Intelligeni AIOps capability to enhance operational efficiencies in the cybersecurity space. It encompasses and transcends traditional cyber security management tools by offering an integrated, analytics-driven approach with real-time insights and an overarching governance framework to safeguard digital ecosystems. By combining holistic insights into cybersecurity operations with enhanced operational efficiencies Intelligeni® CyberOps results in a fortified security posture and improved board level CISO metrics.

Drawing from the foundation metrics of Security operations, Risk Management, and Cyber Resiliency, Intelligeni® CyberOps meticulously measures and enhances system capabilities across key security functions—Identify, Protect, Detect, Respond, and Recover. It ensures that cyber operations align with security objectives, maintaining the confidentiality, integrity, availability, and accountability of information systems and gauge performance amidst potential cyber disruptions, tracking the timeline from disruption detection to response and system recovery, reinforcing the fabric of security operations.

Our Certifications and Delivery Centers

Our defence centers are state-of-the-art setups dedicated to evaluating, developing, and modeling the Next Gen Cyber tools to strengthen the security and stability of customer infrastructure. It is also used for solution demos to prove the strength and intelligence of the proposed solution to our customers. Conducting proof of value (POV), and proof of concept (POC) and verifying that a particular concept or theory has practical potential are some of the key areas we focus on.

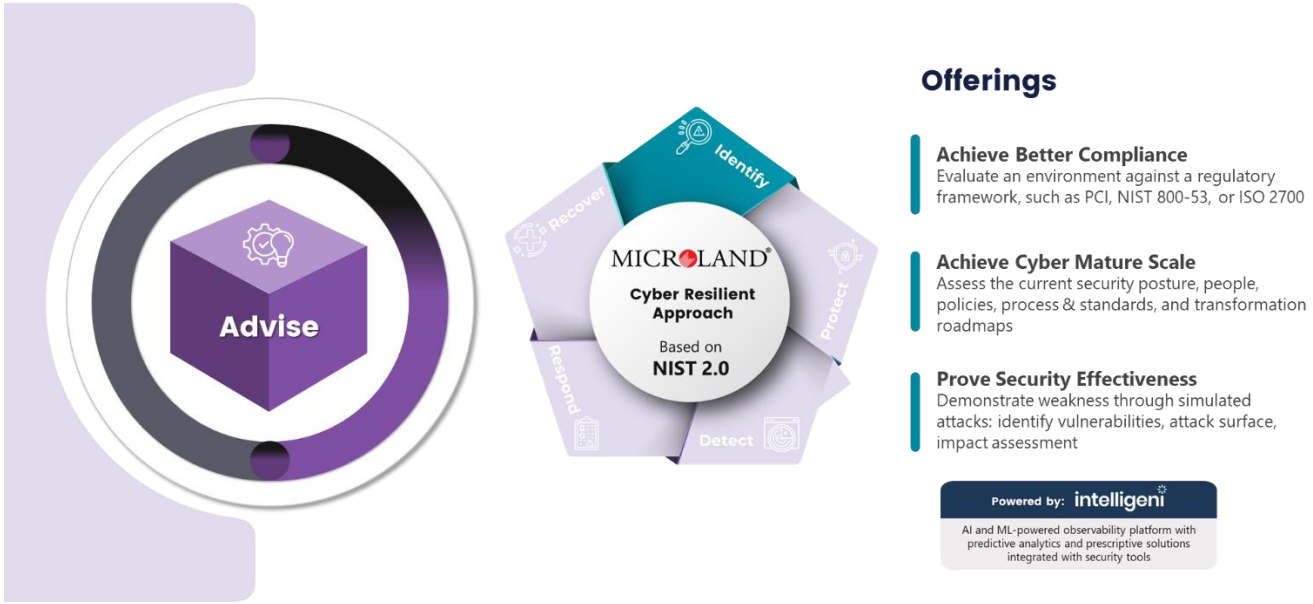
- Microland's Assurance framework has been certified to ISO IEC 27001 and ISO 20000-1 for over a decade.
- UK GDC certified on CES and CES+ by UK govt's authorized agency.
- BS 10012 - global standard on personal information management
- Active participant & a part of DSCI and IAPP

Cyber-Advisory Services

Our Cyber-Advisory Services are focused on designing a cyber-resiliency first approach for our clients in ever-evolving cybersecurity and helping clients comply with complex industry and geo-specific compliance and regulations.

We cover a broad spectrum of services that include:Bett

- **Compliance**: Compliance assessments evaluate an environment against a reference model, which could be a governance or regulatory framework such as PCI, SOX, NIST 800-53, or ISO 27000
- **Cyber Maturity Assessment**: Assessment of the security posture of an enterprise, their people strategy, policies, process, and standards to provide a digital transformation roadmap
- **Active Assurance**: Demonstrate weaknesses in the environment through simulated attacks, assess the attack surface, and ensure protection from a wide variety of security threats
- **Risk Advisory**: Assessment of vulnerabilities, configuration, or policies across multiple areas (like Data, Cloud, and Identity), identify the associated risks (both business and technical) and finally provide recommendations along with mitigation plans.



Microland's SOC Maturity Assessment

Microland's SOC Maturity Assessment evaluates a customer's security posture, processes, and tools against cyber threats. It assesses readiness, based on in-house or outsourced Security Operations Center (SOC), using CMM and NIST frameworks. The goal is to pinpoint strengths and weaknesses, providing solutions for improvement. This helps senior management allocate budgets effectively.

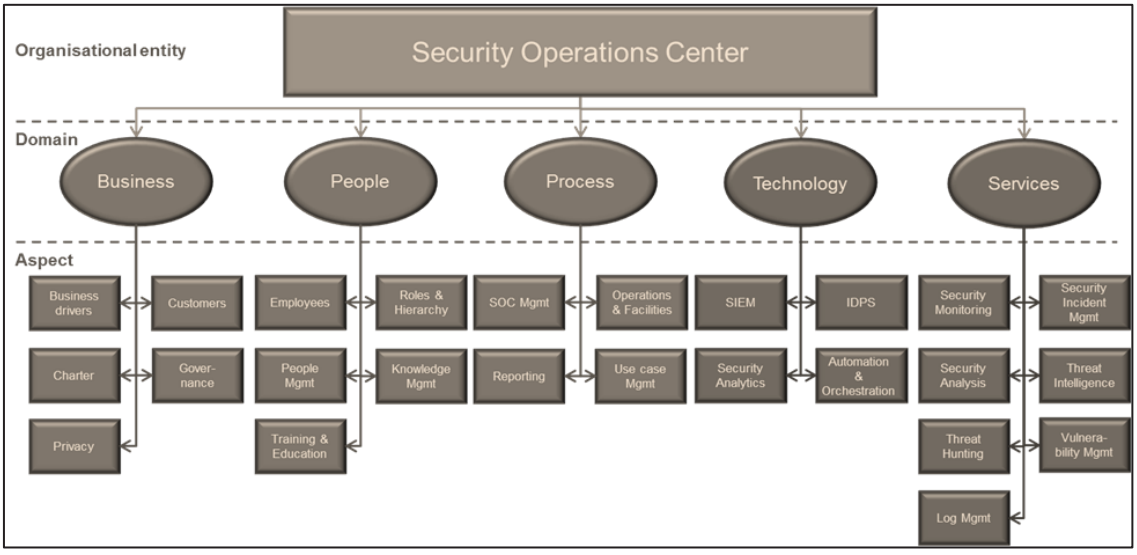
These maturity levels are measured across 5 domains: Business, People, Process, Technology and Services. The maturity levels as implemented in this tool are not staged with pre-requisites for each level. Instead, every element adds individually to the maturity score: a continuous maturity model.

The assessment of technology & services domains to have a higher technical focus and the capabilities of the SOC under these domains are categorized under one of the 4 capabilities levels mentioned below as an indicator of their completeness.

- Level 0: Incomplete
- Level 1: Performed
- Level 2: Managed
- Level 3: Defined

Like maturity levels, progress to a higher capability level is continuous. There are no prerequisites for advancing to a higher level, thus the capability growth is continuous as well.

The different aspects of the assessment under each domain are mentioned in the diagram below:

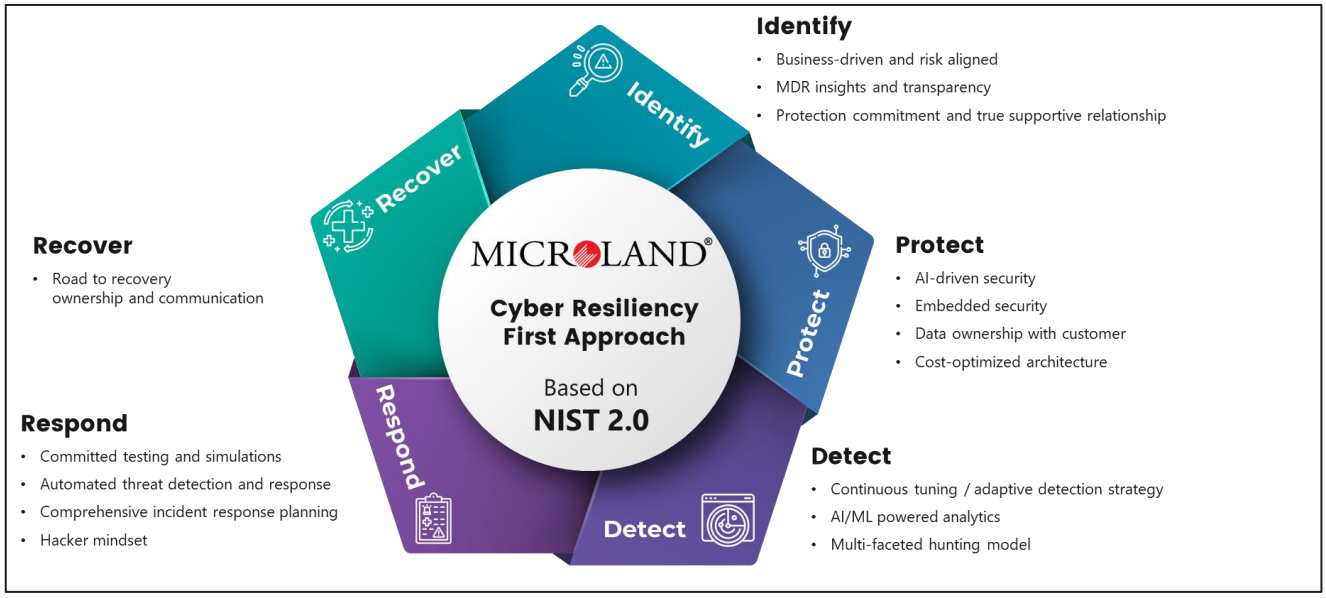


During the SOC assessment, the scope of the assessment under the technology and services domain is defined along with the target maturity level the organization is aspiring to achieve in its security roadmap.

Based on the overall maturity scoring and maturity scoring under each domain the 'Next Step' provides recommendations on the areas to be addressed to improve the maturity of the domain and SOC

Based on the criticality of each domain for an organization, the weightage for the different domains can be varied. For example, Business domain ranks higher for a BFSI organization and hence it can be categorized as 'high' or 'critical'. Setting weightage to 'none' will ignore the element in scoring entirely.

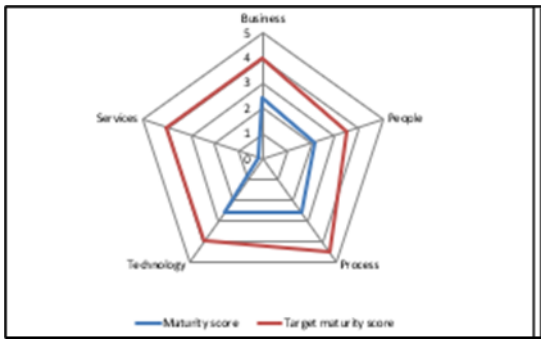
The questions in the assessment are mapped to different functions and categories of the NIST Cybersecurity framework shown in the figure below.

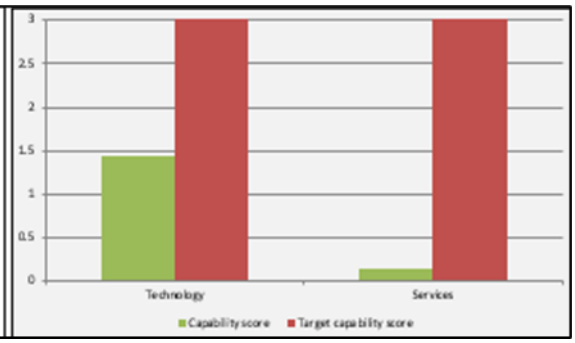


Based on the mapping and the responses to the questionnaire the Assessment also provides a NIST Score highlighting the maturity of the SOC under each of the 5 functions and categories under each.

