

# Hexaware Security Services - Snapshot

Customers – 80+	Employee Spread	Scale of Operations	
<ul style="list-style-type: none"> <li>24x7 MSSP servicing multiple customers across verticals &amp; geographies offering the complete gamut of security services.</li> </ul>	<ul style="list-style-type: none"> <li>300+ Security SME's</li> <li>24% Americas, 9% EMEA, 67% APAC</li> </ul>	<ul style="list-style-type: none"> <li>100,000+ Signals monitored</li> <li>5,000+ identifies &amp; Governed .</li> <li>35+ SOC Delivered customers.</li> <li>28+ GRC Audit projects completed</li> </ul>	<ul style="list-style-type: none"> <li>Certified Professionals carrying:</li> <li>CCSA, SCSA, ECSA, CCSE, CCNP, CEH, CCDA, CCSE+, CISSP, CISA, CISM, CRISC, TOGAF, CCIE, ISO27K certifications</li> </ul>

Security Service Offerings		Service Delivery Excellence
<p><b>Predictive Security</b></p> <ul style="list-style-type: none"> <li>Extended Detection &amp; Response</li> <li>Threat Modelling</li> <li>User Entity Behavioral Analytics</li> </ul> <p><b>Preventive Security</b></p> <ul style="list-style-type: none"> <li>Privileged Identity Management</li> <li>Identity Governance &amp; Administration</li> <li>Data Protection</li> <li>Certificate &amp; Key Management</li> <li>Endpoint Security</li> <li>Network &amp; Perimeter Security</li> <li>Dark Web &amp; Cyber Brand Protection</li> <li>Security User Awareness</li> </ul>	<p><b>Detection Security</b></p> <ul style="list-style-type: none"> <li>SIEM &amp; SOC</li> <li>Sandbox Detection.</li> <li>Application Security</li> <li>Vulnerability Management &amp; Penetration Testing</li> <li>Red Teaming &amp; Incident Response</li> </ul> <p><b>Remediation Security</b></p> <ul style="list-style-type: none"> <li>Endpoint Detection &amp; Response</li> <li>Security Orchestration &amp; Automated Response</li> </ul> <p><b>Compliance &amp; Reporting</b></p> <ul style="list-style-type: none"> <li>Evidence Collection &amp; Reporting</li> <li>Security Assessments to frameworks and standards</li> <li>Compliance Dashboarding</li> <li>Continuous cloud compliance</li> </ul>	<ul style="list-style-type: none"> <li>Next Generation Security Operations Platform</li> <li>Security Platform as a Service for SIEM, SOAR, VM, EDR, XDR etc. aligned to business needs.</li> <li>&gt;35% Automation-based efficiencies</li> <li>Our Tensai for SecOps frameworks leverages industry best practices and frameworks</li> <li>Full Stack SMEs with continuous skill upgrade</li> <li>COE lab Access for expert advises</li> <li>Red team and Blue team for Emergency responses</li> </ul> <p><b>Sample Engagements</b></p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">   <small>Powering Today. Protecting Tomorrow.</small> </div> <div style="text-align: center;">  </div> <div style="text-align: center;">  </div> <div style="text-align: center;">  </div> <div style="text-align: center;">  </div> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 10px;"> <div style="text-align: center;">  </div> <div style="text-align: center;">  </div> <div style="text-align: center;">   <small>To a Future With More Cheers</small> </div> <div style="text-align: center;">  </div> <div style="text-align: center;">  </div> </div>

# Our Security Service Themes



## Predictive Security Posture

- ML/AI to Empower customers with predictive threat detection.
- Actionable Insights and Early Warning
- Behavior-Based Anomaly Detection
- Advanced Threat Intelligence Integration or Proactive Threat Hunting and Detection



## tensai Sec Ops Framework

- Governance Framework based on Industry best practices and our experience
- Realigning the team structure to meet Security Posture Objectives instead of delivering security activities
- Data Driven Insights



## Automation Driven Operations

- Rapid Incident Response and Remediation
- Continuous Compliance and Policy Enforcement (Compliance As A Code)
- Automated Threat Detection and Hunting



## Focus on Digital Identity Assurance

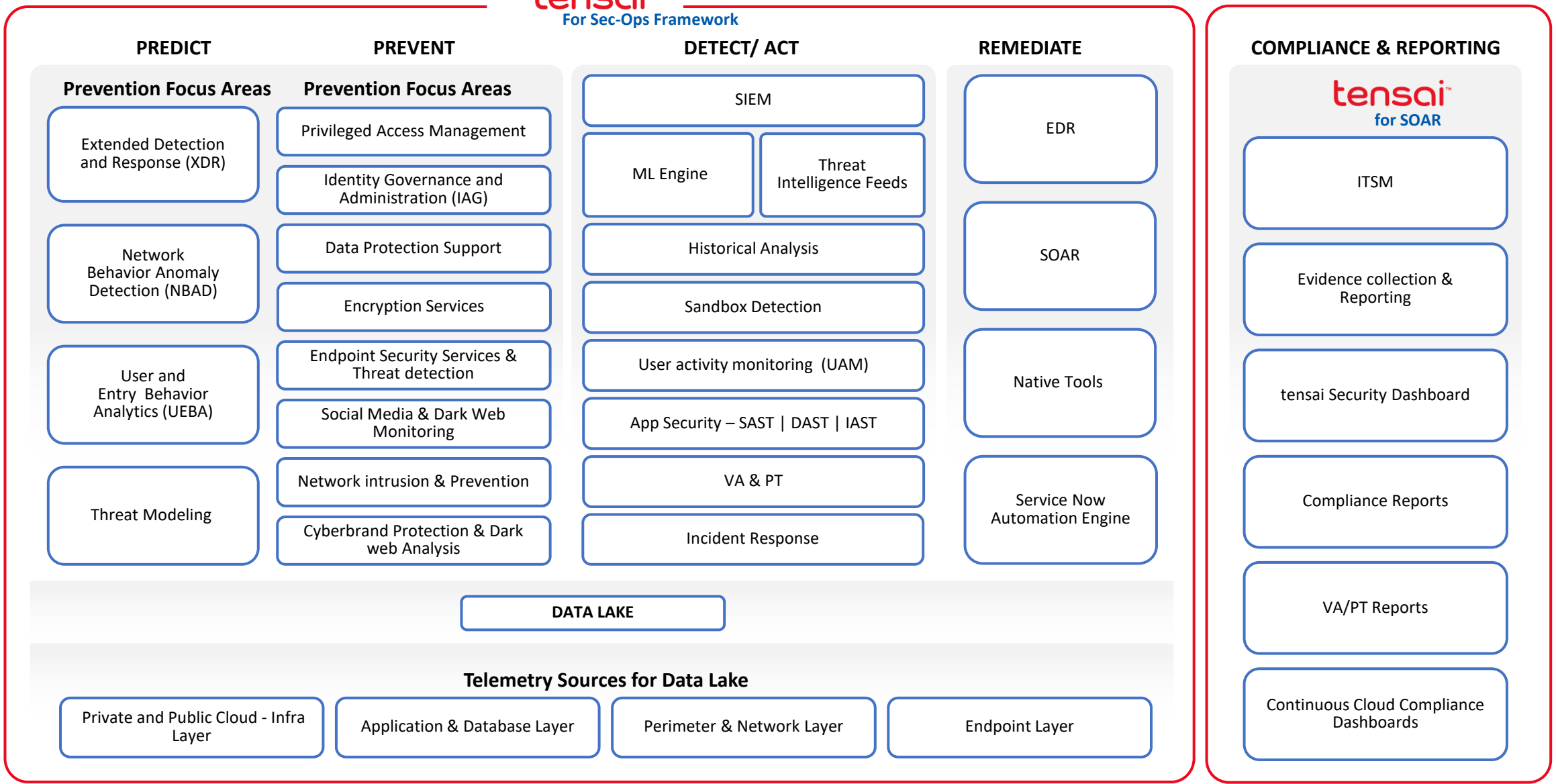
- Identity Governance and Compliance
- Prevention of Identity-Related Threats
- Enhanced Identity Verification
- Adaptive Risk-Based Authentication
- Zero Trust Architecture
- Identity Fabric Immunity



## 360 Application Security

- Build Pipelines with DevSecOps Integration
- utilize Interactive Application Security Testing / Runtime Application Self-Protection
- Implement Secure Coding Practices
- Cloud-Native Application Security

# Tensai Sec Ops Framework




# Predict Function




Leverage cutting edge AI & ML based tools & enhanced processes, ensure to bring in predictive actionable insights to enhance customer's security posture and safeguard critical assets.

Data Lake & Predictive Analytics      User Behavioral Analytics      Network Behavioral Analytics      Threat Modelling


 **Predictive Analytics**


- Predictive analytics leverages historical data to identify patterns, trends, and correlations that can be used to make predictions about future events or outcomes.
- A security data lake serving as a centralized repository for storing vast amounts of security-related data, including logs, events, alerts, network traffic, and other relevant information.
- Security analysts and data scientists' access and query the security data lake to gain insights and perform advanced analytics.
- Continuous improvement and innovation.

