CRYPTOGEN NEPAL

CGN

20
25

MSSP Alert
A CyberRisk Alliance Production
TOP 250

ICT AWARD 2020
STARTUP CATEGORY

ISO 27001:2022
CERTIFIED

About Us

We are CryptoGen Nepal, also known as CGN, a Nepal-based cybersecurity firm working globally. We have been listed as **Top 80 globally** for CyberRisk Alliance's Top 250 Managed Security Service Providers (MSSPs) for the last two consecutive years. Founded in 2019 by like-minded security professionals with years of experience, we now have a team of around fifty cybersecurity experts across diverse domains.

CryptoGen Nepal

- Security Operations Center
- IS Audit & VAPT
- Dark Web Monitoring
- Vulnerability Management
- Security Awareness & Cyber Drill
- Incident Response
- Security Consultation
- ISO Readiness 27001, 27701, 27002 & 27033

Our cybersecurity engagements

United States

United Kingdom

Australia

United Arab Emirates

Bangladesh

Nepal

Team Composition

Offensive Security

- Vulnerability Assessment
- Penetration Testing
- Red Teaming

Security Operations

- Monitoring
- Incident Response
- Digital Forensics
- Professional Service

Compliance
Risk management
Governance

Risk & Compliance

- IS Audit
- SWIFT Audit
- ISO/IEC 27001

Research & Development

- Product Research
- Product Development

Business Development

- SME
- Corporate
- BFSI
- Government

Products & Professional Services

Tenable-Vulnerability Management

- NIC Asia
- Himalayan Bank
- MBL
- Nepal Bank
- Prabhu Bank

FortiSIEM

- Supreme Court (SIEM)
- NEA (SOC)
- Everest Bank (SOC)
- Himalayan Bank (SOC)

iZoologic

- Nepal Police

CTM360

- Everest Bank

SayCure

- Himalayan Bank
- Datahub (Excel Development)

LogPoint

- Kamana Sewa
- SCT (SOC)

DNS-LogRhythm

- Laxmi Sunrise
- NIMB
- NTC
- Nepal Police
- Siddhartha Bank

Valued Clients

Largest Telco

+10 Class 'A' Commercial Banks in Nepal

2 Largest Payment Service Providers

+12 Global Customers

International Customers

GrowByData

uxcam

Zelda Security

taabl

stickman CYBER

paramount Assuring Value REGIONAL LEADER IN CYBERSECURITY

Valued Clients

Security Audit

- नेपाल बैंक लिमिटेड NEPAL BANK LIMITED
- Ncell
- NABIL BANK
- Agricultural Development Bank Limited कृषि विकास बैंक लिमिटेड तपाईं हाम्रो घरआंगनको बैंक
- NEPAL LIFE सुरक्षा र समृद्धि
- Siddhartha Bank

VAPT

- GrowByData
- fonepay
- uxcam
- IME group pioneering spirit
- khalti
- NMB
- कुमारी बैंक लिमिटेड KUMARI BANK LIMITED
- ZINOB INC. PVT. LTD.
- eSewa
- KHWOPA COLLEGE OF ENGINEERING BHAKTAPUR, 2008
- Zelda Security