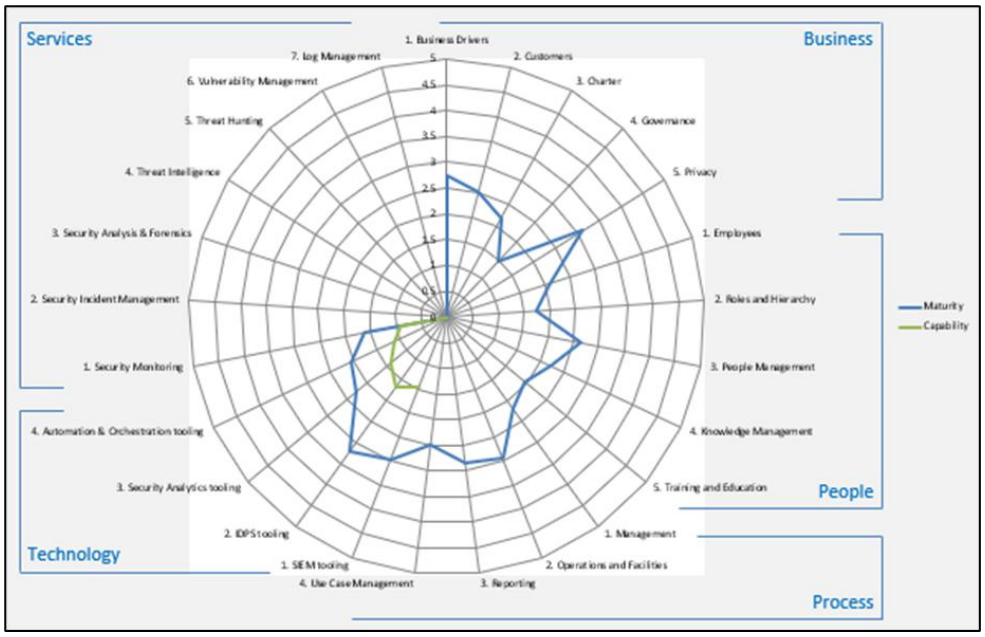
The Assessment will provide an extensive scorecard with Security Maturity Scoring under the CMM model and NIST CSF framework.

The snapshots of the CMM Scorecard are provided below.



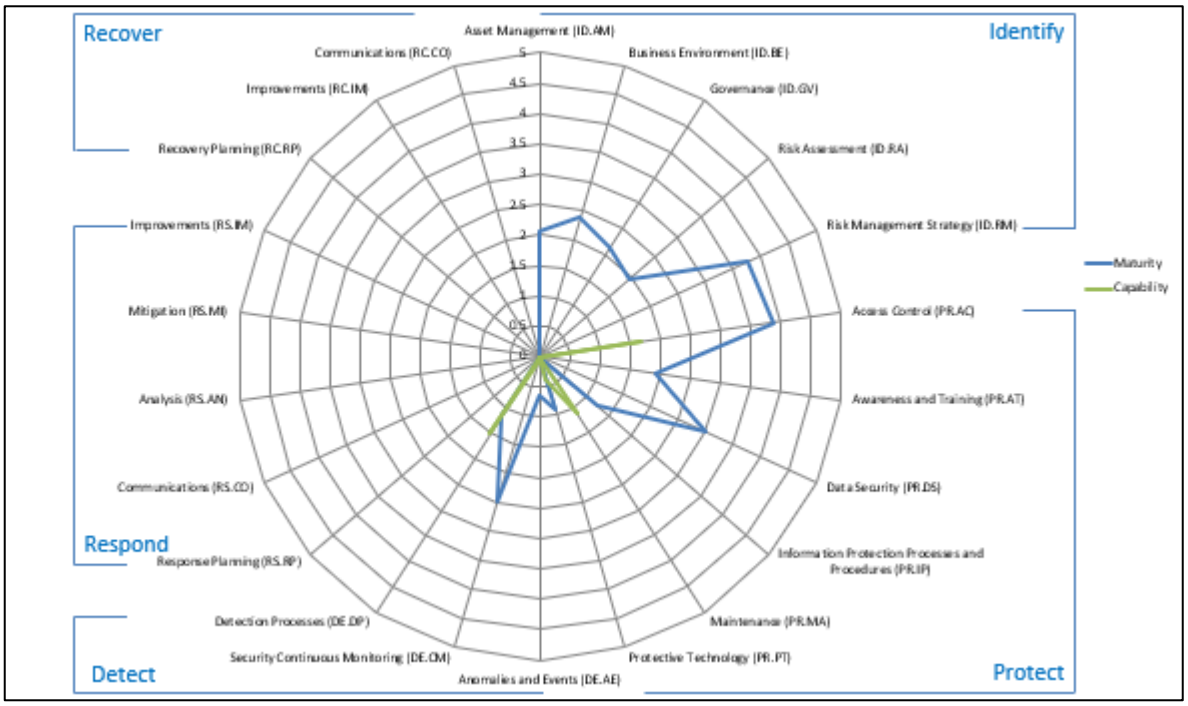


Domain	Aspect	Maturity Score	Maturity Target	Capability score	Capability target	In scope?
Business	1. Business Drivers	2.75				
	2. Customers	2.5				
	3. Charter	2.19				
	4. Governance	1.46				
	5. Privacy	3.13				
	overall: *Business*	*2.41*	*4*	*N/A*	*N/A*	
People	1. Employee	2.08				
	2. Roles and Hierarchy	1.72				
	3. People Management	2.63				
	4. Knowledge Management	2.23				
	5. Training and Education	1.96				
	overall: *People*	*2.12*	*3.5*	*N/A*	*N/A*	
Process	1. Management	2.19				
	2. Operations and Facilities	2.94				
	3. Reporting	2.84				
	4. Use Case Management	2.5				
	overall: *Process*	*2.62*	*4.5*	*N/A*	*N/A*	
Technology	1. SIEM tooling	2.97		1.47		Yes
	2. IDPS tooling	3.2		1.68		Yes
	3. Security Analytics tooling	2.27		1.41		Yes
	4. Automation & Orchestration tooling	2.03		1.14		Yes
	overall: *Technology*	*2.62*	*4*	*1.43*	*4.5*	
Services	1. Security Monitoring	1.63		0.91		Yes
	2. Security Incident Management	0		0		Yes
	3. Security Analysis & Forensics	0		0		Yes
	4. Threat Intelligence	0		0		Yes
	5. Threat Hunting	0		0		Yes
	6. Vulnerability Management	0		0		Yes
	7. Log Management	0		0		Yes
	overall: *Services*	*0.23*	*4*	*0.13*	*4.5*	



The NIST Scorecard will is as shown in the snapshot below:

Domain	Aspect	Maturity Score	Capability score
Identify	Asset Management (ID.AM)	2.05	N/A
	Business Environment (ID.BE)	2.38	N/A
	Governance (ID.GV)	2.14	0
	Risk Assessment (ID.RA)	1.96	0
	Risk Management Strategy (ID.RM)	3.75	N/A
	overall ***Identify***	***2.46***	***
Protect	Access Control (PR.AC)	3.88	1.69
	Awareness and Training (PR.AT)	1.92	0
	Data Security (PR.DS)	3	0
	Information Protection Processes and Procedures (P	1.25	0
	Maintenance (PR.MA)	0	1.13
	Protective Technology (PR.PT)	0.92	0.38
	overall ***Protect***	***1.83***	***0.53***
Detect	Anomalies and Events (DE.AE)	0.63	0.03
	Security Continuous Monitoring (DE.CM)	2.5	0.11
	Detection Processes (DE.DP)	1.17	1.52
	overall ***Detect***	***1.43***	***0.55***
Respond	Response Planning (RS.RP)	0	0
	Communications (RS.CO)	0	0
	Analysis (RS.AN)	0	0
	Mitigation (RS.MI)	0	0
	Improvements (RS.IM)	0	0
	overall ***Respond***	***	***
Recover	Recovery Planning (RC.RP)	N/A	N/A
	Improvements (RC.IM)	N/A	N/A
	Communications (RC.CO)	N/A	N/A
	overall ***Recover***	***N/A***	***N/A***



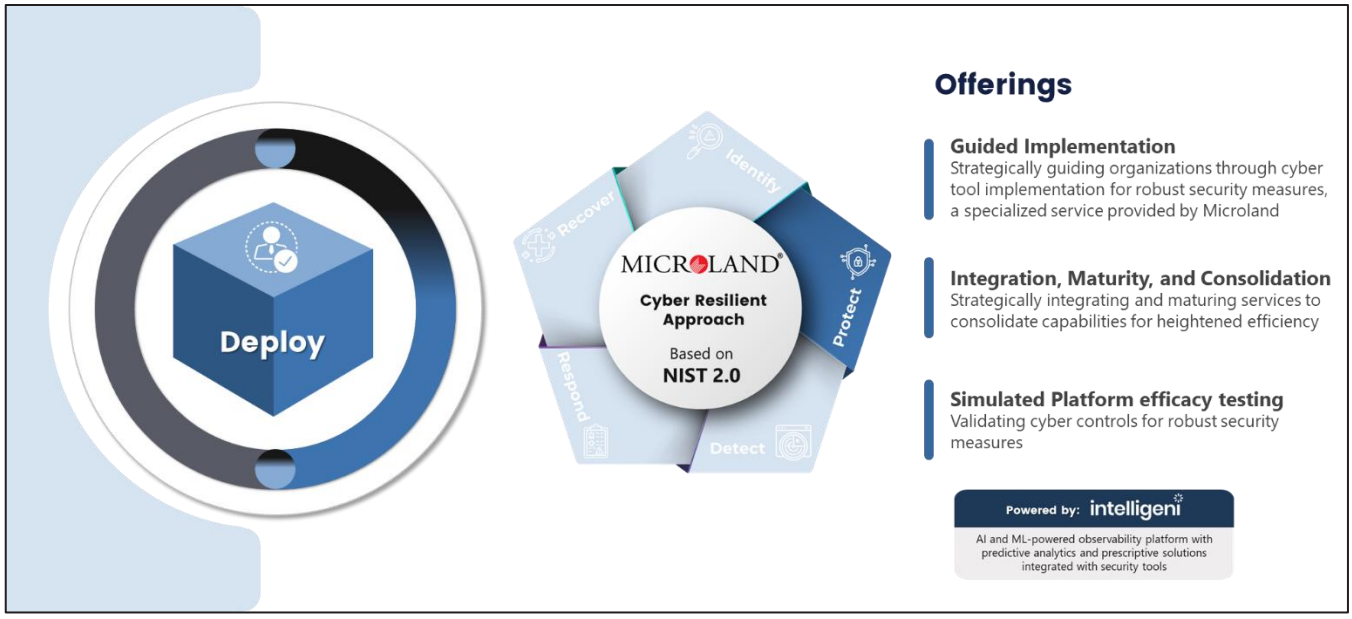
The SOC Assessment will be 3-4 weeks exercise based on the availability of the stakeholders from the customer organization being available for the interviews for the assessment. At the end of the assessment, the findings will be shared with the SOC team and senior management of the customer along with a presentation highlighting the results and recommendations for the next steps to achieve the target maturity score.

The Assessment can be a periodic exercise conducted every year or twice a year to ascertain if the SOC is in the right trajectory to the target maturity.

Cyber-Deploy Services

Microland has a unique process of delivering cybersecurity transformation services through a comprehensive repository of accelerators, reusable assets, and frameworks for accelerating the adoption of security compliance and cyber-resiliency initiatives, with expertise across industry domains.

Security Transformation Services like design, implementation, integrations of new cyber technologies solutions or replacement of an existing legacy technology.