 **Other Predictive Functions**


- Threat analysis using a hybrid approach utilizing both checklist-based and non-checklist-based systems.
- XDR service leverages advanced analytics and machine learning algorithms to identify and prioritize both known and unknown (zero-day) threats.
- Using advanced artificial intelligence algorithms, our NBAD solution intelligently prioritizes the network's critical assets over other traffic.

## Predict







Data Lake Based Pattern Matching




Enhanced Visibility



Improved threat hunting capabilities



Spot suspicious user behaviour

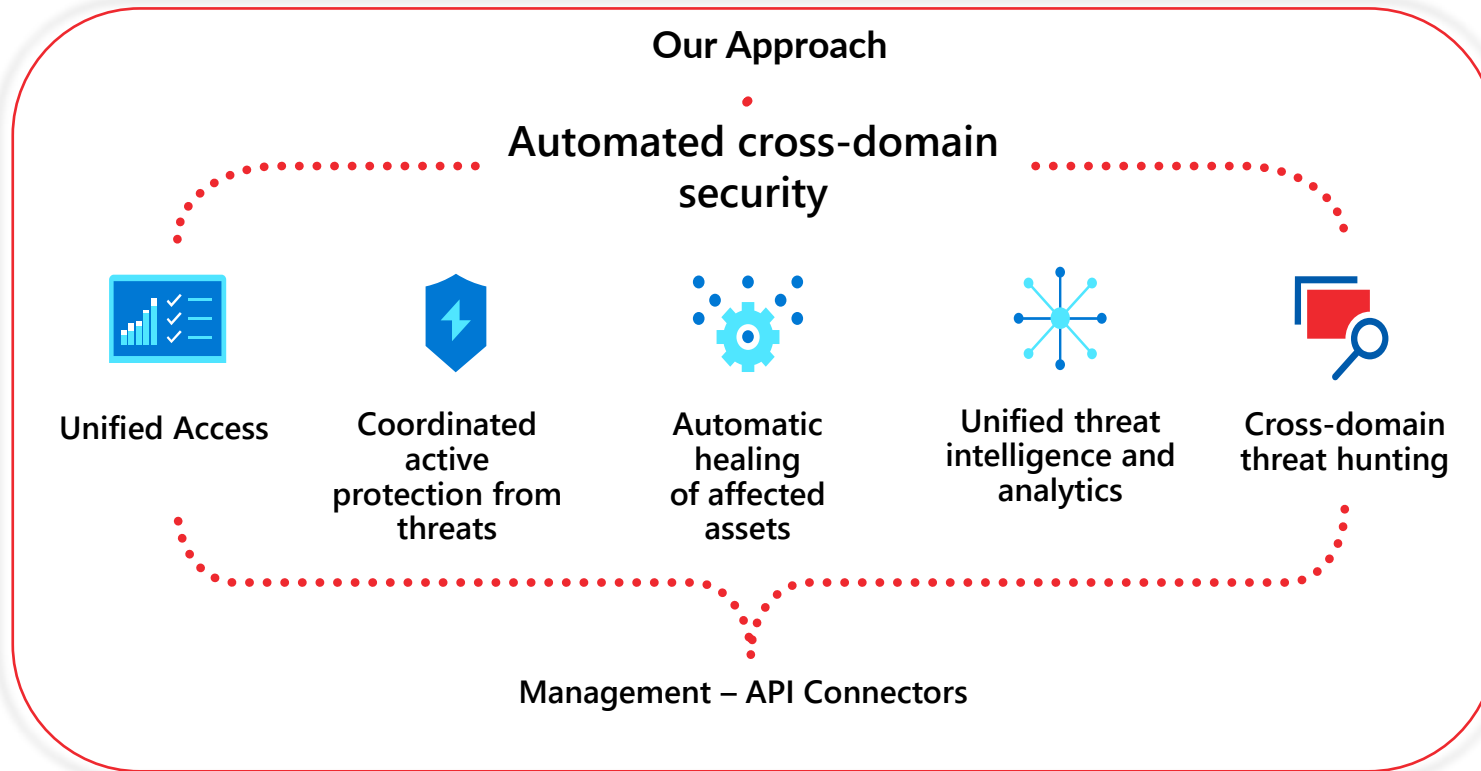


Predict security anomalies

# Predict – XDR

## Problem Statement

- Fragmented Security tool
- Lack of visibility.
- Alert Fatigue and false positives.
- Slow incident response.
- Complex Threat Detection and Response:
- Slow Incident Response:
- Compliance and Reporting Burden:



## Benefits:

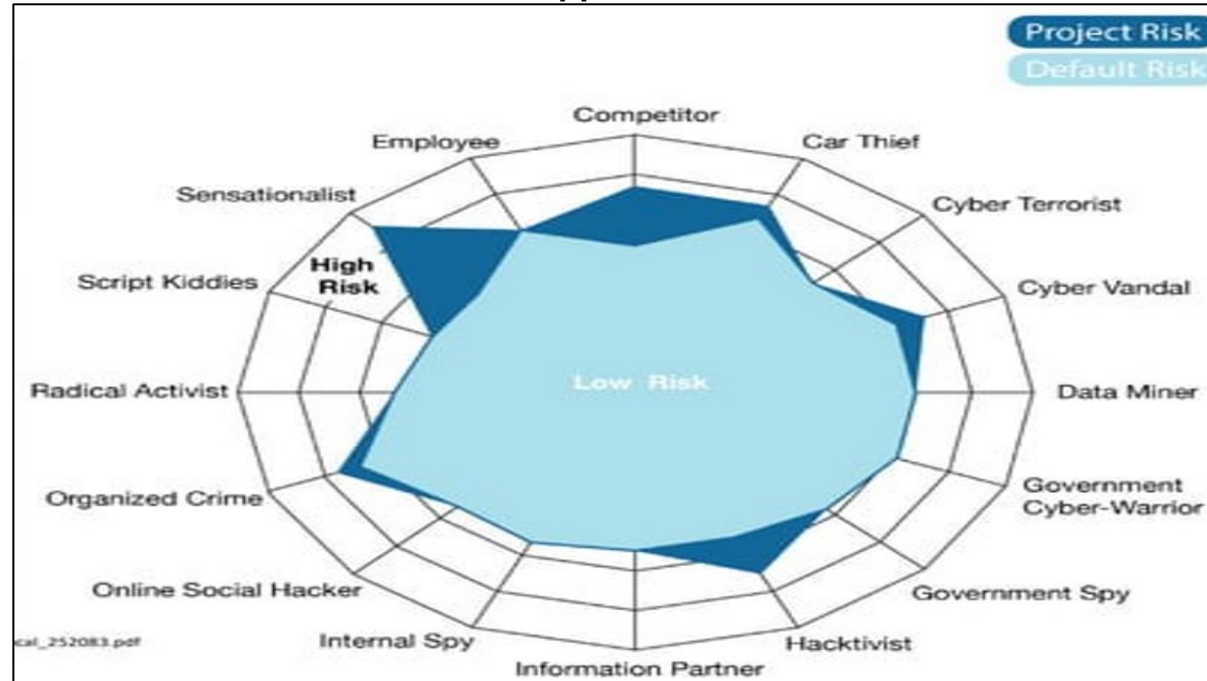
- XDR consolidates various security tools into a single platform,
- XDR offers holistic visibility across diverse data sources.
- XDR incorporates advanced threat detection capabilities.
- XDR provides automated and orchestrated incident response capabilities.
- XDR offers built-in compliance functionalities and reporting capabilities

# Predict - Threat Modelling

## Problem Statement

- Pain areas and benefit of user and entry behavioral analysis for customer in predictive security.
- Traditional security approaches often focus on known threats.
- Without a clear understanding of the threats they face, customers may allocate their security resources inefficiently.

## Our Approach



## Benefits:

- Threat modeling enables customers to proactively identify potential threats and vulnerabilities.
- Customers can develop and implement targeted security measures to mitigate identified risks.
- Prioritize their security investments based on the identified risks.
- Align the security practices with compliance and regulatory requirements.
- anticipate potential attack scenarios and plan their incident response strategies accordingly.
- anticipate potential attack scenarios and plan their incident response strategies accordingly.
- Promotes “a security-by-design” approach

# Prevent Function

**Delivery Strategy**

**Engagement Themes**



**Key Features**

**Functions**

**Enablers & Accelerators**

**Key Benefits & Commitments**

Prevent function encompasses advanced security solutions designed to proactively mitigate risks and prevent security breaches

IAM & PAM	DLP	Endpoint Security	Network Security
 <p><b>IAM, PAM &amp; DLP</b></p> <ul style="list-style-type: none"> <li>IAM service provides a centralized platform for efficient user identity and access management across systems and applications, ensuring consistent access controls and streamlined user provisioning processes.</li> <li>PAM solution allows temporary privilege elevation for regular user accounts, reducing the need for continuous elevated privileges and minimizing the potential attack surface.</li> <li>Help customers define policies and implement security measures to prevent accidental or intentional data leaks or exposure to unauthorized individuals.</li> </ul>		 <p><b>Endpoint &amp; Network Security</b></p> <ul style="list-style-type: none"> <li>Comprehensive visibility, detection, and remediation capabilities by integrating agent-based and agentless protection within a unified platform.</li> <li>Classify more data, revoke permissions, enforce policies, and trigger alerts for our IR team to review.</li> <li>DLP - continuously monitoring and analyzing data usage patterns to detect and respond to potential threats and policy violations.</li> </ul>	