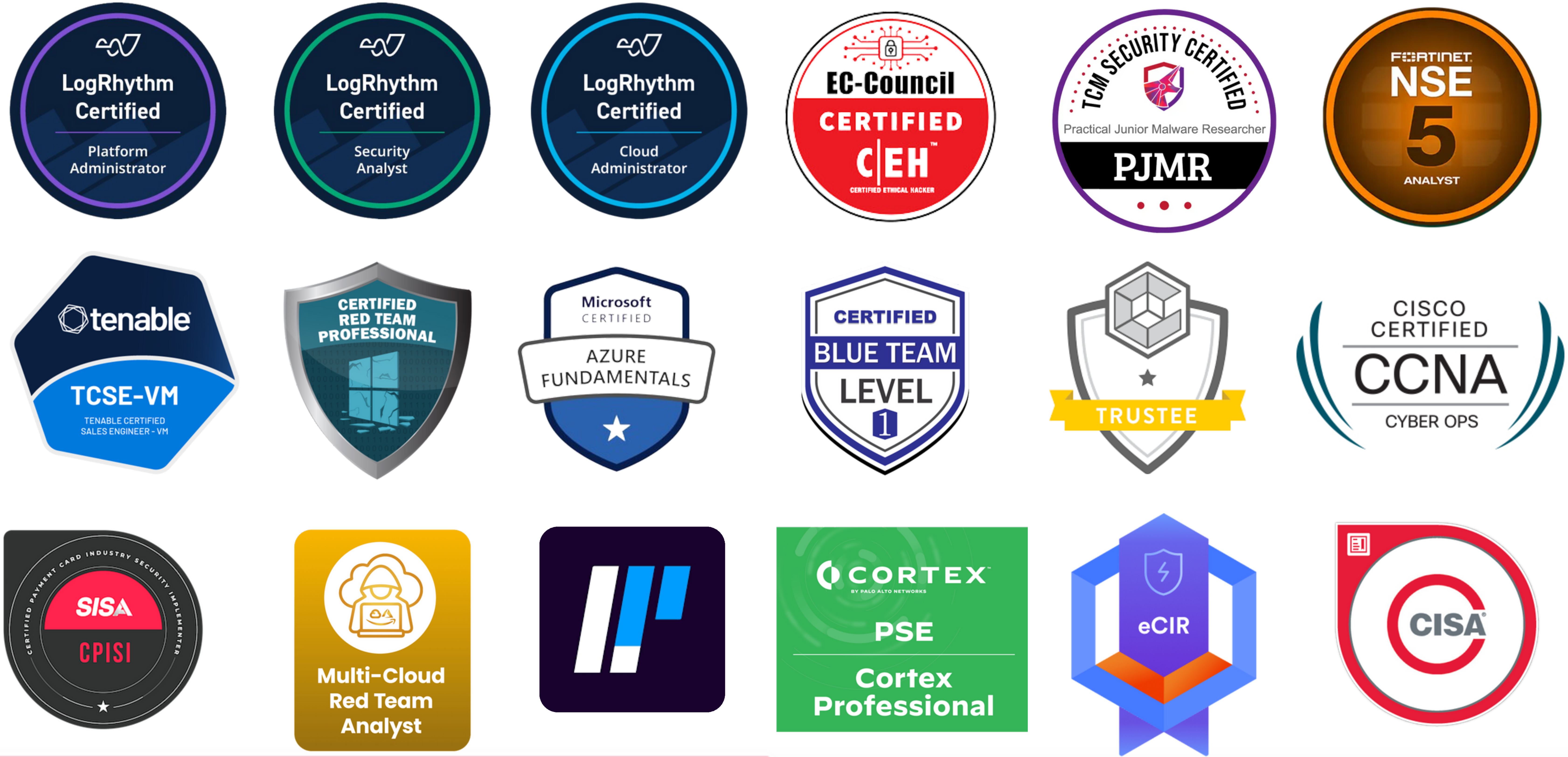
SIEM & SOC

- नेपाल प्रहरी सत्य सेवा सुरक्षणम्
- NIMB नेपाल इन्भेष्टमेन्ट मेगा बैंक लि. NEPAL INVESTMENT MEGA BANK LTD.
- Nepal Telecom
- Laxmi Sunrise
- नेपाल विद्युत प्राधिकरण स्थापित २०४२ ESTD. 1985 NEPAL ELECTRICITY AUTHORITY
- taabl
- कामना सेवा विकास बैंक लि. Kamana Sewa Bikas Bank Ltd.
- HBL Himalayan Bank Limited