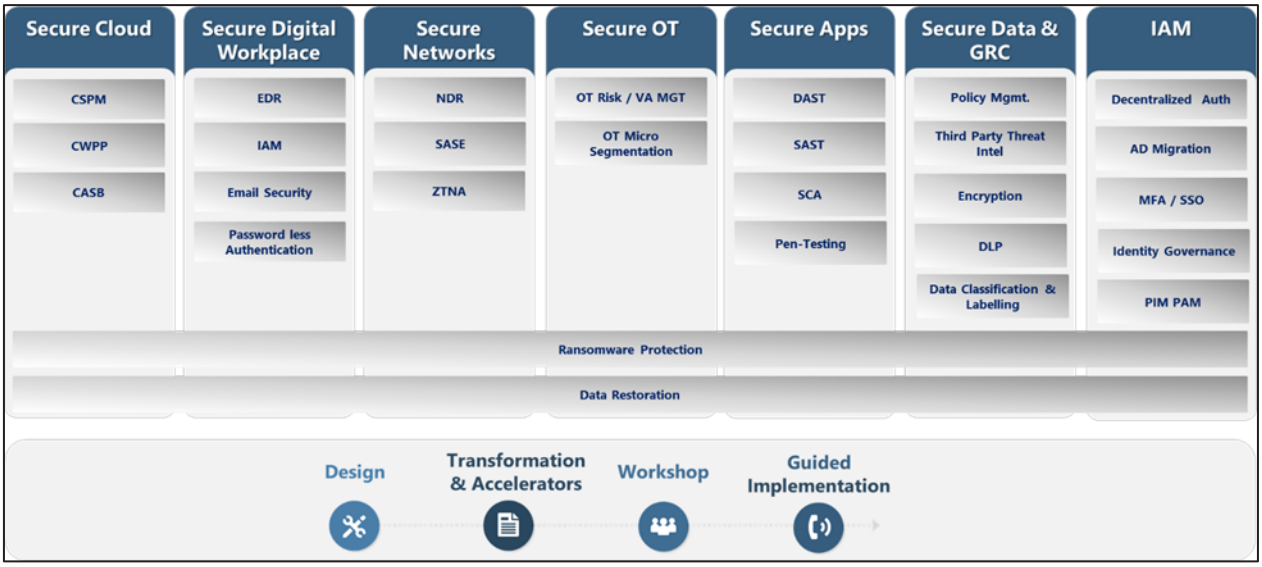
Our Security transformation services are offered to customers as part of the transition phase of Managed Security services or to our existing security customers. As part of technical services, we established a Content Engineering team that provides continuous content development on playbook development and threat-hunting use cases.

Our approach includes:

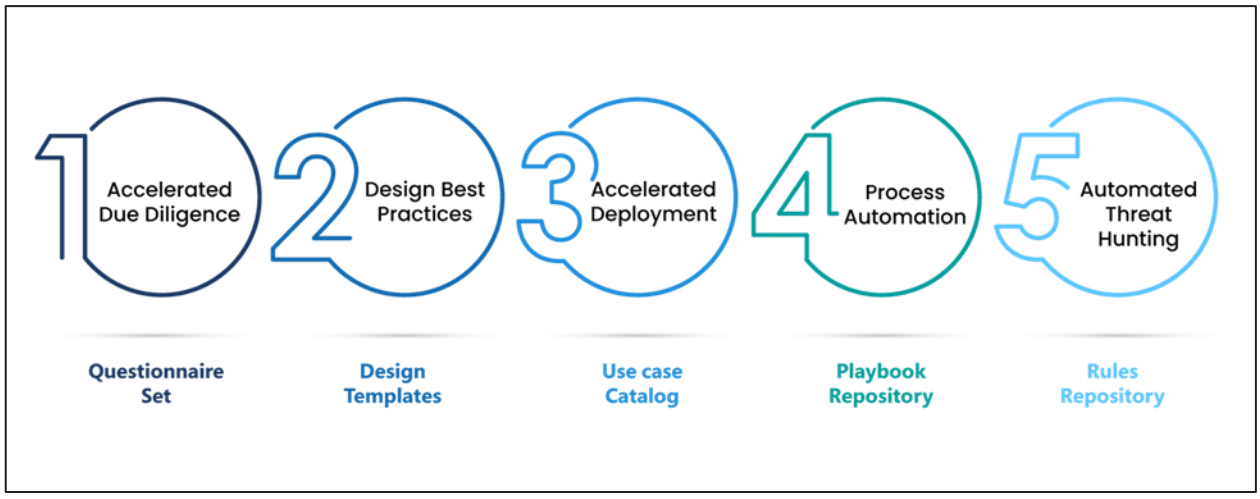
- Right Platform: We advise the right platforms that address the specific needs of the enterprise and collaborate with client teams to ensure seamless adoption.
- Use-case Catalog: We have curated use cases for a multitude of client requirements, challenges, and needs
- Plan: We help prepare an execution plan and define an implementation roadmap with distinct milestones

- Deploy: We provide accelerated deployment as per defined architecture within agreed-upon timelines
- Configure: We ensure all aspects of the solution are aptly configured for the client-specific environment
- Optimize: Our approach ensures we reduce errors and maximize efficiency
- Test: It is our constant endeavor to ensure we meet stringent quality standards that we set for ourselves

The areas of engagement could range across set of technologies and landscape, as depicted below:



We deliver a rapid transformation using accelerators across the following areas:



As a trusted advisor, we are focused on helping customer on security priorities to accelerate business transformation with:

- Autonomous Response & Orchestration package
- SASE deployment accelerators
- Zero Trust evolved IAM service deployment.
- Password Enterprise program - FIDO standards with cost-effective hardware authentication.
- Rapid Onboard Program MDR
- Continuous Threat Content Service
- OT converged MDR service
- Unified DevSecOps (Code scanning, SAST, DAST, SCA analysis, software supply chain protection mitigation)

We have set up a security implementation process that works towards building a comprehensive repository of accelerators, reusable assets, and frameworks for accelerating customer security compliance as per industry standards. Across the below services, we leverage a host of technologies and technology partnerships:

- Identity & Access Management (IAM) services: OKTA, SailPoint, Ensurity
- End user security: SentinelOne, Microsoft, VMware Carbon Black, CrowdStrike
- Network Security: Vehere
- NextGen SIEM with Log management & Onboarding: Securonix, Microsoft Sentinel
- Collaboration Security: Microsoft Defender
- Application Security: CloudDefense
- Cloud Security: CloudDefense
- Risk-based vulnerability management: Balbix
- Comprehensive Cyber risk posture management: CloudDefense, Balbix
- Red Teaming and VA-PT: Multiple platforms

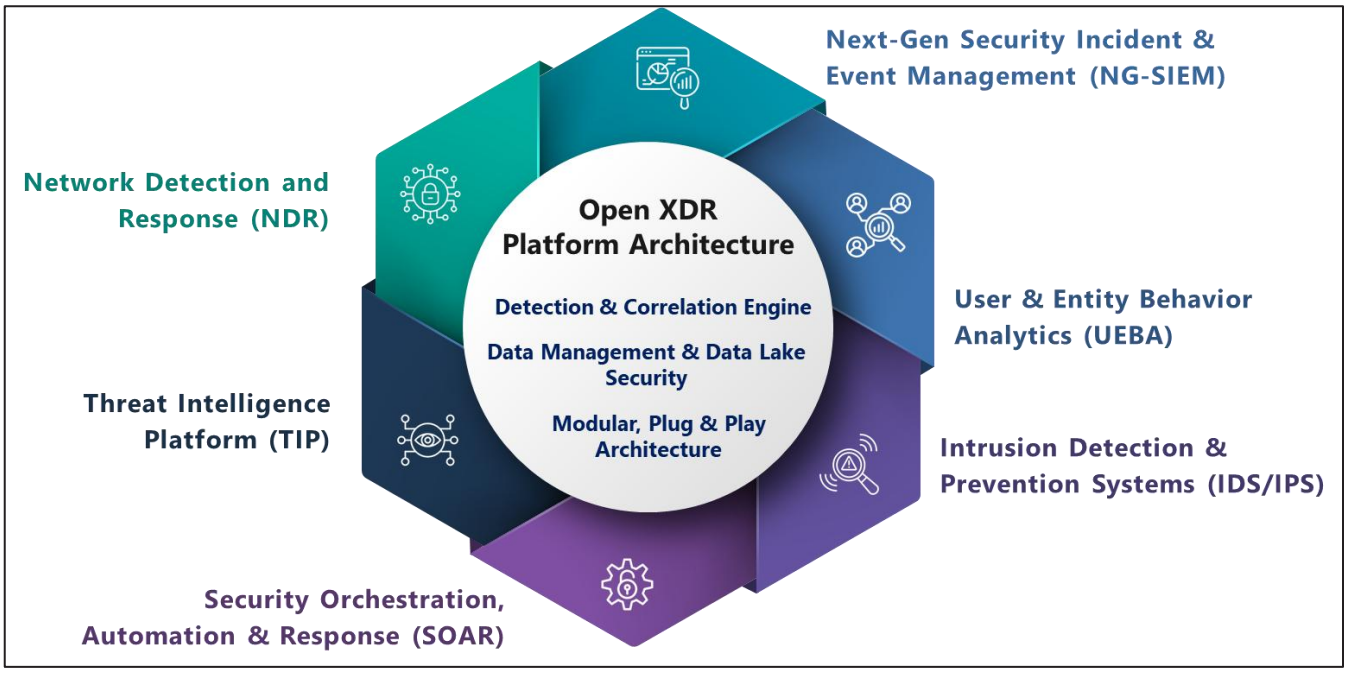
Cyber-Run Services

We offer end-to-end Managed Security Services with our 'Cyber Resilient First' approach which caters to ever dynamic cybersecurity landscape and addresses the requirements of our customers.

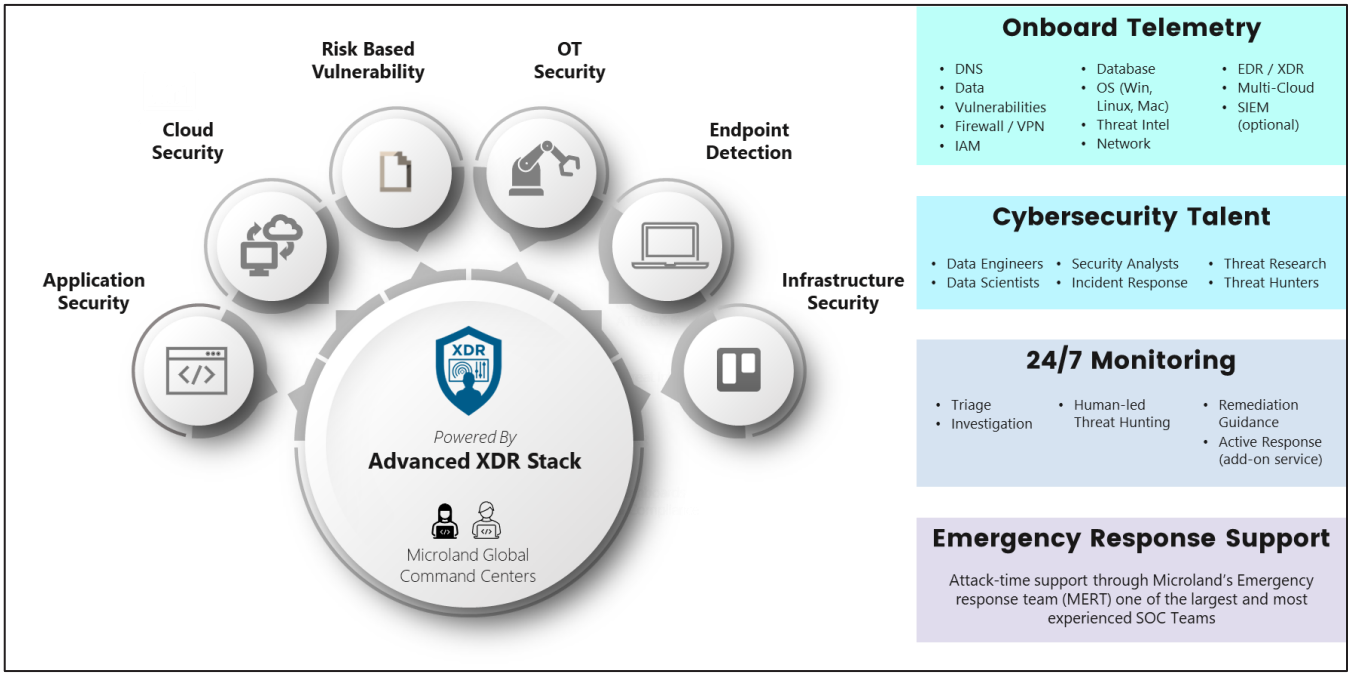
These services are categorized under:

Managed Detection and Response (MDR) Services

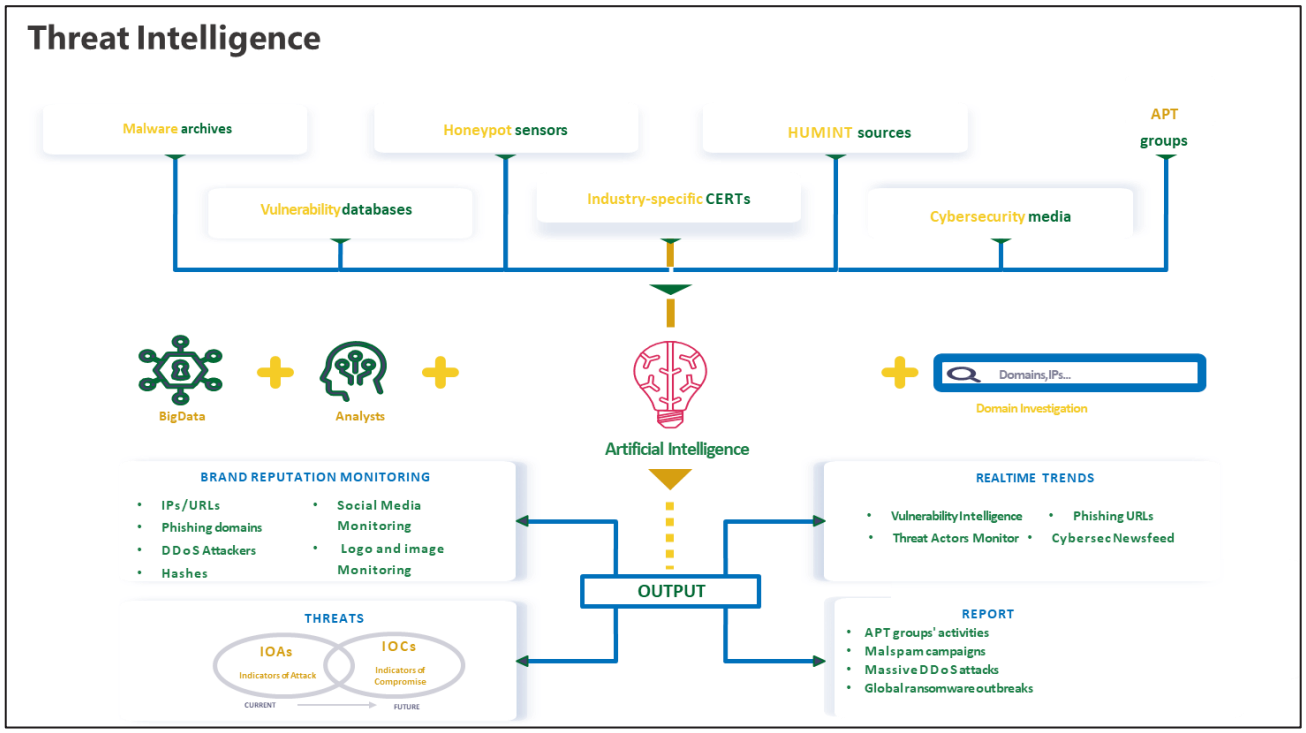
Our NextGen Open XDR Security stack revolutionizes cybersecurity with Platform-driven services, safeguarding enterprise assets across IT/OT infrastructure. Through cross-signal correlation and best-in-class SOC operations, we ensure granular visibility and superior detection. Powered by cutting-edge AI and Machine Learning, our integrated platform delivers autonomous detection and orchestration, covering end-to-end cyber needs. Augmented by our proprietary innovations, our MDR service provides robust defense against threats. OpenXDR compatibility with diverse security products offers unparalleled flexibility and vendor-agnostic capabilities.



Customized MDR Services for impactful defense



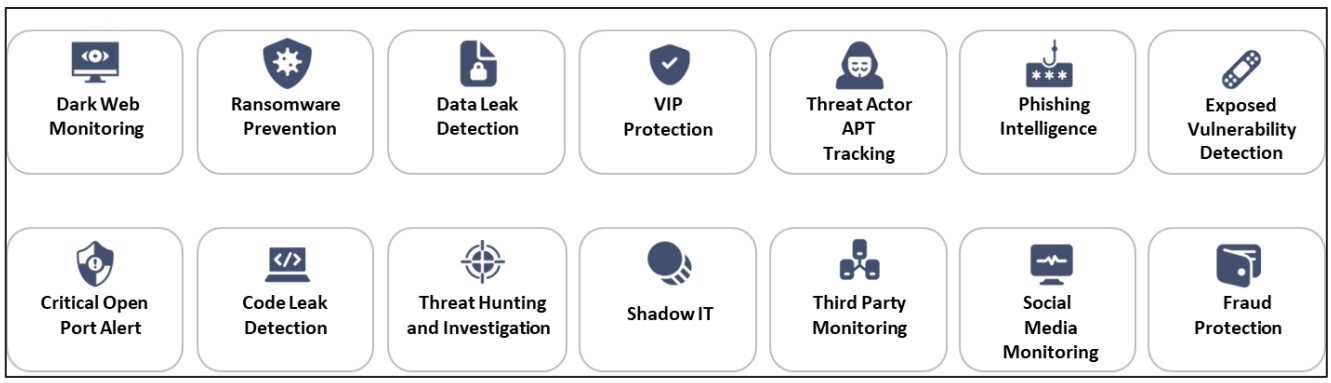
Threat Intelligence for MDR Service Consumption



Dark Web and Cyber Crime Intelligence

Our service (including Partner Team) for dark web and cybercrime intelligence combines the technical expertise of our global threat research and dark web monitoring team with the power of big data to bring in early warning threat intelligence signals and cybercrime insights of relevance and interest to you from across the deep and dark web.

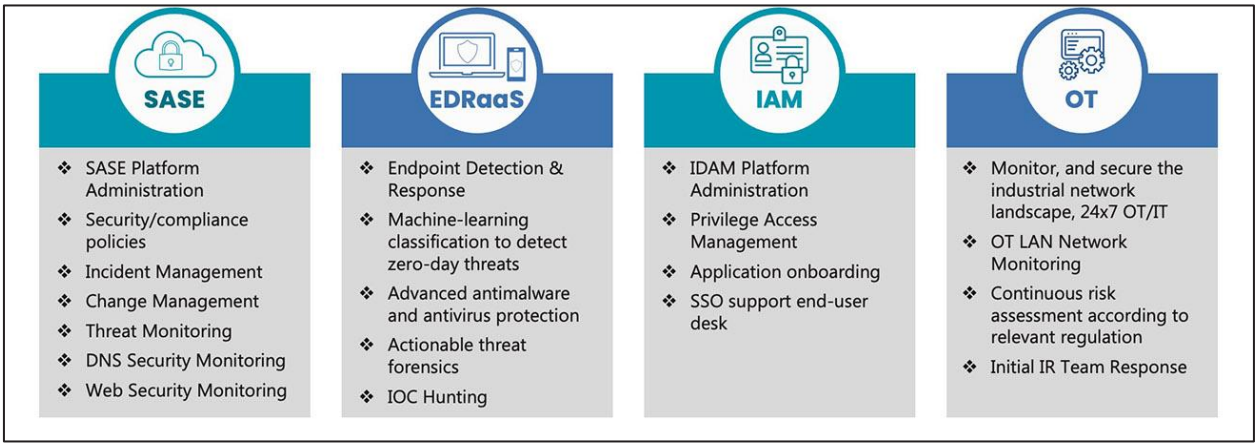
Through our big data analytics and automation platform as well as tradecraft and human intelligence (HUMINT) Cycle gathers terabytes (TB) of data daily across 1700+ cyber-crime forums and dark web forums, ransomware sites, hundreds of Telegram and Discord channels, and other marketplaces to gain unmatched insights into the activities of the threat actors, their targets, their motivations and their tools and techniques.



Managed Security Platform Services

Microland collaborates with cutting-edge technology platform providers to bring end-to-end impact for our clients at the front lines of cyber transformation. We provide a comprehensive ecosystem of managed Cybersecurity platforms, where clients can opt for services such as **Identity and Access Management (IAM), Secure Access Service Edge (SASE), End Point Detection & Response (EDR), Network Detection & Response (NDR), Business Email Security, Data Loss Prevention(DLP)** or choose from a bundle of multiple services packaged as an offering.

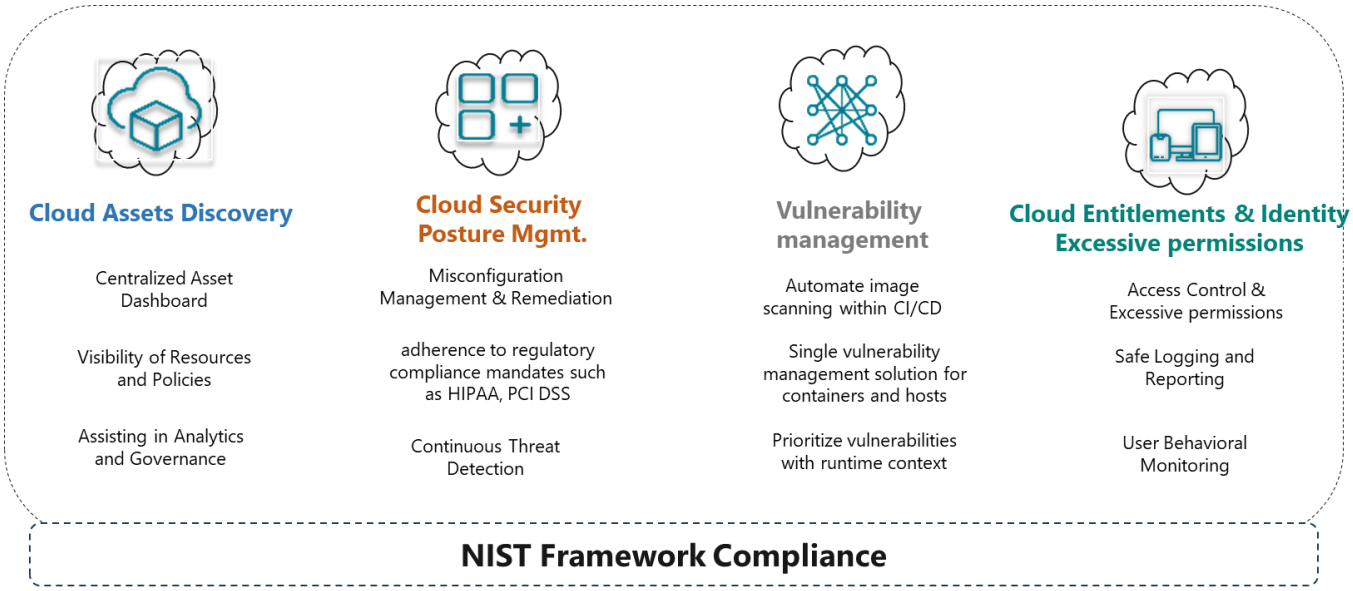
Our Managed Security Platform Services are depicted below:



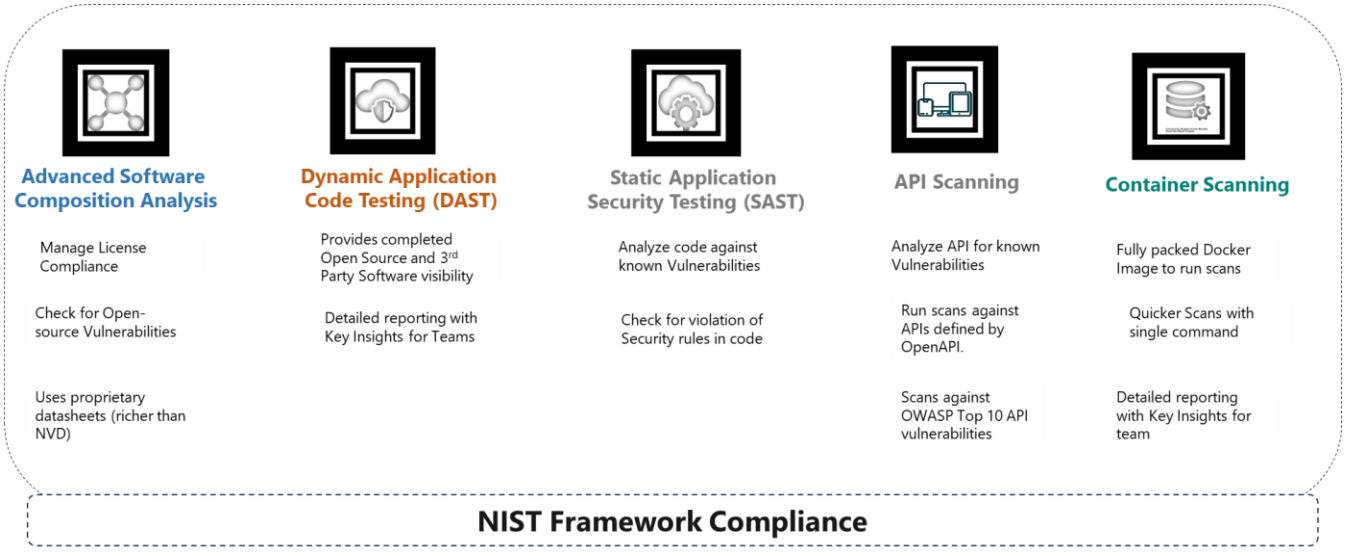
Security Automation

Microland offers cutting-edge cloud security solutions, including CIEM, CWPP, CSPM, DAST, SAST, PAI scanning, and container scanning. Our services ensure real-time threat detection, compliance enforcement, and application vulnerability remediation. Choose from individual options or bundled packages for comprehensive protection. Partner with us for end-to-end cloud security across your digital transformation journey.