**Prevent**



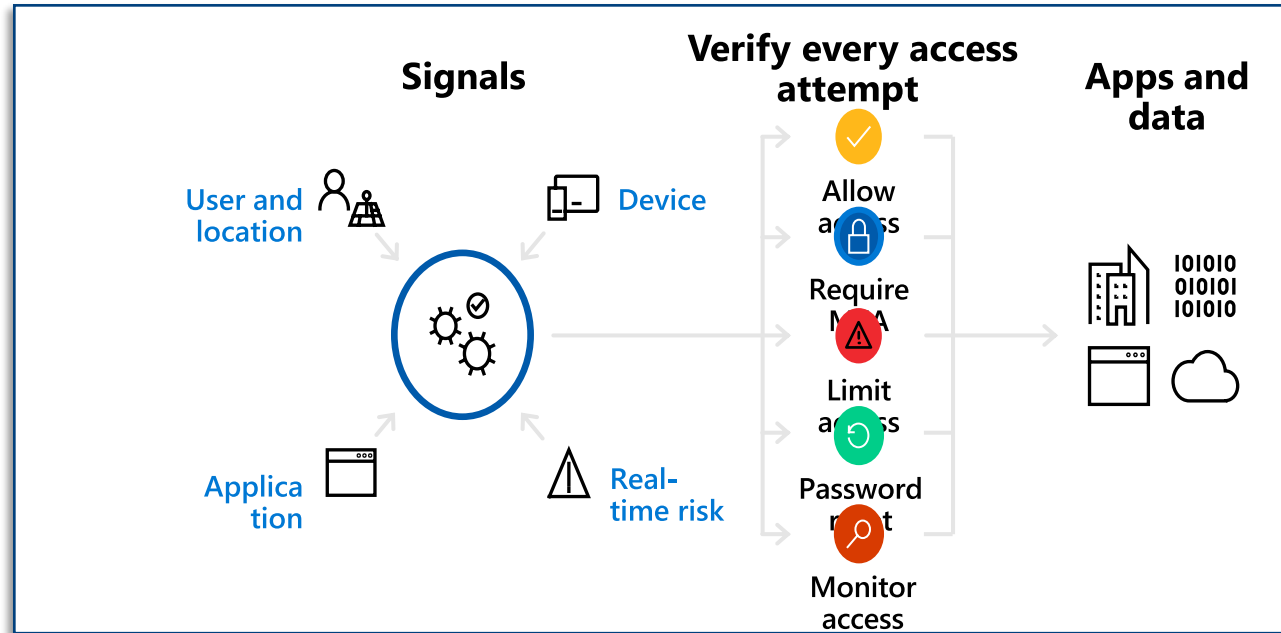
 <p><b>Risk Reduction</b></p>	 <p><b>Cost saving</b></p>	 <p><b>Protection of sensitive data</b></p>	 <p><b>Enhanced Reputation and customer Trust</b></p>	 <p><b>Regulatory compliance</b></p>
--	---	--	--	---

# Prevent – Focus Areas- IAM & PAM Services

## Problem Statement

- Challenges in gaining comprehensive visibility and control over user access to their systems and resources.
- Customers may be vulnerable to identity theft or credential abuse.
- Customers may struggle to meet regulatory compliance requirements and pass security audits

## Our Approach



## Benefits:

- Enhance the security posture and mitigate risks associated with unauthorized access.
- Centralized access management capabilities.
- Improves the user experience by simplifying and streamlining access to resources.
- IAM and PAM services help customers meet regulatory compliance requirements and pass security audits.
- Specialized controls and monitoring for privileged accounts.
- incorporate predictive analytics and machine learning capabilities

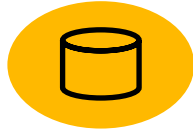


# Prevent - Data Protection

## Problem Statement



88% of organizations no longer have confidence to detect and prevent loss of sensitive data<sup>1</sup>

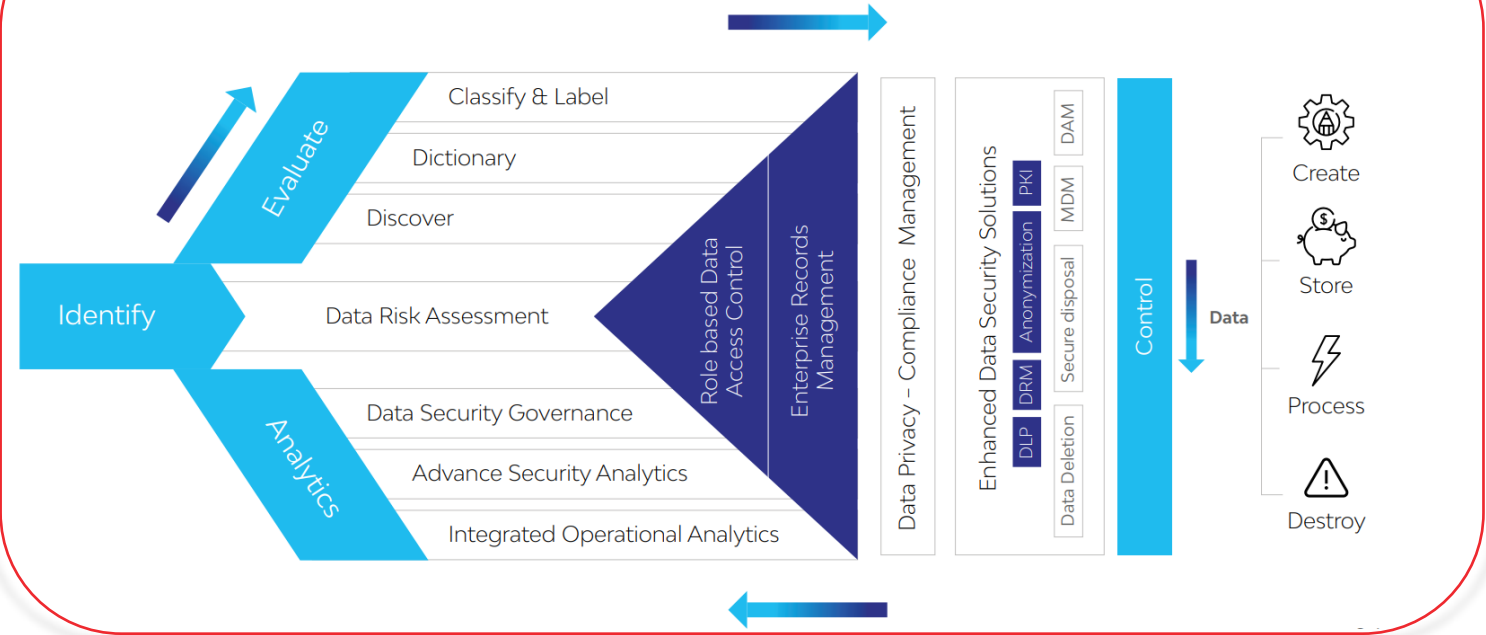


>80% of corporate data is "dark" – it's not classified, protected or governed<sup>2</sup>



83% of companies are experiencing challenges in ensuring regulatory and industry compliance from ineffective data management<sup>3</sup>

## Our Approach



## Benefits:

Understand & govern data  
Manage visibility and governance of data assets across your environment

Safeguard data, wherever it lives  
Protect sensitive data across clouds, apps, and devices

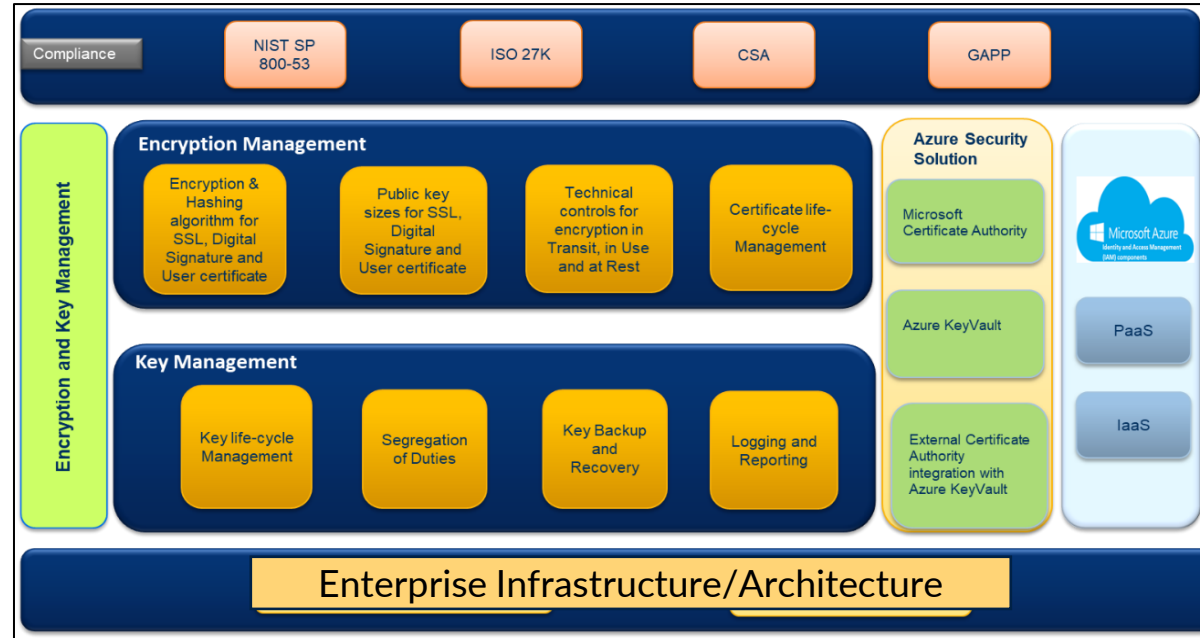
Improve risk and compliance posture  
Identify data risks and manage regulatory compliance requirements

# Prevent - Encryption

## Problem Statement

- Risk of data breaches and unauthorized access to their sensitive information.
- Many industries have strict compliance and regulatory requirements regarding the protection of sensitive data.
- Customers may face challenges in preventing data loss, especially when data is transmitted or stored in unsecured environments.