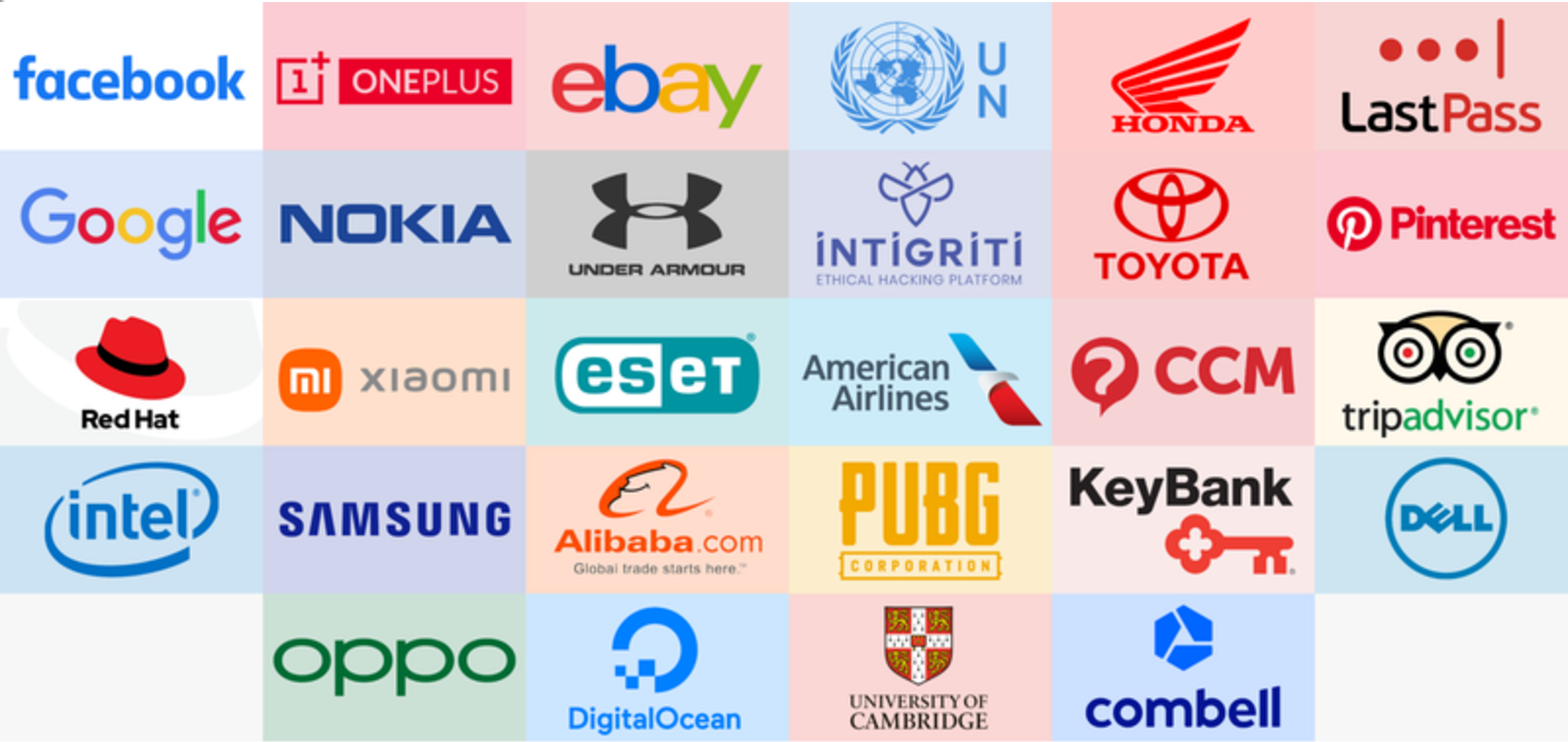
Professional Services

- नेपाल प्रहरी सत्य सेवा सुरक्षणम्
- NIC ASIA
- paramount REGIONAL LEADER IN CYBERSECURITY
- stickman CYBER
- त्रिभुवन विश्वविद्यालय TRIBHUVAN UNIVERSITY KATHMANDU, NEPAL
- Digital Network Solution

Team Strength



Team Recognition



Information System Audit (IS Audit)

An information Systems audit is the process of testing controls and reviewing against dictated organizations' policies. Audits are meant to provide confidence to stakeholders while making keen observation and conformity to regulations. At CryptoGen Nepal, we aim to provide highly professional audit services creating values to our professional and demanding clients.

Security Awareness Program

Effective security awareness program turns the end users and participants into a strong last line of defense against cyber-attacks. We have a growing library of interactive cybersecurity training modules, videos, and articles that are constantly updated. From phishing attacks to insider threats, our customizable cybersecurity education curriculum covers a wide spectrum of security hazards. We offer these customized training programs to the corporate level participants.

Security Assessment and Hardening

A corporate business solution is made up of numerous interconnected digital infrastructures, such as operating systems, virtual machines, web servers, databases, and so on. It's important to review the underlying infrastructures for security weaknesses in order to reduce the attack surface. As a result, Cryptogen Nepal steps in to offer Operating System hardening, Server hardening, and Database hardening services.

Security Operations Center (SOC)

Many assets are safeguarded by security operations center (SOC) teams, including intellectual property, personnel data, business systems, and brand integrity. SOC team act as the key point of collaboration in coordinated efforts to monitor, assess, and defend against cyberattacks as part of an organization's comprehensive cybersecurity framework.

Vulnerability Assessment & Penetration Testing (VAPT)

Vulnerability assessment is a method of identifying a system's defects, issues, and vulnerabilities in a methodical manner. It is a thorough examination of the system with the goal of identifying and exploiting possible flaws. Penetration testing is a detailed examination of found vulnerabilities that is then escalated to have the most impact on the system; we refer to this as VAPT (Vulnerability Assessment & Penetration Testing).

Vulnerability Management

Vulnerability management is the process of finding, analyzing, prioritizing, and remediating vulnerabilities that are identified on a regular basis. Risk based vulnerability management helps find criticality rating of all the assets presented so that patch team can focus on fixing the vulnerabilities that matter most. Based on your needs and requirements, CryptoGen Nepal can assist your organization in selecting, deploying, and training the industry's top vulnerability management solutions.

Cyber Security Consultant

As a consultant we posses various expertise knowledge and experiences ranging from the operation, risk, compliance including Vulnerability Assessment and Penetration testing, Firewall Management, Encryption Technologies, Threat Intelligence. No matter how complex your business questions, we have the capabilities and experience to deliver the answers.

SWIFT CSP Assessment

Society for Worldwide Interbank Financial Telecommunications (SWIFT) under Customer Security Program (CSP) aims at detection and prevention of fraudulent activity by means of a set of mandatory security controls and community wide information sharing initiative. Annual assessment of local environment against the mandatory and advisory controls as laid down as per SWIFT Customer Security Controls Framework (CSCF) need to be done. CryptoGen Nepal is a listed CSP Assessor for such independent external assessments under this SWIFT CSCF.

ISO 27001 Assurances

We can support you throughout your ISO 27001 readiness and certification phases. We review all the available policies, procedures, forms and formats and map them with the documentations required for an organization to comply with the international standard. We follow ISACA guidelines along with some of the best known industry practices, regulatory requirements of the land, IT frameworks, Guidelines & Standards like COBIT 5, ISO 27001, NIST Framework, NRB IT guidelines, NTA Cyber Bylaws, ITIL, PCI DSS, etc.