Our SecOps Services are depicted below:



CloudSecOps Services

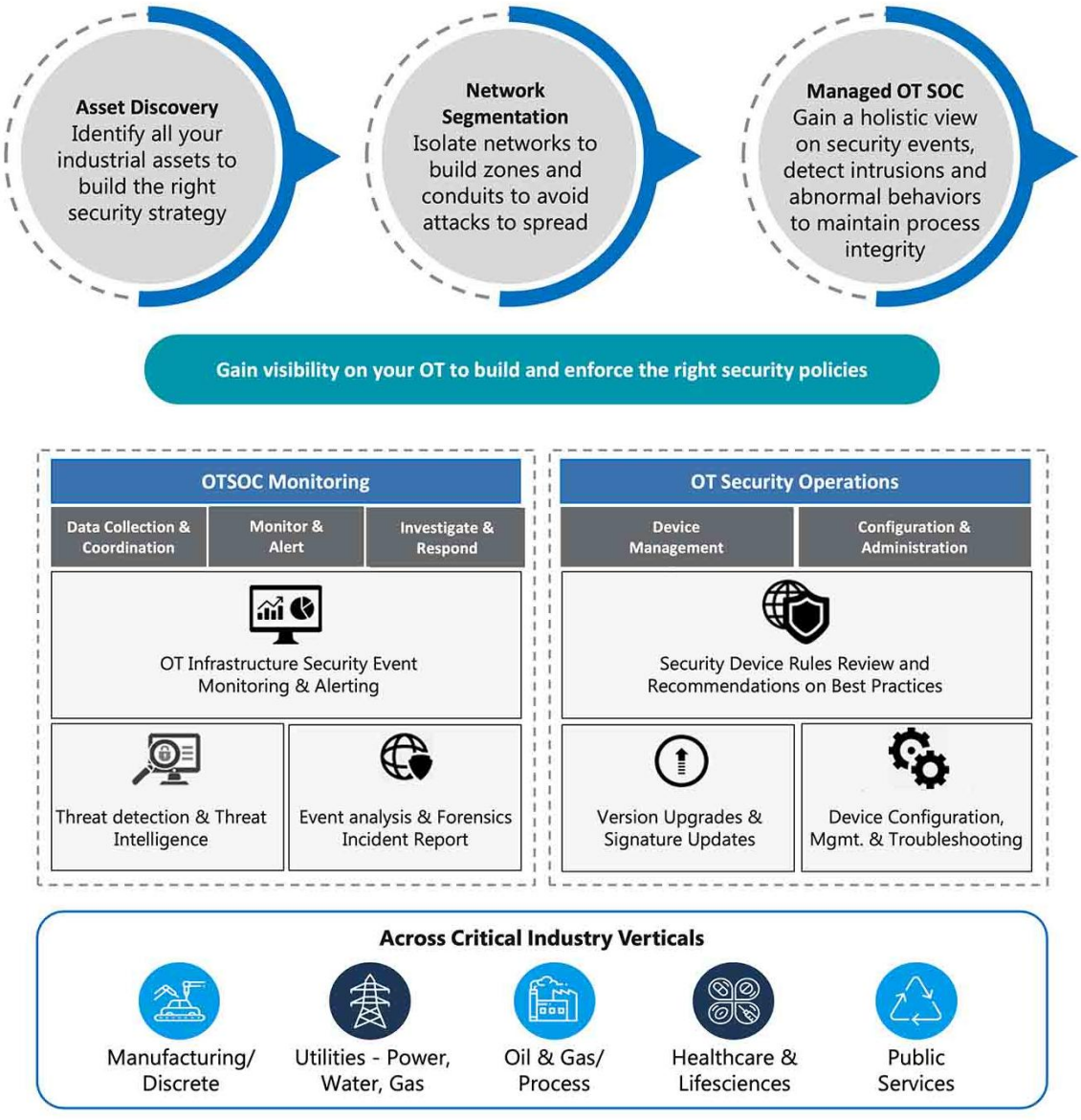


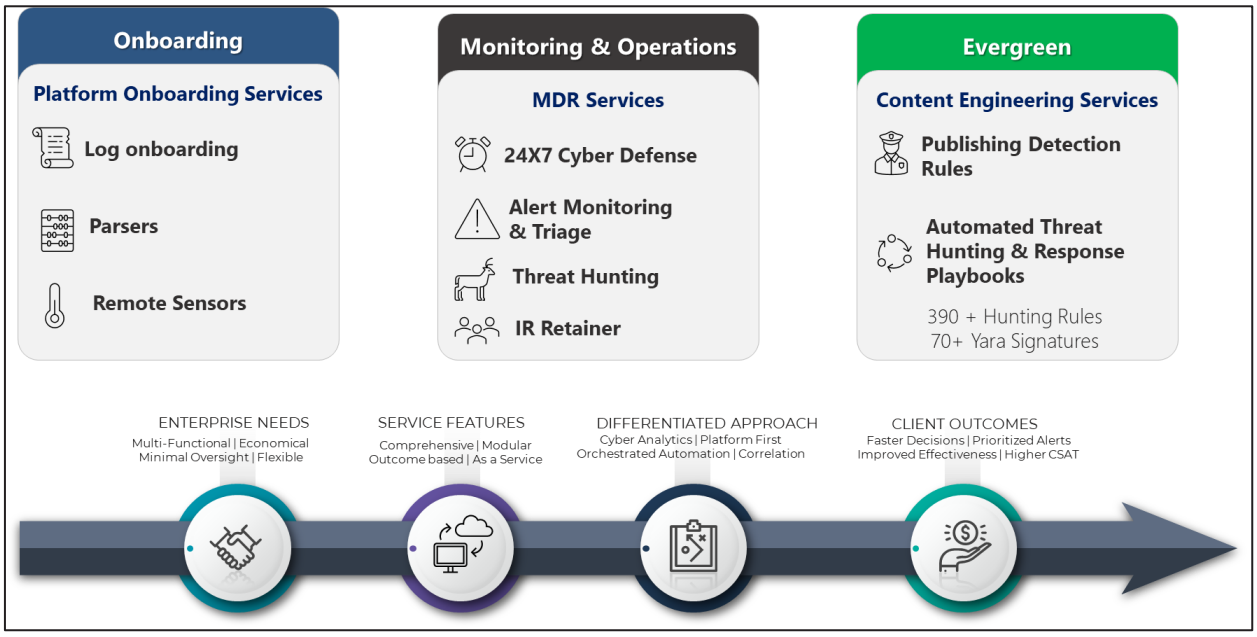
DevSecOps Services

OT Managed Security Services

Unlocking the full potential of Industry 4.0 requires a common, connected, and standardized infrastructure in which people, processes, and technologies can be seamlessly connected. Our services offer a unified approach to engineer, monitor, and secure the industrial network landscape, managed by a remote 24x7 OT/IT Operations Team. We have also reshaped our model of delivery to include co-managed, dedicated, shared hosting models and a combination of dedicated & shared support resources (based on the client landscape).

We take the clients through a step-by-step journey towards achieving the highest standards of OT Security Monitoring & Operations, which in most cases is also industry vertical aligned based on compliances and other industry characteristics.





Through our partnerships with the world's leading cyber technology firms, we can provide best-in-class solutions to accelerate innovation and business transformation for clients.

Microland's ecosystem of cyber alliances is dynamic and continuously evolving with a group of leading organizations which include Microsoft, Securonix, Zscaler, Cysiv, Balbix, CloudDefense, and many more. Also, we collaborate with many cyber startups who bring in innovations and cutting-edge technology to advance our cyber resilience agenda, which results in even greater end-to-end impact for customers at the front lines of cyber transformation.

Microland offers different variants of MDR solutions with a host of partners like:

- Next-gen SIEMs like Securonix, Azure Sentinel, Cysiv (GCP)
    - We offer Azure Sentinel with Microsoft XDR for typical customers with a large Microsoft landscape
- Endpoint Detection & Response (EDR) solutions like Microsoft Defender, Carbon Black, CrowdStrike
- Network Detection & Response (NDR) solutions like Dark Trace, Vehere and Automated Detection & Response (ADR) solutions like LogicApps, Devos SOAR Platforms.

Partnering with Microland with its unique approach of delivering cyber services, presents a range of benefits to clients:

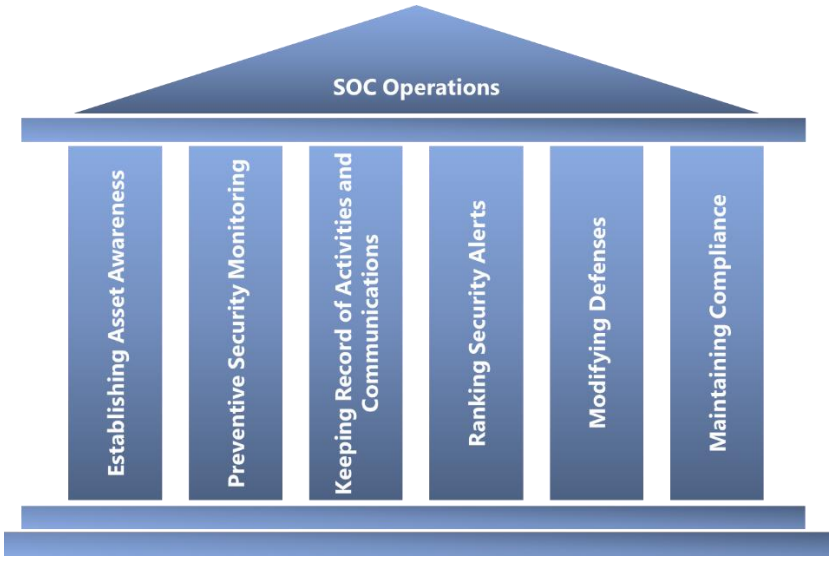
- Flexible service layer (silver, gold, platinum) with fully offshore, onshore, hybrid, and co-managed, with supporting Data Residency for the US, UK, India, Australia, Singapore and ME regions. Microland also provides regional-specific compliance service operations.
- Platform-driven holistic cyber-service with three core layers of speed, response, and elastic scale. With our MicroShield platform and operating model, clients have the flexibility powered by the cloud, with the right operating model that is tailored to them.
- Manage your IT-OT with edge security with monitoring and security logs for all edge activity, particularly activity relating to operations and configurations.
- 24x7 management with alert-focused threat monitoring, triaging, and containment automated platforms.
- Threat Intelligence and Threat hunting with tailored use case deployment
- Automation and Orchestration with over 270 connectors and over 100 playbooks
- Advanced services for incident response and remediation with Forensics services supported by Microland Global defence centers
- Microland's MDR team of Data Scientists and Content engineering team, Blue Team defender analysts and Purple team, Red Team threat researchers and hunters, and incident response professionals operate as an extension to the client's organization and collaborate to defend client assets to further help elevate its overall security posture.

Microland SOC Services

Microland has a holistic approach to providing Managed SOC services. The approach is based on the underlying principle that Microland follows. This is also supported by adherence to the agreed service window and service levels.

Principles of SOC Operations

Microland's security operations are based on six tenets which allows us to develop a comprehensive approach towards cybersecurity.



1. **Establishing Asset Awareness**: Asset discovery is one of the vital activities before we start monitoring the estate. This baselines the state for monitoring. The asset (and identity) data can be collected from various sources within the organization such as CMDB, SCOM, LDAP, and Active Directory.