## Our Approach



## Benefits:

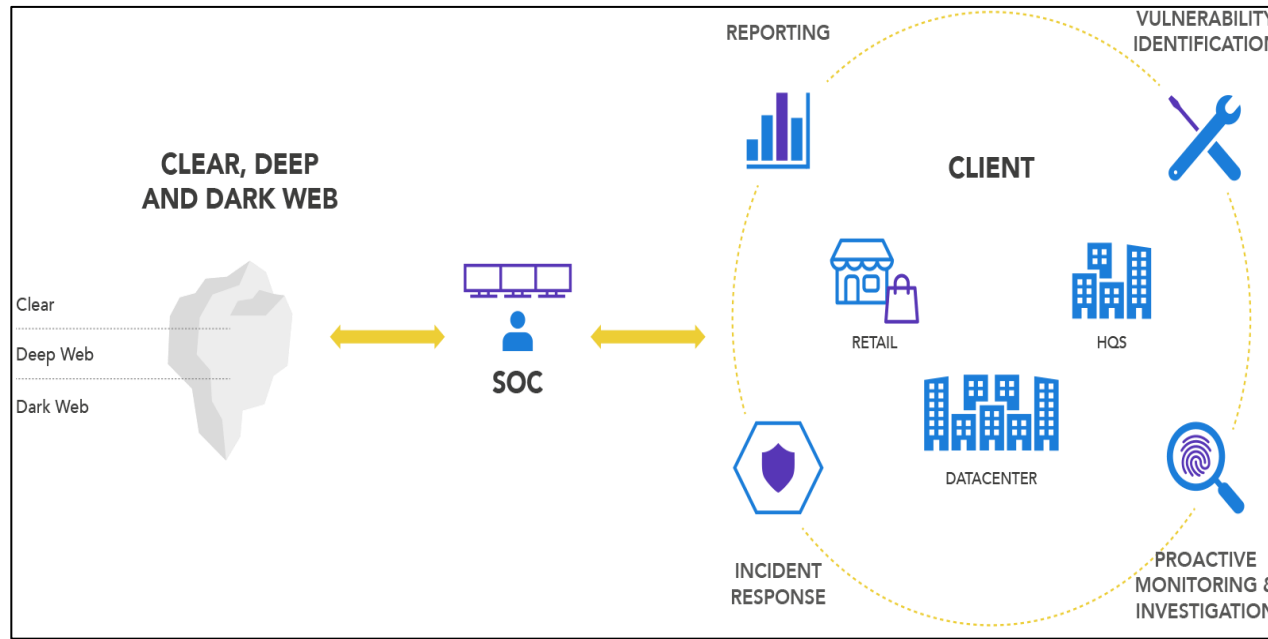
- Confidentiality of sensitive data by transforming it into an unreadable format.
- Securely transmit data over networks or through communication channels.
- Meet compliance and regulatory requirements related to data protection.
- Build trust and maintaining customer confidence.
- Assist customers in maintaining data sovereignty and privacy.
- Mitigate the risk of data tampering or modification during transit or storage.

# Prevent – Dark web Monitoring

## Problem Statement

- Customers may have limited awareness of whether their sensitive information is circulating on the dark web.
- Customers may be at risk of identity theft and fraud if their personal or financial information is exposed on the dark web.
- Without Dark Web Monitoring, customers may have a delayed incident response time.


## Our Approach



## Benefits:

- Enables customers to detect data breaches and compromised information at an early stage.
- Proactively respond to potential threats.
- Customers can detect instances of their stolen data being misused for fraud or identity theft.
- Demonstrates a commitment to protecting customer data.
- supports customers in meeting compliance and regulatory requirements.
- Provide customers with a competitive advantage

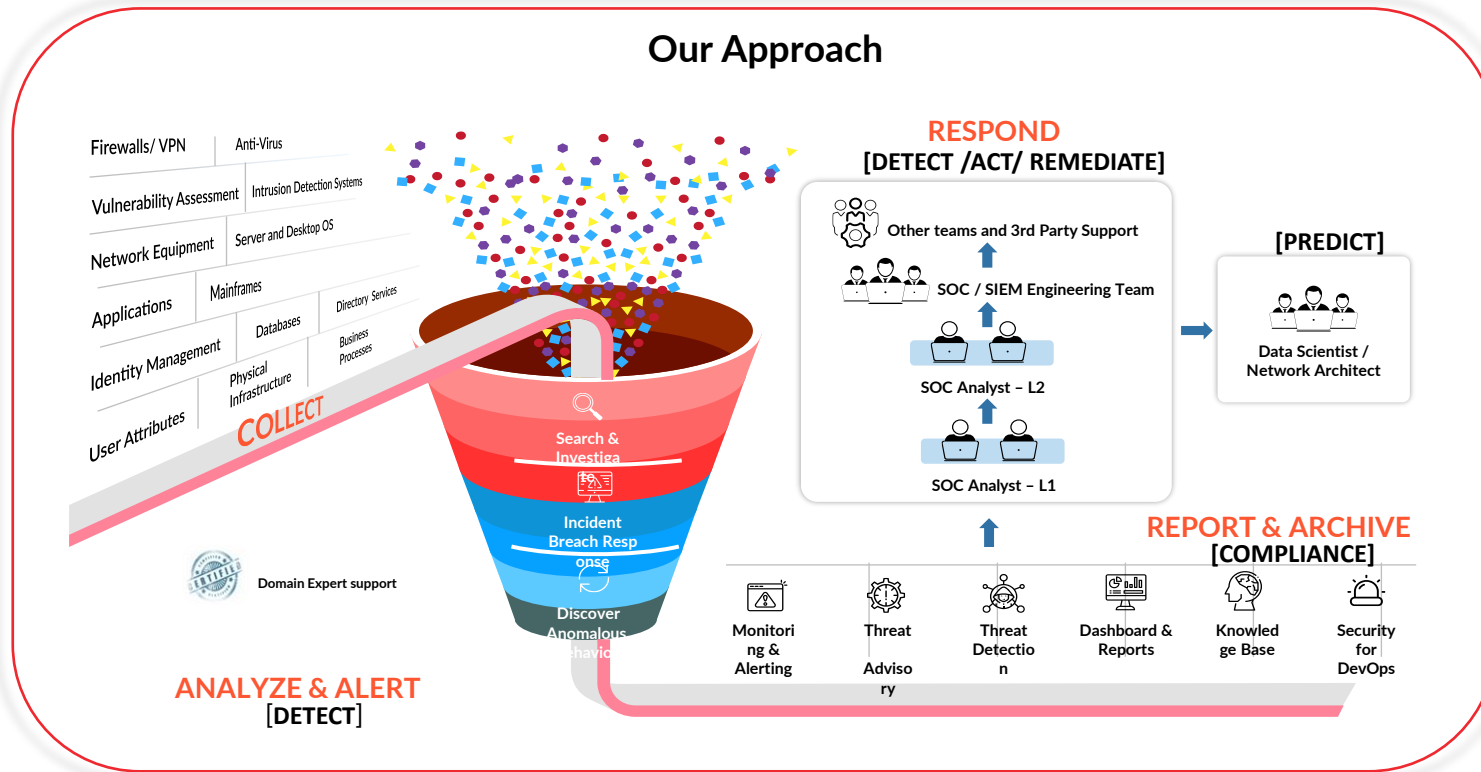
# Detect Function

<p><b>Delivery Strategy</b></p>	<p>Effectively monitor, detect, analyze, and respond to security incidents in real time, Incorporate threat feeds, industry reports, and intelligence sharing communities into your monitoring and analysis processes.</p>		
<p><b>Engagement Themes</b></p>	<p><b>SIEM / SOC</b></p> <p><b>SIEM / SOC</b></p> <ul style="list-style-type: none"> <li>Implement 24/7/365 monitoring capabilities to detect security incidents in real-time.</li> <li>Monitor network traffic, system logs, endpoints, and cloud environments for suspicious activities, anomalies, and indicators of compromise.</li> <li>Establish an incident response process that includes triage, containment, eradication, and recovery steps</li> </ul>	<p><b>Security Assurance</b></p> <p><b>Security Assurance</b></p> <ul style="list-style-type: none"> <li>Prioritized vulnerability assessments and remediation</li> <li>Exhaustive penetration tests for gap assessment</li> <li>Conduct regular vulnerability scanning on critical assets, including IP and web applications.</li> </ul>	<p><b>Application Security</b></p> <p><b>Application Security</b></p> <ul style="list-style-type: none"> <li>Collaborate with customers to incorporate security into the software development lifecycle.</li> <li>Perform the code scan to identify potential vulnerabilities, coding errors, and security flaws via SAST &amp; DAST.</li> <li>Conduct code reviews and follow-up scans to ensure that the vulnerabilities have been adequately resolved.</li> </ul>
<p><b>Key Features</b></p>	<p><b>Detect</b></p>		
<p><b>Functions</b></p>			
<p><b>Enablers &amp; Accelerators</b></p>	<p><b>Key Benefits &amp; Commitments</b></p> <ul style="list-style-type: none"> <li>Rapid incident response</li> <li>Threat intelligence integration:</li> <li>Reduced risk of exploitation</li> <li>Enhanced visibility into security posture</li> <li>Streamlined patch management</li> </ul>		