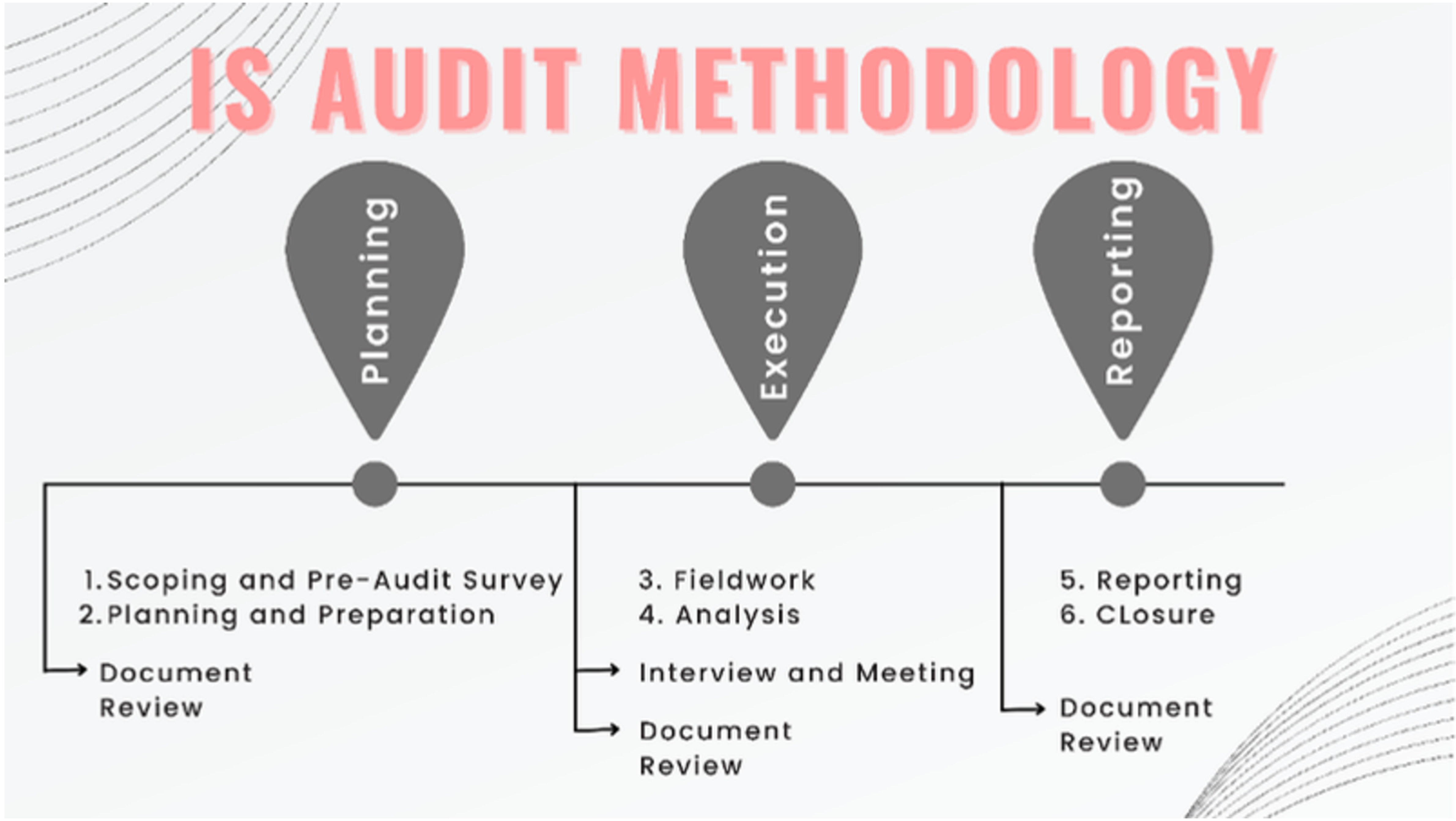
Darkweb Monitoring and Brand Protection

Provides solution for scanning and monitoring the Dark Web 24x7 for any exposed accounts connected with user email address; this contains the victim's name, phone number, social security number, address, bank details and other crucial personal details as well as responds to those threats.

We Provide Various Protection suites such as Brand Protection, Anti-Phishing , Brand Monitoring, Website Threat Protection, Third Part Assessment and Data Loss Recovery which include C-Level Executives account monitoring, domain suites, social suite, mobile app suite, brand suite which checks if the attacker is impersonating as legitimate person/firm.

IS Audit

- IT Frameworks
- ISO/IEC 27001
- Regulatory Audit
- Ransomware Readiness
- NIST Framework
- SOC 2



IS AUDIT METHODOLOGY

1. Scoping and Pre-Audit Survey
2. Planning and Preparation

→ Document Review

3. Fieldwork
4. Analysis

→ Interview and Meeting

→ Document Review

5. Reporting
6. CLosure

→ Document Review

VAPT: Vulnerability Assessment and Penetration Testing

Vulnerability Assessment

- Identification of Security Gaps in Business Infrastructure
- Professionals using global standard methodologies
- Experts in Web Applications, Modern APIs, Mobile Applications, IOT, Block Chain, Cloud Infrastructure
- Using industry standard tools such as Tenable, BurpSuite, Metasploit