2. **Preventive Security Monitoring**: When it comes to cybersecurity, prevention is always going to be more effective than being reactive. Rather than responding to threats as they happen, our SOC team will work to monitor a network around the clock. By doing so, they can detect malicious activities and prevent them before they can cause any severe damage to the estate.

3. **Keeping record of Activities and Communications**: In the event of a security incident, SOC analysts need to be able to retrace activities and communications on a network to find out what went wrong. To do this, the team is tasked with a detailed log management of all the activity and communications that take place on the network.

4. **Ranking Security Alerts**: When security incidents occur, the incident response team works to triage the severity. This enables a SOC to prioritize its focus on preventing and responding to security alerts that are especially serious or dangerous to the business.

5. **Modifying Defenses**: Effective cybersecurity is a process of continuous improvement. To keep up with the ever-changing landscape of cyber threats, our security operations center works to intimate respective teams to continually adapt and modify a network's defenses on an ongoing, as-needed basis.

6. **Maintaining Compliances**: In addition to threat management, a security operation center also must protect the business from legal trouble. This is done by ensuring that they are always compliant with the latest security regulations.

Scope of SOC Services

Development and Onboarding

- Assist with the deployment, and configuration of SIEM & other Security tools
- Onboarding of end-user devices on the EDR tool
- Onboarding of data center assets and management tools to SIEM
- Creation of initial use cases on SIEM

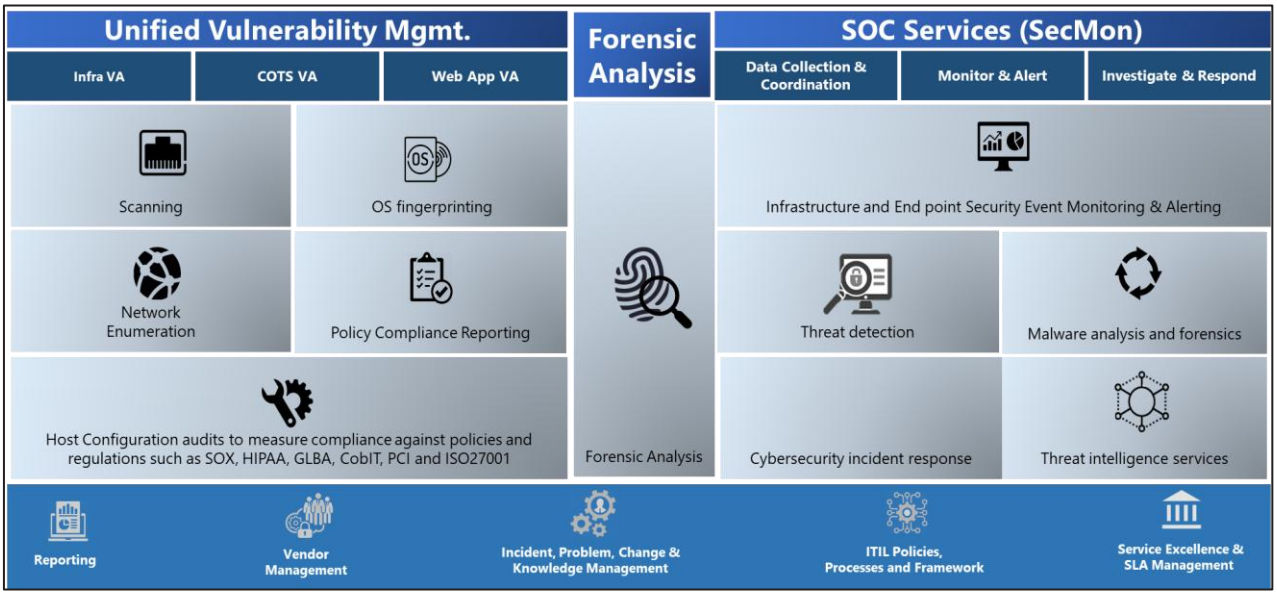
SOC Operations

- Monitoring Security incident and alerting
- Threat detection
- Malware analysis
- Cybersecurity incident and response
- Threat intelligence services
- Vulnerability scanning of all external ranges and internal system
- Assessment of security protection of key systems
- Identifying and reporting Identity management vulnerability
- Identifying and reporting Patching in compliance and vulnerability
- Identifying false positive targets
- Supporting Local resources for containment and resolution of incidents
- Root cause analysis
- Post incident - provide a detailed report of the incident including root cause, timeline, remediation, and recommendations
- Forensic analysis service capable of detailed investigation particularly focuses on data loss post incident but also able to support internal investigation such a legal / HR
- Policy and Compliance reporting
- Security device rule review and recommendations
- New query configuration on SIEM

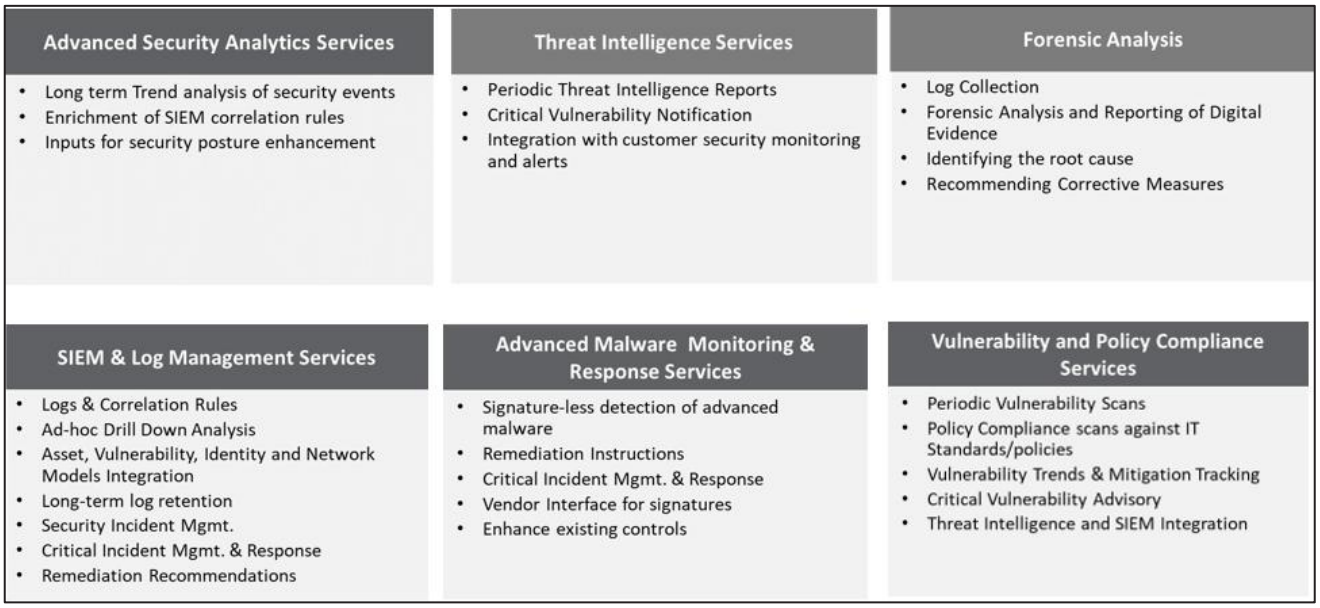
SOC Operating Model

To support the customer to achieve its targeted cyber maturity, we are looking at the holistic approach to get the desired future estate and retain the elements of current estate to reap-

out benefits. The target operating model post we implement out solution will be simplified and futuristic.



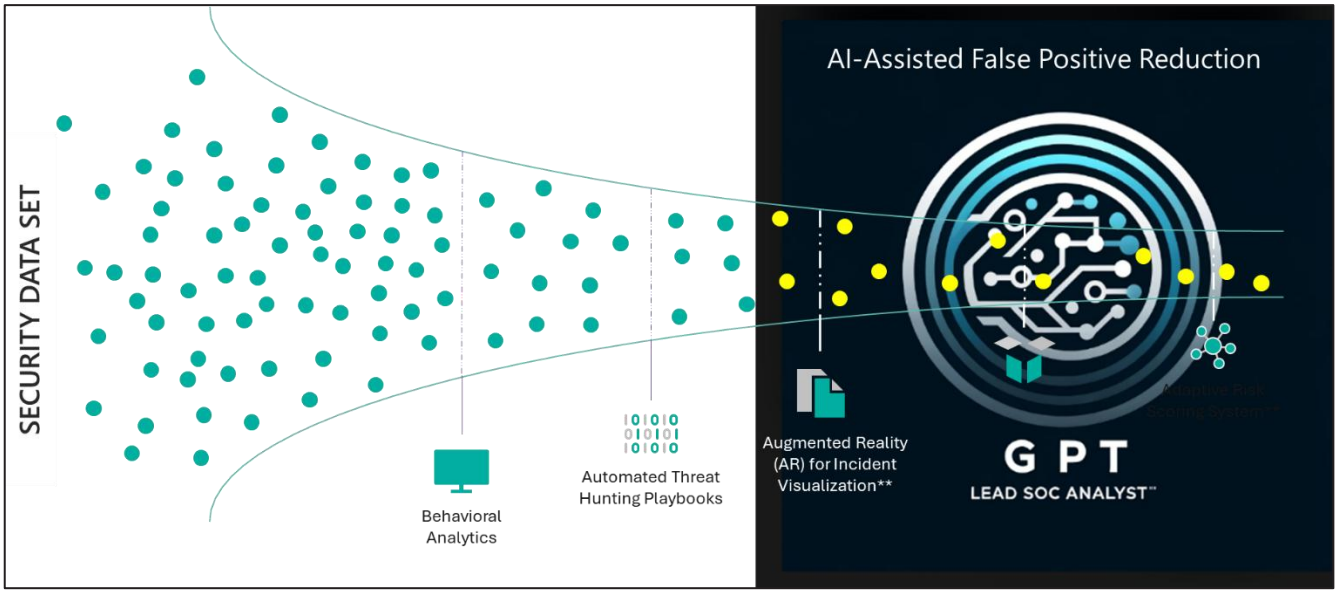
The target operating model has three key pillars from service perspective – SOC Services, Vulnerability Assessment and Forensic Analysis. Under these tower Microland team will be delivering following services.



Our framework for SOC Maturity

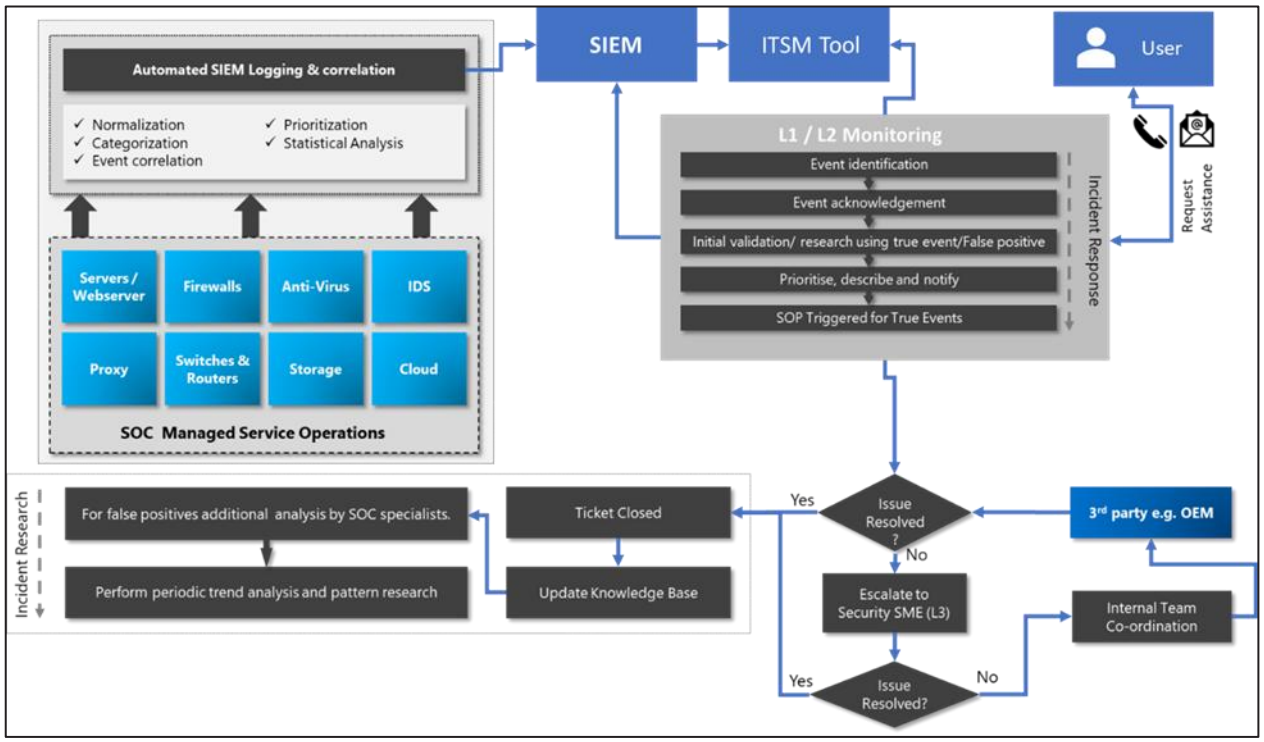
	Maturity Levels	Gen I - Security (Siloed Detection & Prevention)	Gen II - SOC	Gen III - Reactive SOC	Gen IV – XDR	Gen V - AI Defense
Technology	SIEM	---	Traditional SIEM	NextGen SIEM	XDR Platform	XDR platform
Technology	Network	Firewalls IDS Proxies Web Application Firewalls	IPS Vulnerability Management Sandboxing	Secure Web & Email Gateways Deception Technology	NextGen Firewall TIP & Dark-web Monitoring SOAR	MDR with AI Analytics AI Led Contextualization and threat containment
Technology	Endpoint	Anti-Virus Anti-Malware	Endpoint Protection (EPP) IAM & Authentication DNS & DHCP Email Filtering	Basic EDR & DLP Access Management Email Security CASB	EDR with Remediation UEBA	EDR with Deep Telemetry capabilities
Capabilities	Process	Siloed Monitoring & Detection	24x7 Monitoring & Alerting Threat Intelligence Compliance Mgmt.	Incident Playbooks Use-cases Incident Forensics Security Roadmap	Playbooks Distributed Deception Behavior analytic	Autonomous Defense Response NLP Quantum defense Software supply chain
Capabilities	People	IT Network & Security Team	Dedicated SOC Analysts & Security Engineers	Incident Response (IR)	Threat Hunters & Data Scientists	Integrated SOC Team