# Detect - SIEM

## Problem Statement

- Implementing and managing a SIEM solution can be challenging for customers.
- SIEM monitoring can generate a significant volume of logs and alerts from various systems.
- Customers may face alert fatigue due to the sheer number of alerts generated by the SIEM system



## Benefits:

- Centralize the collection and analysis of security logs from multiple sources.
- Enable real-time detection of security incidents by analyzing log data.
- Employ correlation and contextual analysis techniques Facilitates incident investigation and forensic analysis.
- Assist customers in meeting compliance and regulatory requirements.
- SIEM monitoring allows for continuous monitoring of security events and the integration of threat intelligence feeds

## Partnerships

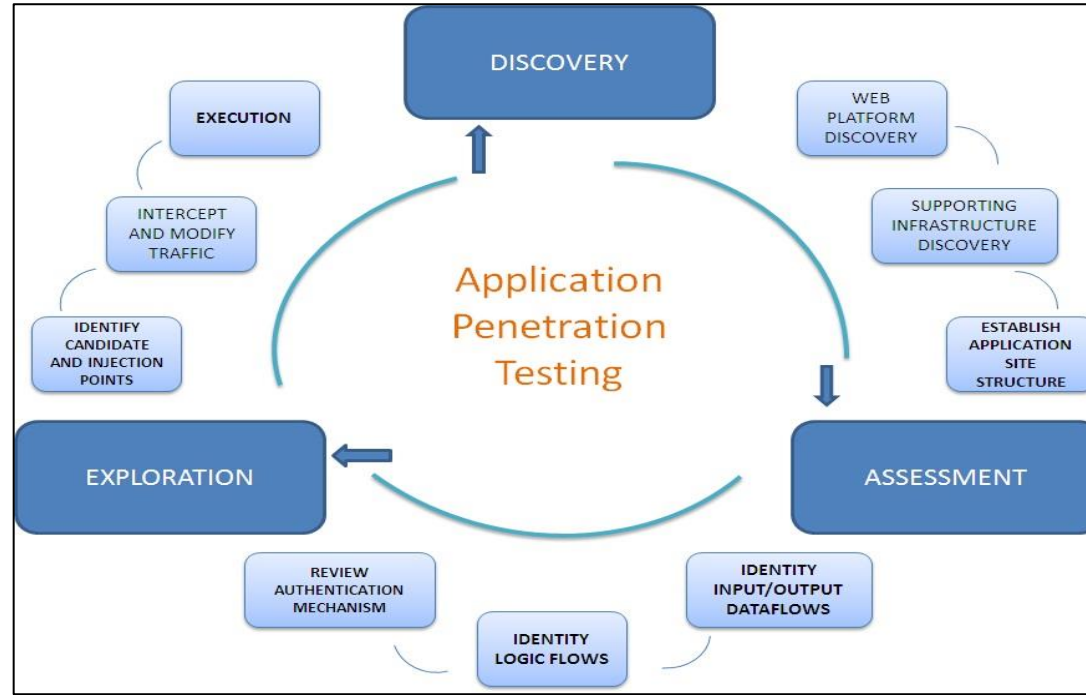


# Detect - SAST/DAST

## Problem Statement

- SAST and DAST tools can sometimes produce false positives..
- Utilizing SAST and DAST tools requires technical expertise and knowledge of secure coding practices and vulnerability detection.
- Integrating SAST and DAST tools into the development workflow can be complex and time-consuming

## Our Approach



## Partnerships



## Benefits:

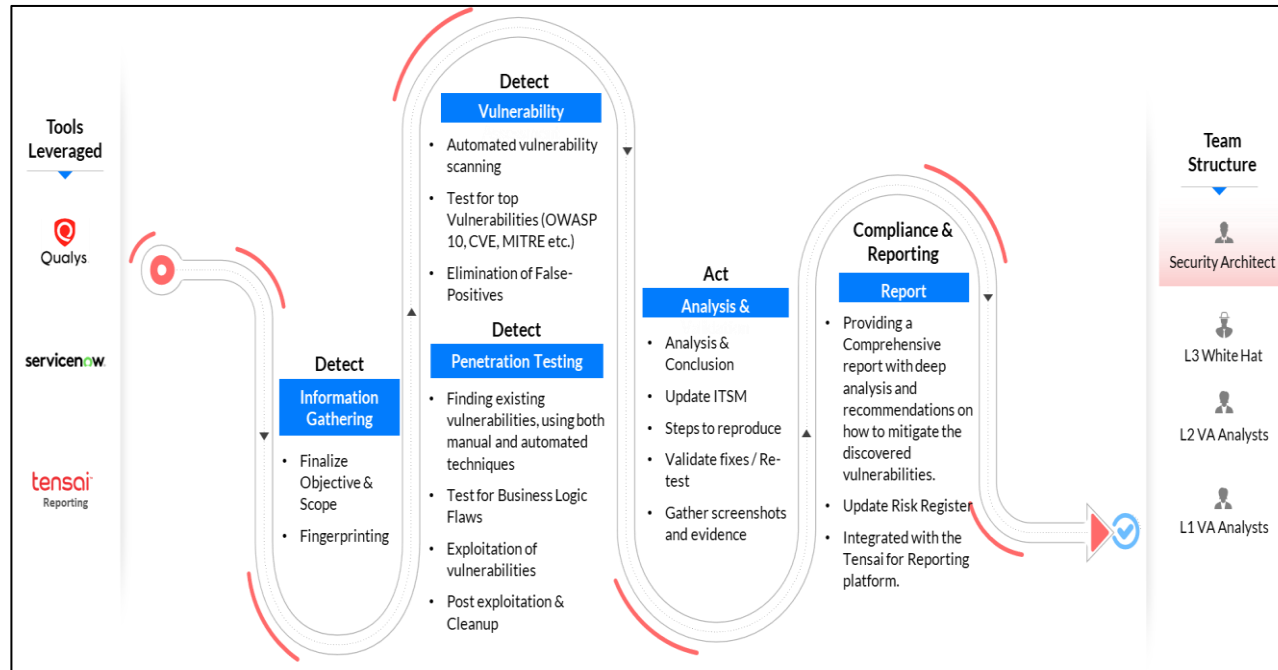
- Identify security vulnerabilities in their applications.
- Identify vulnerabilities early in the development lifecycle.
- Contribute to improving the overall security posture of applications.
- support customers in meeting compliance and regulatory requirements related to application security.
- Detecting and addressing vulnerabilities early in the development process can lead to cost savings.
- provide valuable insights for continuous improvement of the development process.

# Detect - Security Assurance - VA & PT

## Problem Statement

- Conducting comprehensive vulnerability assessments and penetration tests can be resource-intensive for customers.
- Customers may fall into the trap of developing a false sense of security.
- The scope of VA/PT testing may not encompass the entire IT infrastructure or all applications within an organization.

## Our Approach



## Benefits:

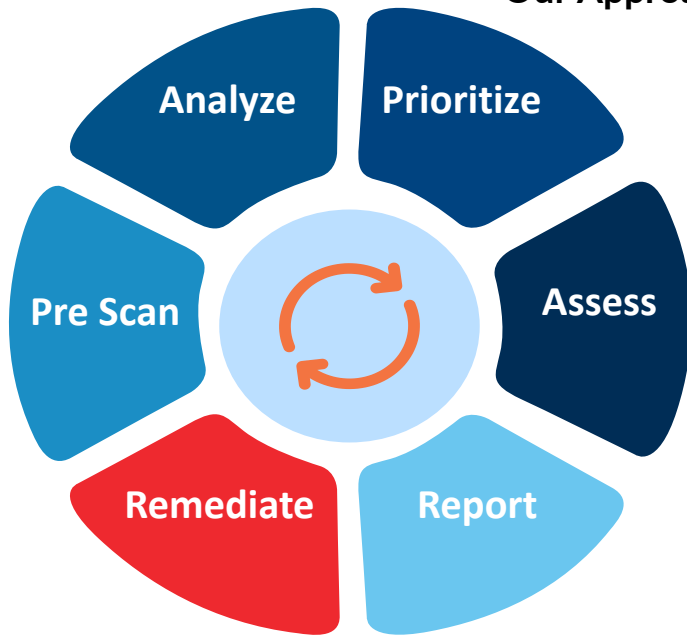
- Provides customers with a comprehensive assessment of vulnerabilities within their systems and applications.
- Simulating real-world attacks on systems and applications.
- Prioritizing security risks based on their severity and potential impact on the organization.
- Meeting compliance and regulatory requirements.
- Provides customers with actionable insights and remediation guidance
- Contributes to continuous.