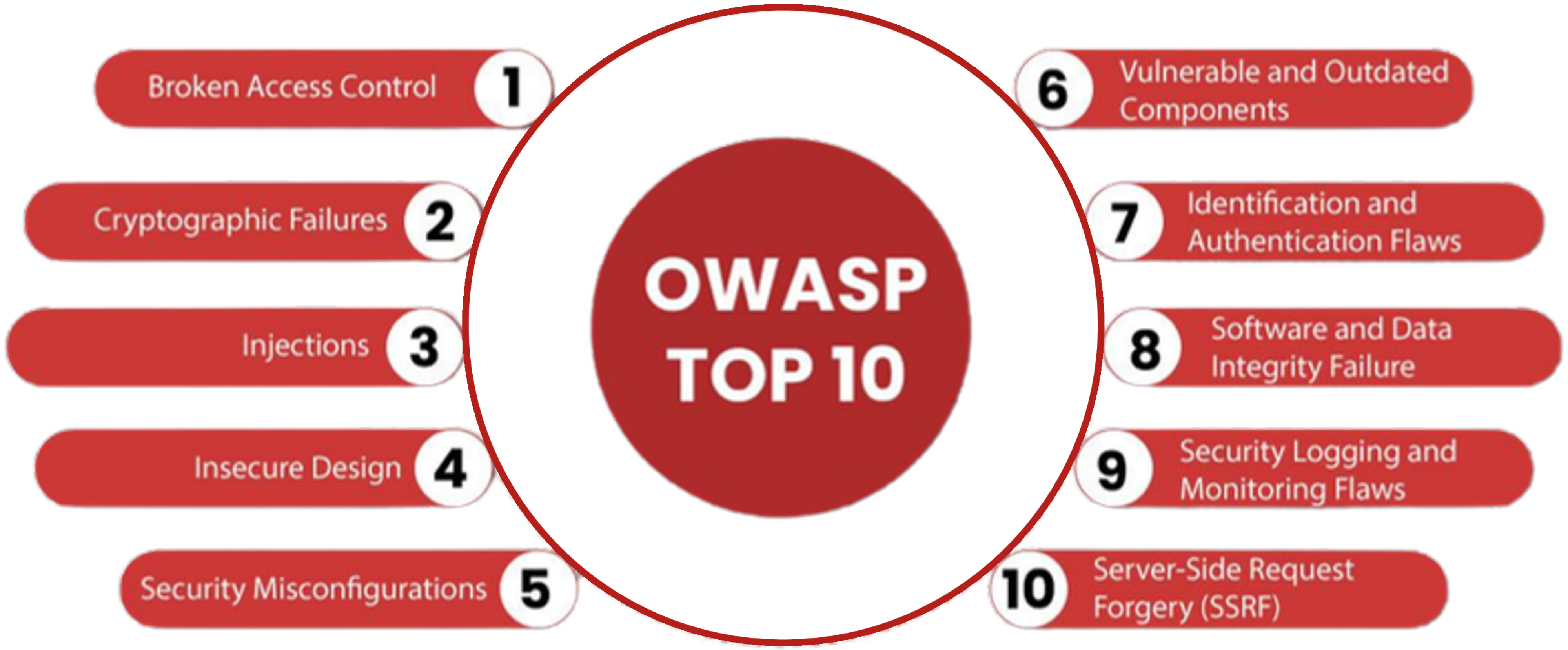
Penetration Testing

- Simulated cyber risk assessment
- Manual breach evaluation
- Provide attack narrative on identified vulnerabilities.
- Quick report for critical findings