Harnessing AI in our Security Operations Center



SOC Delivery Model

SOC Architecture

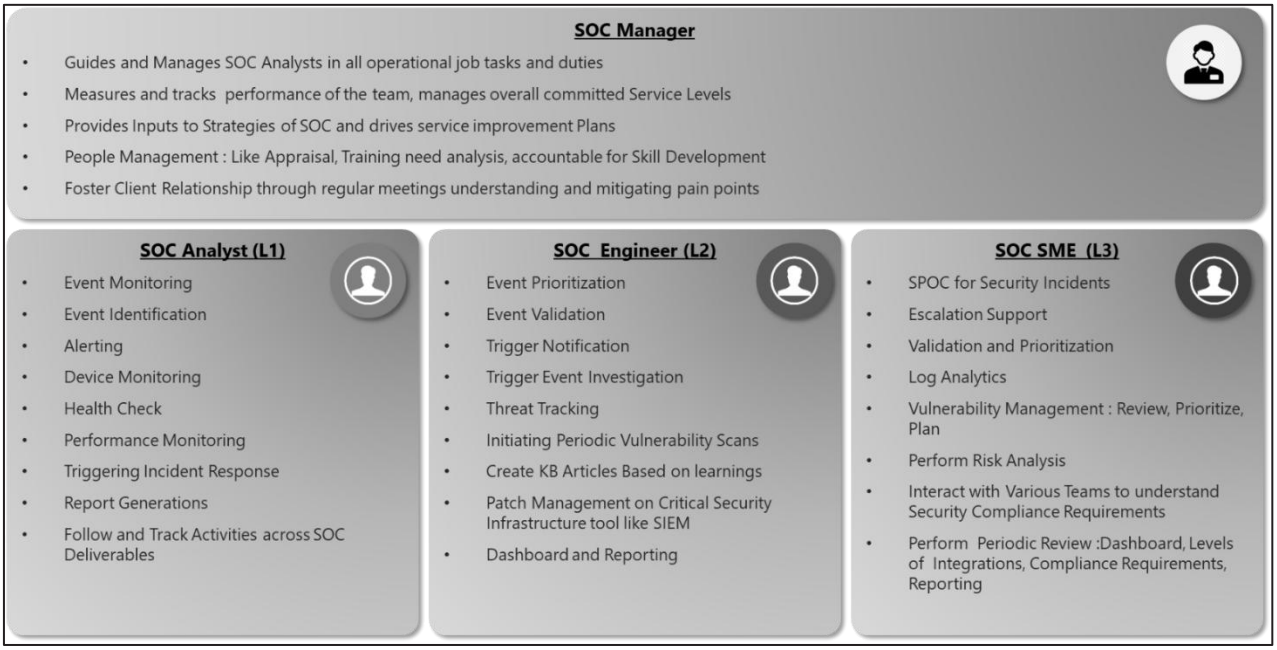


The SIEM solution deployed keeps on monitoring/analyzing the events that are produced by the assets in the estate. If auto ticketing is configured in the SIEM tool, it will log an incident in the ITSM tool (SCSM). The SOC team can also be reached for a probable incident/request by the internal team through phone or email. In that case, the team asked the requestor to log a ticket/request in ITSM to ensure it's tracked to closure.

These tickets will be picked up by our L1 / L2 team who will run a few checks to identify and see if it's not a false positive case. In case it's a true incident, based on the priority the team picks and starts working on the issue. If it's a known issue and a corresponding SOP is available, the team runs the SOP and closes the ticket once fixed.

Our SOC Structure

A high-level team structure of Microland's SOC team is shown below:



Our Managed SOC Deliverables

Items	Descriptions
SIEM & Log Management Services	• Logs & Correlation Rules • Ad-hoc Drill Down Analysis • Asset, Vulnerability, Identity and Network Models Integration • Long-term log retention • Security Incident Mgmt. • Critical Incident Mgmt. & Response • Remediation Recommendations • Manage Customer provided tools
Deep Inspection Services	• Add-on to SIEM Services • Additional Data, Application, Identity & Compliance use cases • Increased Security Visibility into IT environment
Vulnerability and Policy Compliance Services	• Periodic Vulnerability Scans • Policy Compliance scans against IT Standards/policies • Vulnerability Trends & Mitigation Tracking • Critical Vulnerability Advisory

Items	Descriptions
	• Threat Intelligence and SIEM Integration
Advanced Malware Monitoring & Response Services	• Signature-less detection of advanced malware • Remediation Instructions • Critical Incident Mgmt. & Response • Vendor Interface for signatures • Enhance existing controls • 24x7 monitoring of events and incidents • Alert and respond to suspicious and malicious events • Document all steps when responding and share with the point of contact in Customer organization • Coordinate and act as a technical point of contact during incident response • Conduct investigations and assist during the response • Provide root cause assessment and lessons learned after an incident • Prioritize events based on criticality • Assist with user training and education • Develop use cases and workflows to common events • Work with third-party vendors for issue resolution during critical failures and when required • Provide insights and analysis (reports) of current trends and vulnerabilities or exploits in the wild or in the news
Advanced Security Analytics Services	• Long term Trend analysis of security events • Enrichment of SIEM correlation rules • Inputs for security posture enhancement
Threat Intelligence Services	• Periodic Threat Intelligence Reports • Critical Vulnerability Notification • Integration with customer security monitoring and alerts • Perform proactive analysis to find issues before they turn into problems • Produce reports as mentioned below:

Produce report as mentioned below:

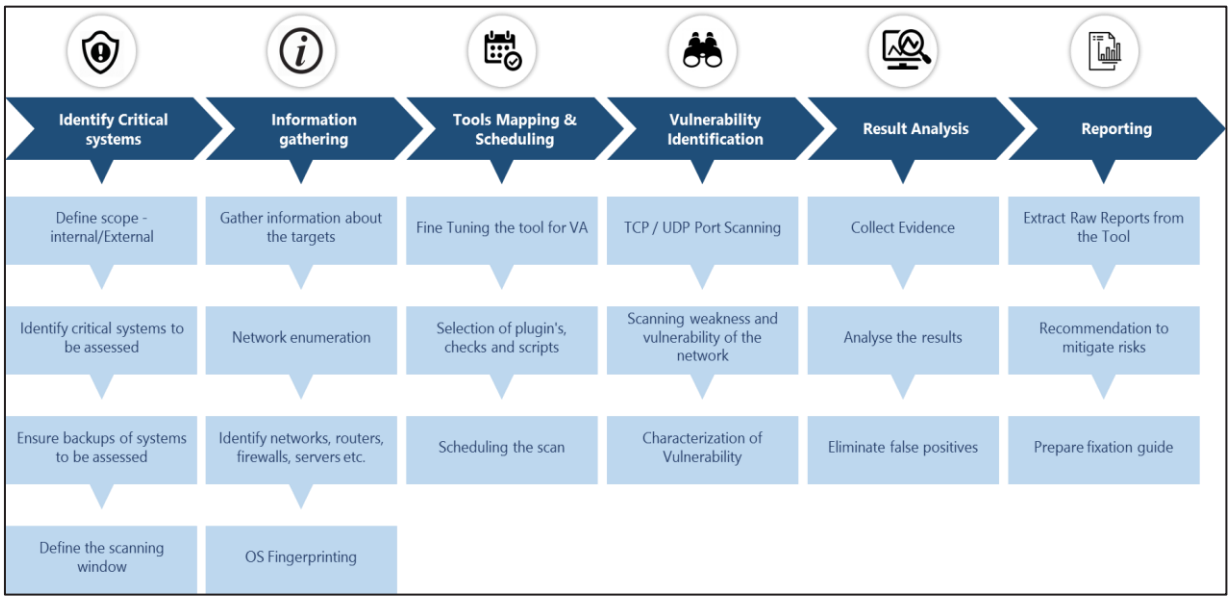
S. No	Report	Frequency
1	AV Compliance Report	Weekly, Monthly
2	SOC Report (No. of devices monitored, No. of EPS, Top 10 events identified, Action taken, Key risks identified)	Weekly, Monthly
3	Vulnerability Assessment Report	Monthly

RACI Matrix

Activities	Customer	Microland SOC
Alert and Warning	IC	RA
Event Data Retention	IC	RA
Executive Security Reporting	IC	RA
Incident Classification	IC	RA
Incident Identification	IC	RA
Incident Notification	IC	RA
Incident Recovery / Resolution	RA	IC
Incident Response	IC	RA
Incident Tracking and Tracing	IC	RA
Policy Compliance	RA	IC
Policy Enforcement	RA	IC
Policy Management	RA	IC
Real-Time Device Event Monitoring	IC	RA
Risk Assessment	IC	RA
Risk Management	RA	IC
Root Cause Analysis	IC	RA
Security Audits	RA	IC
Security Consulting	RA	IC
Technical Reporting	IC	RA
Vulnerability Assessment	IC	RA
Vulnerability Mitigation	RA	IC

Vulnerability Assessment

Vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Vulnerability assessment will be carried out on the assets of the customer every month to proactively detect security vulnerabilities. Microland will use the VA Scanning tool for vulnerability assessment to identify infrastructure vulnerabilities. The below methodology defines the Vulnerability assessment approach.



Vulnerability Assessment Services

Vulnerability Assessment Services include:

- Catalogue Customer's Information Technology (IT) assets and resources (e.g., applications, database, endpoint devices, network and servers), as requested
- Assess current security measures to identify any vulnerability that exists in the customer's network, assets, and resources.
- Conduct wireless security assessment
- Conduct personal security awareness assessment
- Analyze and report vulnerabilities

Vulnerability Assessment Services Reporting and Presentation

Upon completion of each Service, Microland will provide the customer with a vulnerability assessment report which includes the following information at a minimum:

- Detailed results of identified vulnerabilities

- Detailed explanation of the implications of the identified vulnerabilities, business impact, and potential risks
- Detailed steps for immediate mitigation
- Recommended high-risk areas for Customer's immediate attention, as applicable and
- Deliver a presentation to the customer, as requested.