# Detect- Vulnerability Management Approach

## Problem Statement

- Vulnerability management involves dealing with a large volume of vulnerabilities across various systems, applications, and network infrastructure.
- Applying patches and remediation measures to address vulnerabilities.
- Conducting regular vulnerability scans can generate network traffic and consume system resources

## Our Approach



Mutually agreed severity prioritization of vulnerabilities with IT and Business teams based on High risks

Use of Robust Vulnerability Management Tool

Remediation plan based on risk to business operations

Extreme Validation with Automation

Well Defined Vulnerability Metrics to be provided for periodic VAPT



## Benefits:

- Proactive detection of vulnerabilities.
- Prioritize vulnerabilities based on their severity and potential impact.
- A robust vulnerability management approach includes effective patch management processes.
- Implementing a vulnerability management approach helps customers meet compliance and regulatory requirements.
- Prevent potential security incidents and minimize the risk.
- Enables customers to continuously improve their security practices

## Partnerships

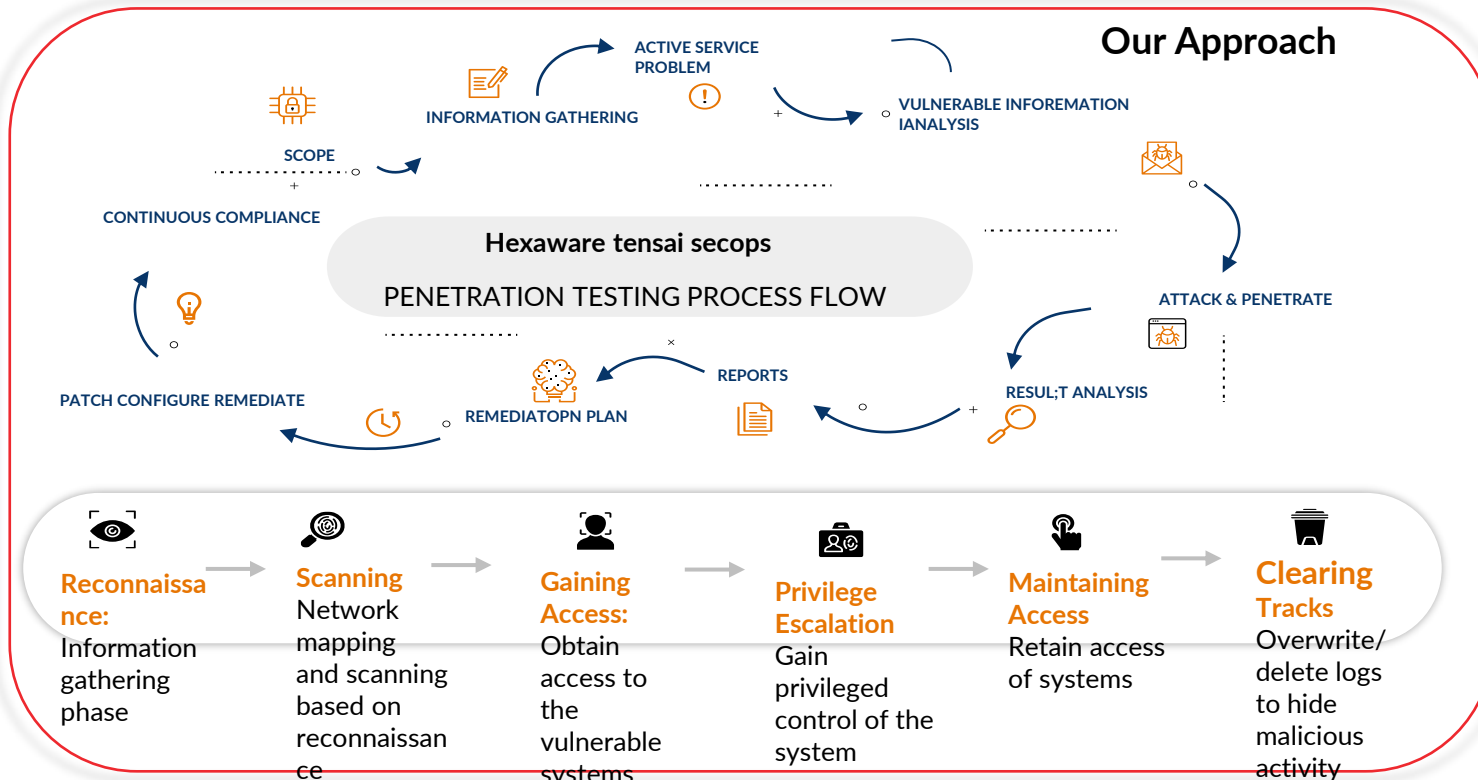




# Detect - Penetration Testing

## Problem Statement

- Vulnerability management involves dealing with a large volume of vulnerabilities across various systems, applications, and network infrastructure.
- Applying patches and remediation measures to address vulnerabilities can be complex and time-consuming.
- Conducting regular vulnerability scans can generate network traffic and consume system resources.



## Partnerships



## Benefits:

- Proactive detection of vulnerabilities.
- Prioritize vulnerabilities based on their severity and potential impact.
- A robust vulnerability management approach includes effective patch management processes.
- helps customers meet compliance and regulatory requirements.
- Proactively addressing vulnerabilities
- Enables customers to continuously improve their security practices.

# Remediate Function

## Delivery Strategy

Deliver the remediation function by prioritizing incidents, planning remediation, leveraging skilled expertise

## Engagement Themes

### EDR

### SOAR



### EDR

- Isolate compromised endpoints, terminate malicious processes, and remove malicious files or artifacts to contain and remediate security incidents promptly.
- Ability to revoke elevated privileges, reset compromised account credentials, and implement least privilege access controls to mitigate the risk of unauthorized access.
- Restore affected endpoints to a known good state or roll back changes made by malicious actors, minimizing the impact of the incident.



### SOAR

- Executing predefined remediation tasks such as isolating affected endpoints, blocking malicious IP addresses, disabling compromised user accounts, or quarantining infected files.
- Prioritizing and tailoring remediation actions based on the severity, impact, and relevance of the incident.
- Automate configuration changes to enforce security policies and best practices.
- Adapt and refine their remediation strategies based on evolving threat landscapes and changing business requirements.