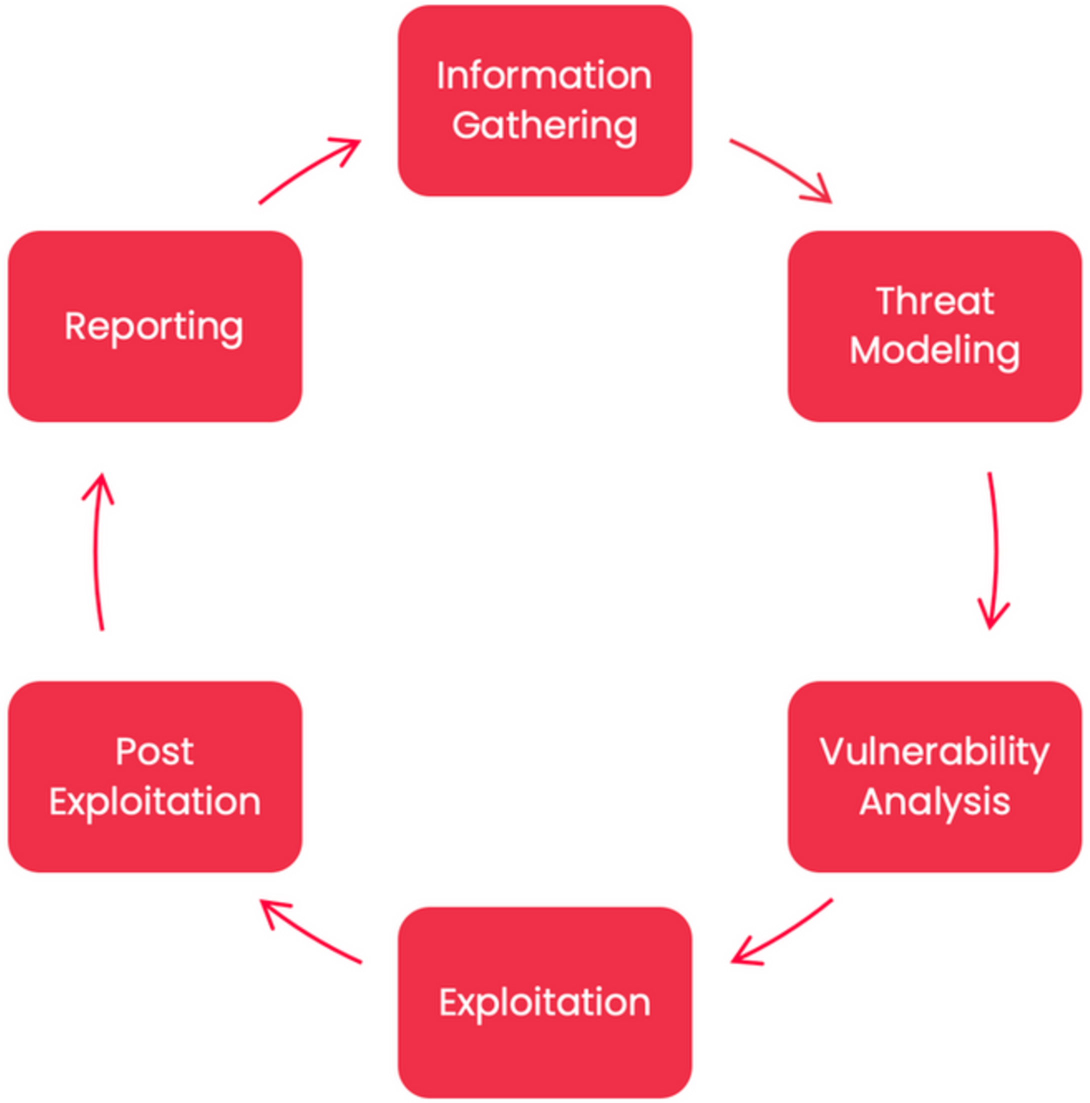
VAPT: Approach

Vulnerability Assessment & Penetration Testing

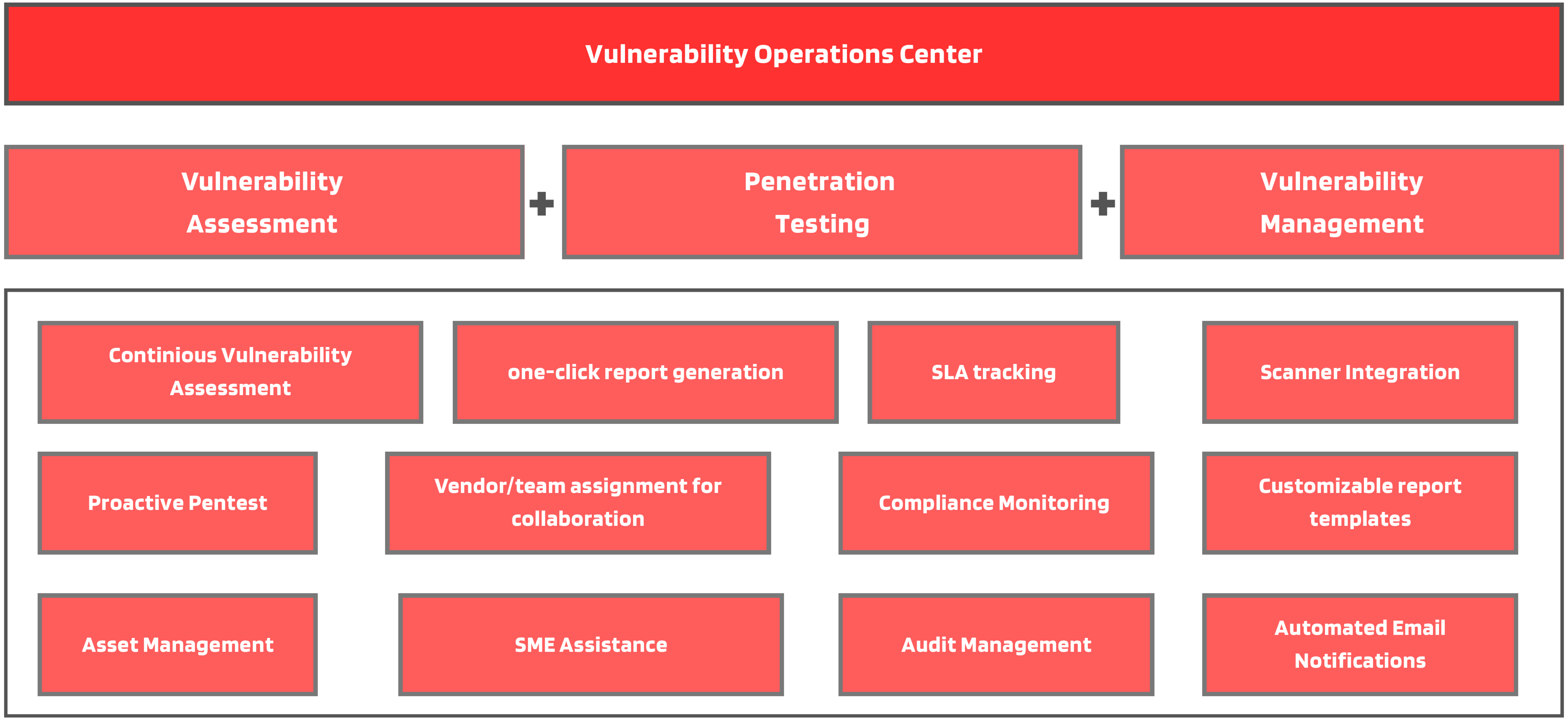
Testing Guideline


OWASP TOP 10
Broken Access Control 1
Cryptographic Failures 2
Injections 3
Insecure Design 4
Security Misconfigurations 5
6 Vulnerable and Outdated Components
7 Identification and Authentication Flaws
8 Software and Data Integrity Failure
9 Security Logging and Monitoring Flaws
10 Server-Side Request Forgery (SSRF)

Methodology



Vulnerability Operations Center



Vulnerability Operations Center

Vulnerability Assessment + Penetration Testing + Vulnerability Management

Continious Vulnerability Assessment