Service Level Agreement (SLA)

Severity Level	Description	Response Time	Escalation Time
Severity 1	Device down, connectivity down	15 mins.*	30 mins.
Severity 2	Port scanning, virus activity	20 mins.	60 mins.
Severity 3	Abnormal traffic, drop packets	45 mins.	120 mins.
Severity 4 (technical advisory)	Vulnerability disclosure/global threat detection/zero-day attacks	Within 24 hrs. of the release of the advisory	
Service Request	Any new change to be	1 business day	
On-Demand Reports	New report template	1 business day	
	Ad-hoc request for reports	1 business day	
Use Cases	Create a new use case	1 business day	
	Modify existing use case	1 business day	
Response time: time taken by the analyst to prioritize and assign the ticket to their name (Ticket acceptance time) Escalation time: Case escalation time – case creation time (time taken for event investigation)			

1. **Severity 1 (Critical)** An emergency severity level [1] impacts everyone or a very large number of critical business processes. Incidents that may become an emergency and are not under control can also be declared emergency or crisis.

   Type of issues: -

   - Connectivity is down, and monitoring is affected
   - Critical situation like System Down or component is down
   - When magnitude is greater than 8

     99% SLA should be met over the total true positive incidents reported in the measured period.

2. **Severity 2 (High)** An urgent severity incident [2] impacts the 'core business' or multiple End-users groups. These high-risk events/policy violations have the potential to cause severe damage to client environments.

   Type of issues: -

- System or data compromises
- Privacy breaches
- enterprise-wide malware outbreak and worm infections/propagation
- significant Denial of Service (DoS) or small size Distributed Denial of Service (DDoS) attacks
- zero-day threats that manifest or apply to our infrastructure
- Unauthorized user privileges escalation
- tampering with critical system files, application files, or databases that will impact system integrity
- Unauthorized (system) policy changes
- unauthorized change of audit log files

95% SLA should be met over the total true positive incidents reported in the measured period

3. **Severity 3 (Medium)** An urgent severity incident [3] impacts the 'core business' or multiple End-users groups. These unauthorized user activities cannot impact system performance or harm data.

   Type of issues:

   - Unauthorized internal scanning activity
   - Attacks targeted at specific servers or workstations
   - Unauthorized creation of ids on critical systems
   - User- caused contiguous failed/successful login attempts
   - Failed attempts of tampering with critical systems, applications, audit log files, and databases
   - Unauthorized accessing critical systems or application files
   - Malware outbreaks impacting a single business unit or a territory

   95% SLA should be met over the total true positive incidents reported in the measured period

4. **Severity 4 (Low)** A service request created on the ticketing tool or sent through the mail

   Type of Service Request:

   - Logs for specific time or device
   - Troubleshooting of logs not reporting to SIEM
   - Creation or deletion of user ID, or changing the access of user IDs

Unified Vulnerability Management

Win the security game—proactively identify vulnerabilities and protect data

When large-scale digital transformation and technologies like cloud and mobility open the doors to new business opportunities, agility, and efficiencies, they also expose the organization to increased breaches. Identifying and remedying vulnerabilities in an enterprise's security systems has become one of the most demanding tasks for specialists. This is where Microland's Unified Vulnerability Management (UVM) solution which complies with industry standards like ITIL, ITSM, and ISO 27000 comes into play.

UVM is our real-time, end-to-end solution that complies with industry standards like ITIL, ITSM, and ISO 27000 and uses best-in-class, industry-recognized tools to scan, discover, report, and remediate vulnerabilities and improve protection. A dashboard also provides leadership with critical real-time views on their organization's security posture while reducing security spending by up to 30%.

As part of unified vulnerability management, we perform the following:

- Define and design Vulnerability Management governance model
- Identify tools/platform based on the customer requirement and deploy
- Web Application Security Scanning
- Define scan policies
- Define and manage target assets
- Schedule scans and execute it without business interruption
- False positive analysis and elimination
- Vulnerability prioritization
- Reporting with KPIs & KRIs
- Follow-up assistance on remediation
- Re-scanning for patched vulnerabilities

Digital Forensics and Incident Response

When large-scale digital transformation and technologies like cloud and mobility open the doors to new business opportunities, agility, and efficiencies, they also expose the organization to increased breaches. Identifying and remedying vulnerabilities in an enterprise's security systems has become one of the most demanding tasks for specialists.

With confidentiality, integrity, and transparency as pillars, our vision is to provide support in managing incidents, defend client organizations against cyber threats, and resolve and recover

in case of unexpected incidents. To bring our tools, technology, and expertise to the forefront of the fight against threats, as a trusted partner.

Below are the areas we cover in our DFIR service offerings:

1. **Pre-attack services**: Engage in posture assessment and threat mapping to identify risk portions as part of proactive engagements. Tailored IR procedures are chalked out for various possibilities such as data breaches, ransomware, malware, inside threats, and other cyber threats.

2. **Incident Response - Detection and Analysis**: Quick and almost live response to contain the incident and recover from it. Our response solution is available both as emergency services as well as continuous detection services for our clients.

3. **Malware Analysis & Threat Detection**: Active search for the threat actors and signs of compromise and providing real-time cyber threat Intel with up-to-date IOCs as ongoing support services in SOC/MDR/XDR Services.

4. **Forensic Assessment**: Understanding the root cause and detailing the analysis of the incident and data elements that have caused the breach/attack.

5. **Post-Attack services**: Collecting the evidence and footprints of the threat actors, assisting with the potential criminal procedures, and handling the documentation and storage recovery.

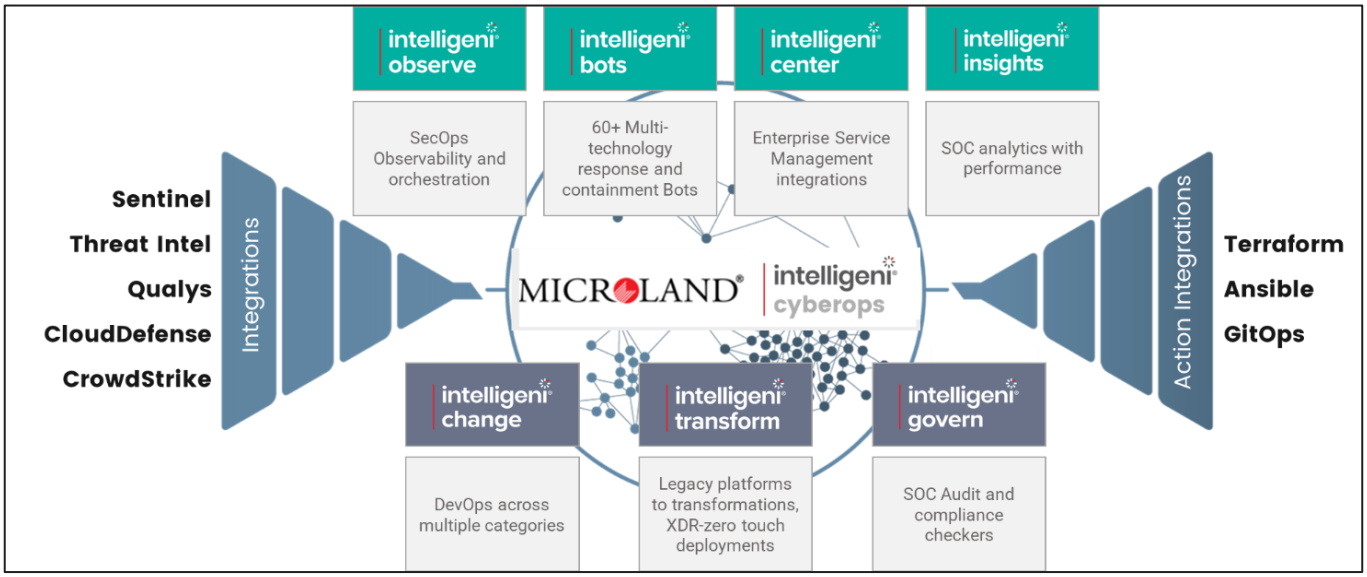
Our DFIR practices being aligned to the industry standards is fundamental as it guides the implementation and engagement of our DFIR processes. We make sure to follow them at every phase of our services:

- SANS: SANS's Incident handling guidance provides a systematic approach to the handling processes of incidents. Our handling phases are aligned as they describe the different tasks and their sequence in preparation, Identification, containment, eradication, and recovery.
- NIST framework: While SANS guides us through detailed phases of DFIR implementation, NIST Cybersecurity Framework gives us the top-view structure - Identify, Detect, Respond, and Recover. We delve deeper into each category and map them to SANS guidelines to enhance our DFIR capabilities.

- NIST 800-61: This security incident handling guide offers detailed guidance on managing incident response. We take out notes from the detection, analysis, containing, eradicating, and recovering methodologies
- MITRE ATT&CK framework: This knowledge pool of framework on the Adversary techniques and tactics is frequently used by our Red and Blue teams. This helps them to create the procedures for various kinds of scenarios in case of incidents, malware attacks, or breaches

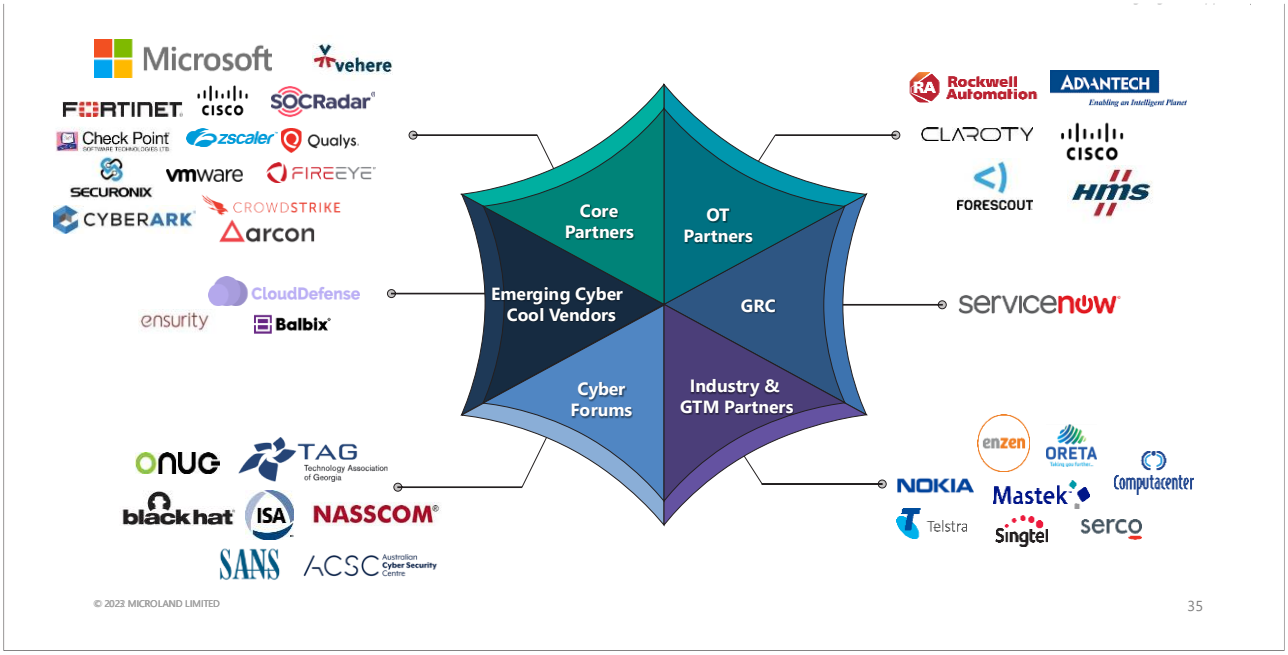
We also count on ISO and other information-sharing and collaboration frameworks for guidance on establishing processes, implementing technologies, and handling incidents.

Microland Security & Observability - CyberOps



Tools

The SOC services can be delivered using Microland-provided tools, customer-provided tools to maximize your investments in technology or a combination of both. Microland's tools include the following:



Why Microland?

Trust & Transparency

25 years+, Microland cyber services has remained resilient, standing as a testament to unwavering trust and transparency

Not a Vendor, but a Partner

Microland in its service delivery excellence and customer centricity goes beyond the role of a vendor to being a partner to its customers and supports the customers beyond the scope of services to drive business outcomes

Flexibility & Agility

Being vendor-agnostic, we leverage the best platforms and solutions that address the unique needs and challenges of the customers. Leveraging Intelligeni, our automation and AIOps platform we are agile and flexible to deploy solutions rapidly for customers

Adaptive Cyber-Strategy

Investing in innovation, platform development, strategic partnerships, and leveraging the latest advanced technologies like AI/ML, automation, Big Data, and analytics, industry-leading tools, and platforms to build best-in-class, integrated OpenXDR-based solutions