## Key Features

## Functions

## Remediate

## Key Benefits & Commitments



Advanced  
Threat  
Detection



Real-time Incident  
Response



Compliance and  
Audit Support



Improved  
Operational  
Efficiency



Consistent and  
Standardized Response

# Remediate – Activity sets & benefits

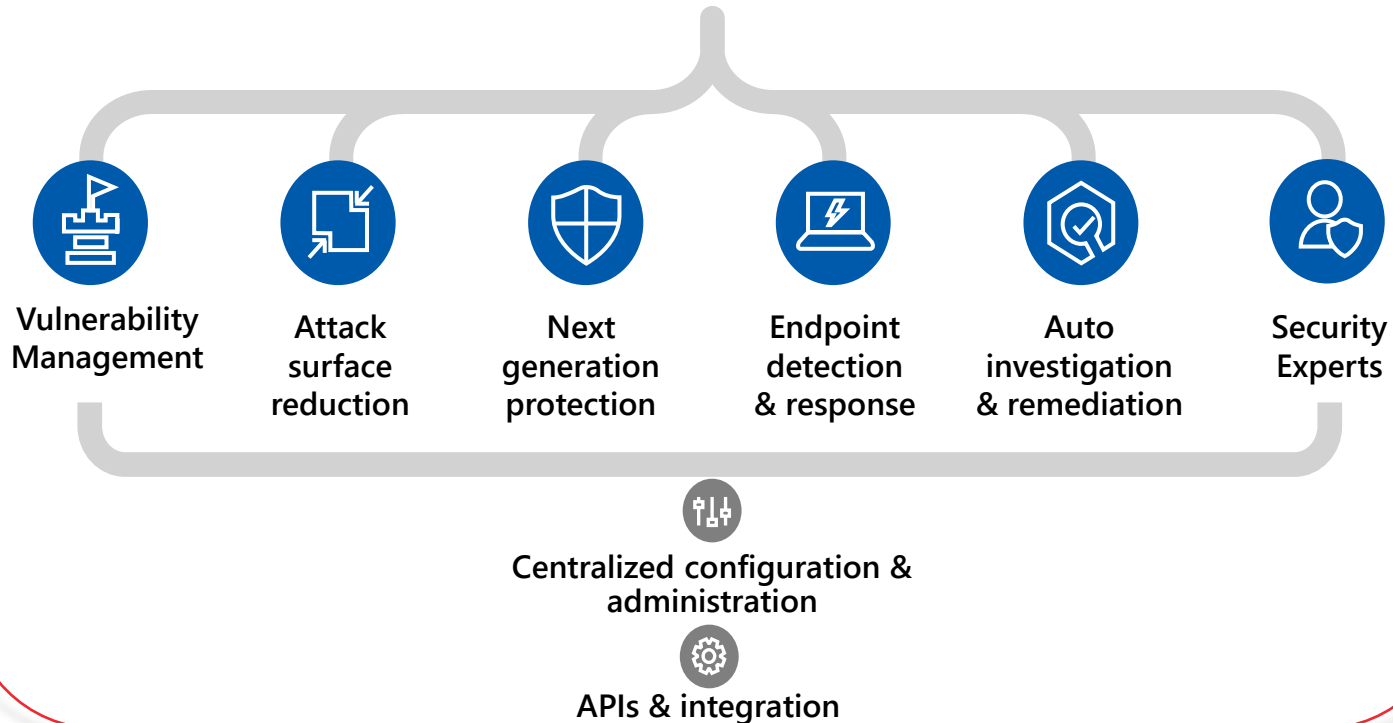
Activities	Benefits
<b>Remediation - End point detection &amp; Response</b>	
<ul style="list-style-type: none"> <li>Proactively searching for signs of advanced threats.</li> <li>Utilizing behavioral analysis and ML algorithms to detect and alert on behavior or malicious activities.</li> <li>Maintaining an up-to-date inventory of all endpoints.</li> </ul>	<ul style="list-style-type: none"> <li>Enables organizations to detect and respond to security threats on endpoints in real-time.</li> <li>Provides with the visibility and capabilities to respond swiftly and effectively to security incidents.</li> <li>Enhance endpoint security by continuously monitoring, analyzing, and detecting suspicious activities and potential threats.</li> </ul>
<b>Remediation -Security Orchestration &amp; Automated Response</b>	
<ul style="list-style-type: none"> <li>Automatically triaging and prioritizing security incidents.</li> <li>Aggregating alerts from various security tools and enriching them with contextual information.</li> <li>Designing and implementing automated workflows and playbooks that define step-by-step response actions for different types of security incidents</li> </ul>	<ul style="list-style-type: none"> <li>Reduces manual intervention and accelerating incident response.</li> <li>Enables security teams to handle a larger volume of incidents.</li> <li>Reducing human errors and ensuring a standardized approach to incident response.</li> </ul>

# Remediate – EDR

## Problem Statement

- Lack of Endpoint Visibility
- Slow Incident Response
- Resource Constraints
- Advanced Threat Protection
- Compliance Requirements

## Our Approach



## Partnerships



## Benefits:

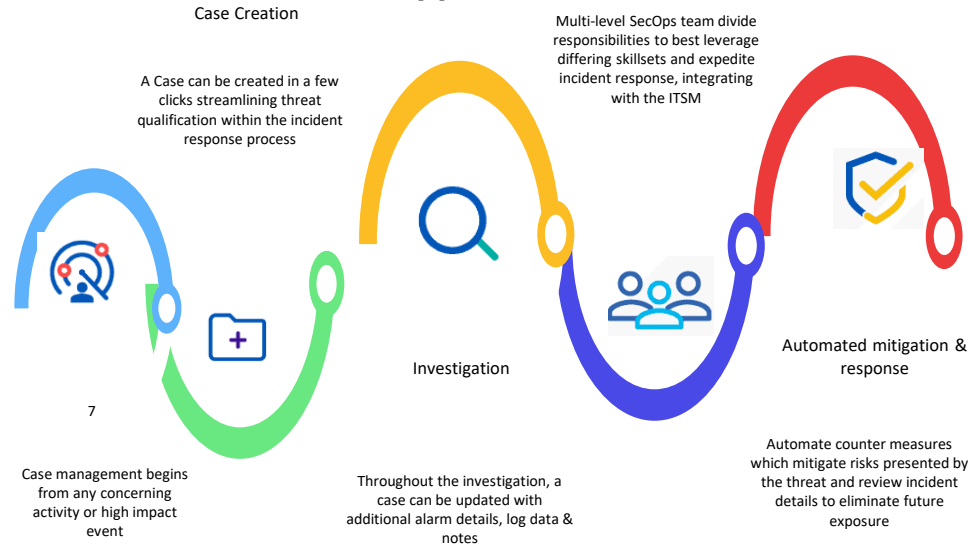
- Proactive detection.
- Customers prioritize vulnerabilities based on their severity and potential impact.
- includes effective patch management processes.
- Implementing a vulnerability management approach helps customers meet compliance and regulatory requirements.
- Prevent potential security incidents and minimize the risk of breaches or unauthorized access to their systems. A vulnerability management approach enables customers to continuously improve their security practices.

# Remediate – SOAR – Automated Security Incident Handling

## Problem Statement

- Implementing a Security Orchestration, Automation, and Response (SOAR) solution can be complex and require integration with existing security tools, systems, and processes.
- Skills and knowledge to design and automate incident response workflows.

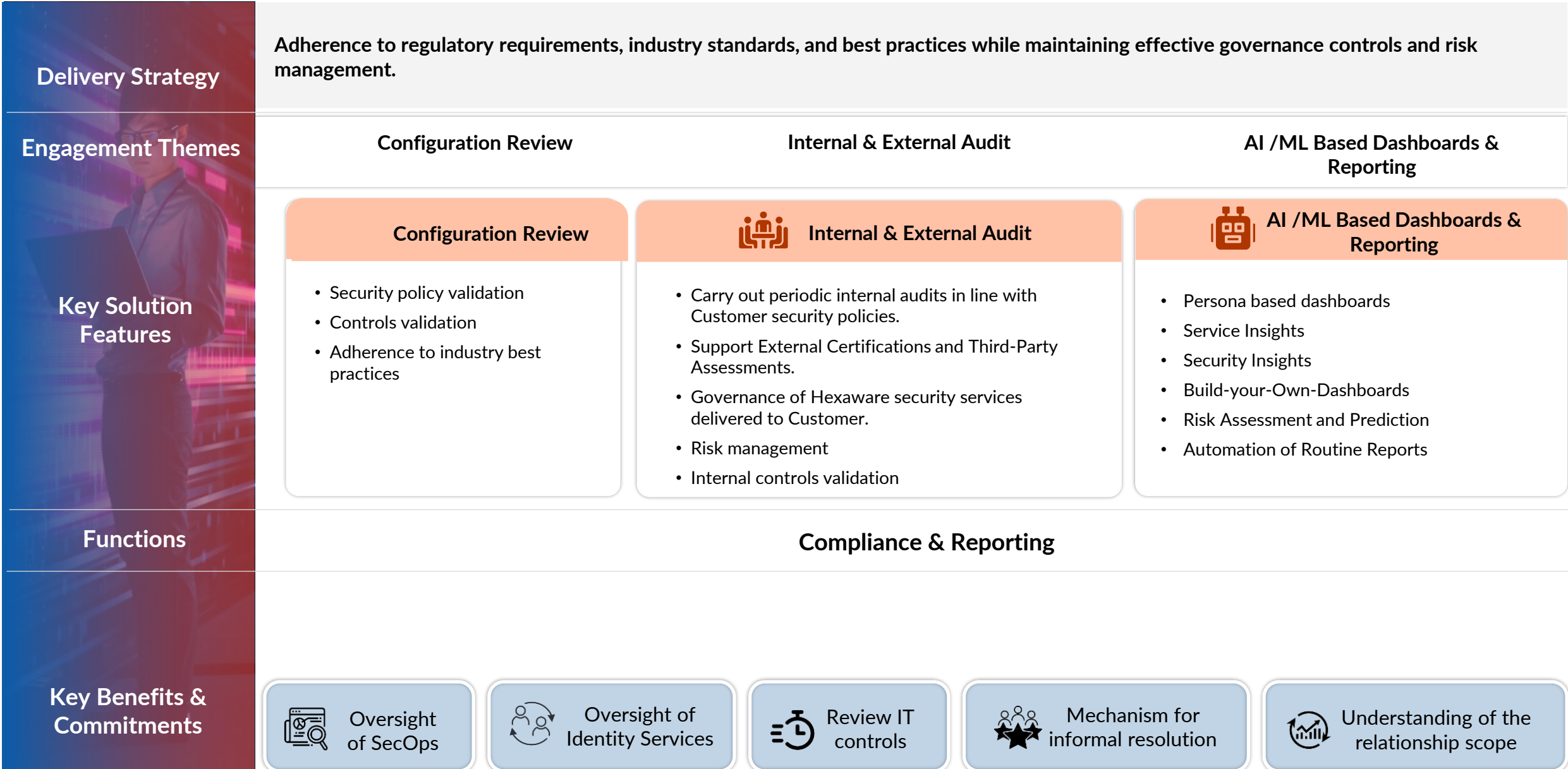
## Our Approach



## Benefits:

- Enables an integration layer, linking customers to connect and orchestrate various security tools and systems.
- Automate various aspects of security incident handling, such as alert triaging, enrichment, correlation, and response actions.
- Consistent and Standardized Workflows: SOAR platforms enable customers to define and automate standardized incident response workflows.