one-click report generation

SLA tracking

Scanner Integration

Proactive Pentest

Vendor/team assignment for collaboration

Compliance Monitoring

Customizable report templates

Asset Management

SME Assistance

Audit Management

Automated Email Notifications

Our Solutions

Our Team at CryptoGen Nepal has invested years of research to develop solutions to cater for Cyber Security requirements

Saycure.

Risk Monitoring

Detect, Correlate, Mitigate Security Risks.

- Threat Intelligence
- Vulnerability Detection
- File Integrity Monitoring

Risk Management

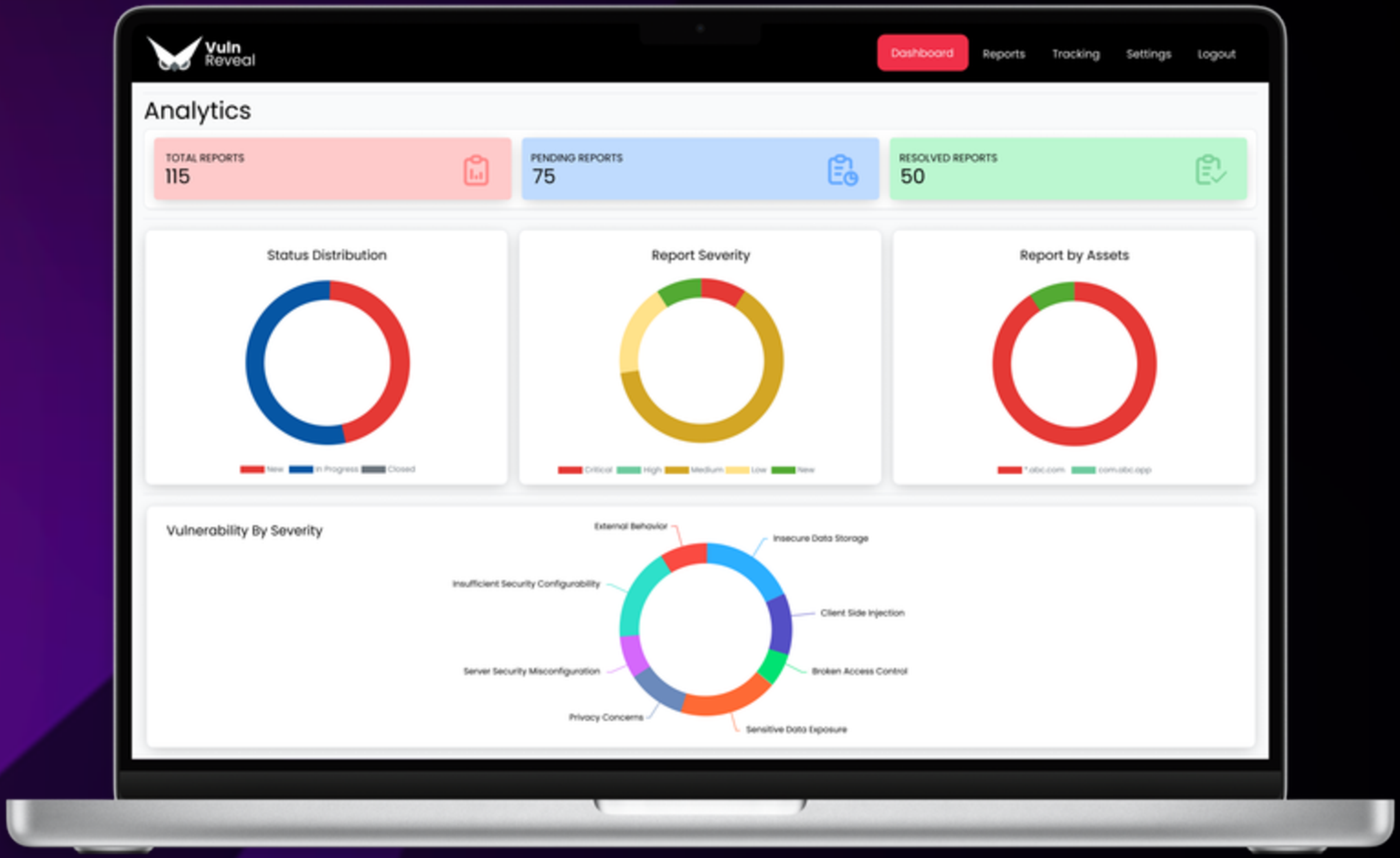
Visual Risk and Compliance Management.