# Compliance & Reporting Function



# Compliance & Reporting – Activity sets & benefits

Activities	Benefits
<b>Compliance &amp; Reporting - Evidence collection &amp; Reporting</b>	
<ul style="list-style-type: none"> <li>Establishing a systematic process for documenting and maintaining the chain of custody of collected evidence</li> <li>Utilizing specialized tools and techniques to collect, preserve, and analyze digital evidence</li> <li>Identifying and collecting relevant data and evidence from various sources.</li> </ul>	<ul style="list-style-type: none"> <li>Proper evidence collection ensures that the collected evidence is admissible in legal proceedings.</li> <li>Thorough evidence collection helps investigators build a solid case by ensuring all relevant evidence is collected and preserved.</li> <li>Verify the facts of an incident or crime</li> </ul>
<b>Compliance &amp; Reporting - Security Assessments to frameworks and standards</b>	
<ul style="list-style-type: none"> <li>Identify relevant security frameworks and standards applicable to the organization's industry.</li> <li>Conduct a gap analysis to assess the organization's current security posture.</li> <li>Perform a comprehensive risk assessment.</li> </ul>	<ul style="list-style-type: none"> <li>Meet industry-specific compliance requirements and regulatory obligations.</li> <li>Enables organization to identify and address gaps.</li> <li>Ensures the implementation of industry-recognized best practices.</li> </ul>
<b>Compliance &amp; Reporting - Compliance Dashboarding</b>	
<ul style="list-style-type: none"> <li>Clarity in defining the objectives and scope.</li> <li>Collect data related to compliance activities.</li> <li>Determine the KPIs and metrics that will be tracked on the compliance dashboard</li> </ul>	<ul style="list-style-type: none"> <li>Provides a centralized and consolidated view of compliance metrics.</li> <li>Enable data-driven decision making by presenting compliance metrics and trends.</li> <li>Automate the generation of compliance reports.</li> </ul>
<b>Compliance &amp; Reporting - Continuous cloud compliance</b>	
<ul style="list-style-type: none"> <li>Identify and define the specific compliance requirements.</li> <li>Conduct an initial compliance assessment to evaluate the organization's current cloud environment</li> <li>Implement and configure appropriate security controls within the cloud environment.</li> </ul>	<ul style="list-style-type: none"> <li>Continuous cloud compliance provides real-time visibility</li> <li>Monitoring helps identify and mitigate compliance-related risks promptly</li> <li>Proactively manage compliance by addressing issues as they arise.</li> </ul>

# Our Consulting – GRC Services

## 02. Internal Audit

- Internal Controls Review
- Information Systems Audit
- Process Audit
- Security Audit
- Policy/Framework Audit

## 04. Security Testing

- Vulnerability Assessment
- Penetration Testing
- Security Usecases Review

## 06. Third Party Audits

- Conduct vendor Risk Assessment

## 08. BCP Consulting

- Define BCP and conduct Business Impact Analysis and Risk assessment. Assist in BCP testing and define SOPs for disaster scenarios

## 01. ISO Certification

Prepare, assist and recommend necessary tools and technologies. Help in preparation of metric dashboard

## 03. GDPR /Privacy Compliance

- GDPR Compliance Audit
- Assist with implementation of controls and processes
- DPO as a service
- Privacy Assessment

## 05. Risk Assessment

- Define Risk assessment framework, conduct audit for the same and make necessary remediation recommendations

## 07. IT Asset Audit

- License Audit
- Process Audit



## Advisory Services

- Data Privacy Officer on Demand
- CISO on Demand
- Compliance Officer on Demand

- Mentor Board
- Members and CEOs on Information Security, Digital Risk, Privacy etc.

- Implement and Manage ISMS

- Assist CIOs in their Operations for Compliance, Assessment, Documentation

## Training Services

- Information Security Awareness

- Secure Coding Guidelines.

- Security Testing

- ISMS Process and Audit Methodology

# Compliance & Reporting Services - Governance, Risk and Compliance Service offering

## Problem Statement

- Compliance with regulatory standards and industry-specific requirements can be complex and challenging for organizations.
- Achieving and maintaining compliance can require significant resources
- The regulatory landscape is constantly evolving, with new standards, laws, and regulations being introduced regularly.



i

## Benefits:

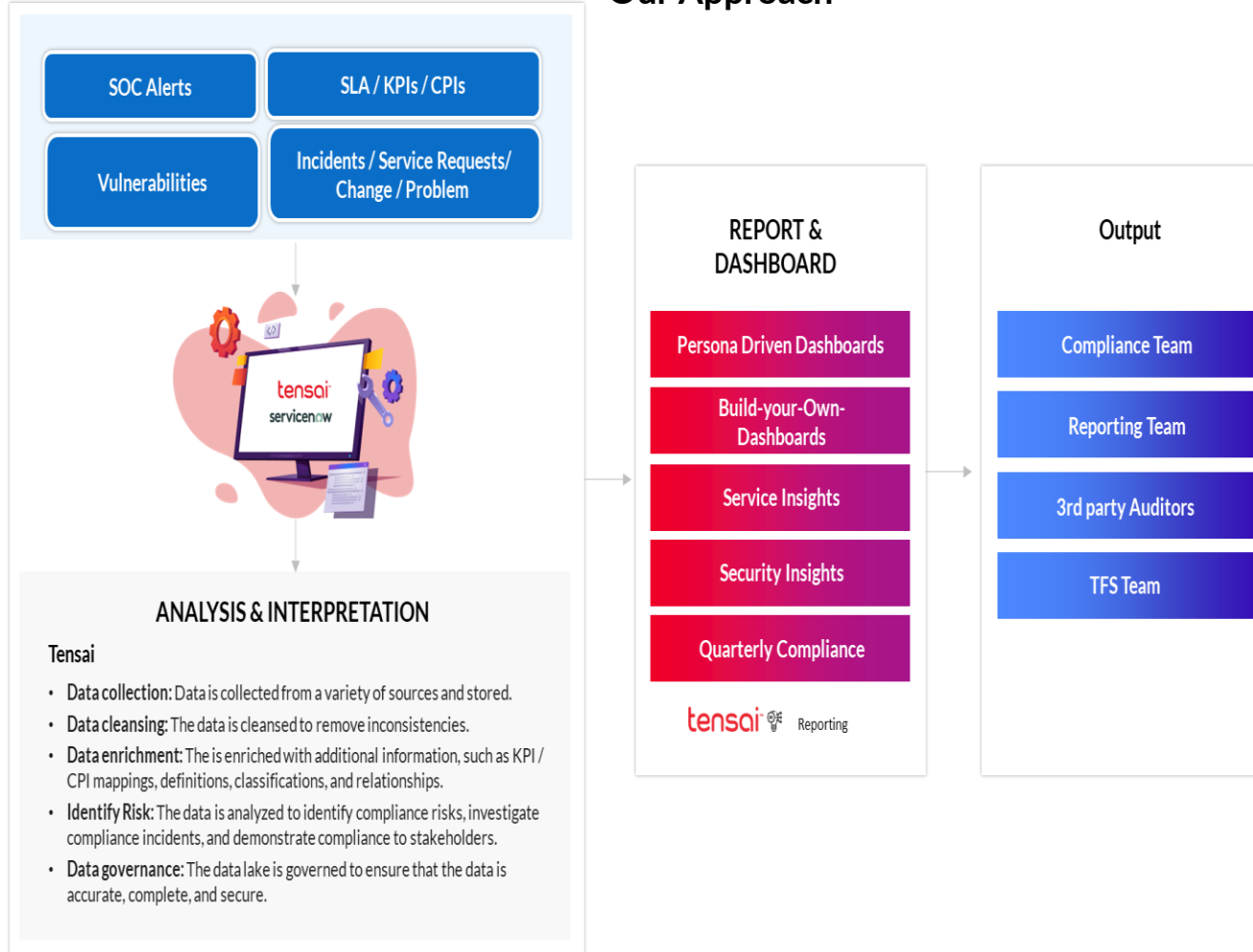
- Align operating strategy with streamlined business process
- Address multiple compliances
- Agile and scalable controlled environment.
- Cross-functional Risk approach
- Standardized GRC processes to enhance decision making
- Embrace governance automation more effectively
- Predictable and optimized results

# Compliance & Reporting Services

## Problem Statement

- Compliance with regulatory standards and industry-specific requirements can be complex and challenging for organizations.
- Achieving and maintaining compliance can require significant resources in terms of personnel, time, and financial investments. The regulatory landscape is constantly evolving, with new standards, laws, and regulations being introduced regularly

## Our Approach



## Benefits:

- Enable organizations to meet legal and regulatory
- Best practices and security frameworks to enhance overall security posture.
- Focus on data protection and privacy.
- Compliance demonstrates a commitment to security and data protection.
- Streamline the audit process by maintaining organized documentation,
- Encompass elements of business continuity planning and disaster recovery.