- Vulnerability Tracking
- Compliance Management & Reporting
- Asset Tracking

CryptoGen Nepal

VulnReveal

Risk Operations Focused Solution



Analytics

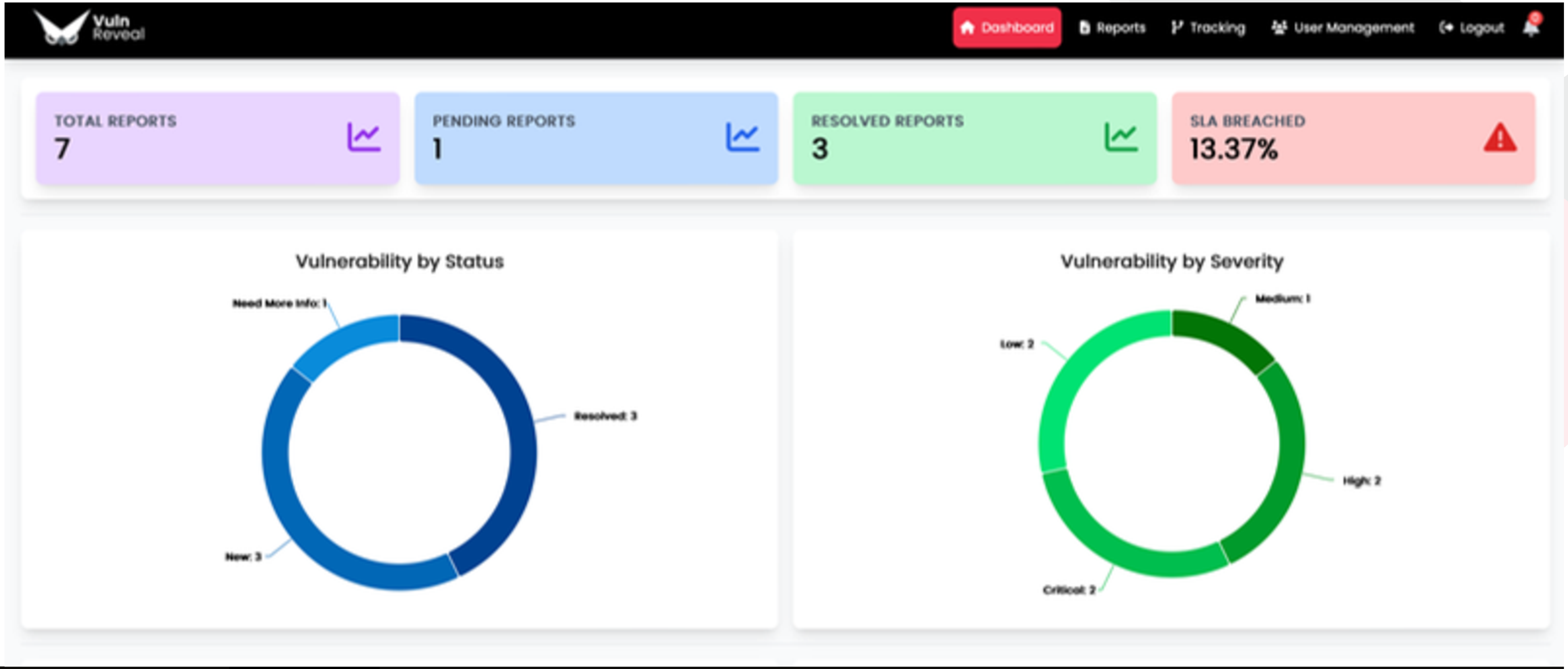
TOTAL REPORTS 115

PENDING REPORTS 75

RESOLVED REPORTS 50

Overview

Powerful Risk Operations management platform with capability to assist for Risk and Compliance Tasks.



TOTAL REPORTS 7

PENDING REPORTS 1

RESOLVED REPORTS 3

SLA BREACHED 13.37%

Vulnerability by Status

Vulnerability by Severity

PRIORITIZE RISK MITIGATION

Streamline with effcient risk management approach.

VULNERABILITY MANAGEMENT

Centralized view of vulnerabilities across infrastructure.

PROFFESIONAL INSIGHT

Our dedicated security professionals provide guidence in relation to the identified security risk.

Value Proposition

Get the complete visibility of all metrics associated with the VOC program and take advanced of all resources associated with your business critical application.

- Metrics based analytics
- Status of reported vulnerabilities
- Report based on criticality of the security risk
- Prioritization and enablement of responsible resources

CROWD SOURCED RISK ASSESSMENT

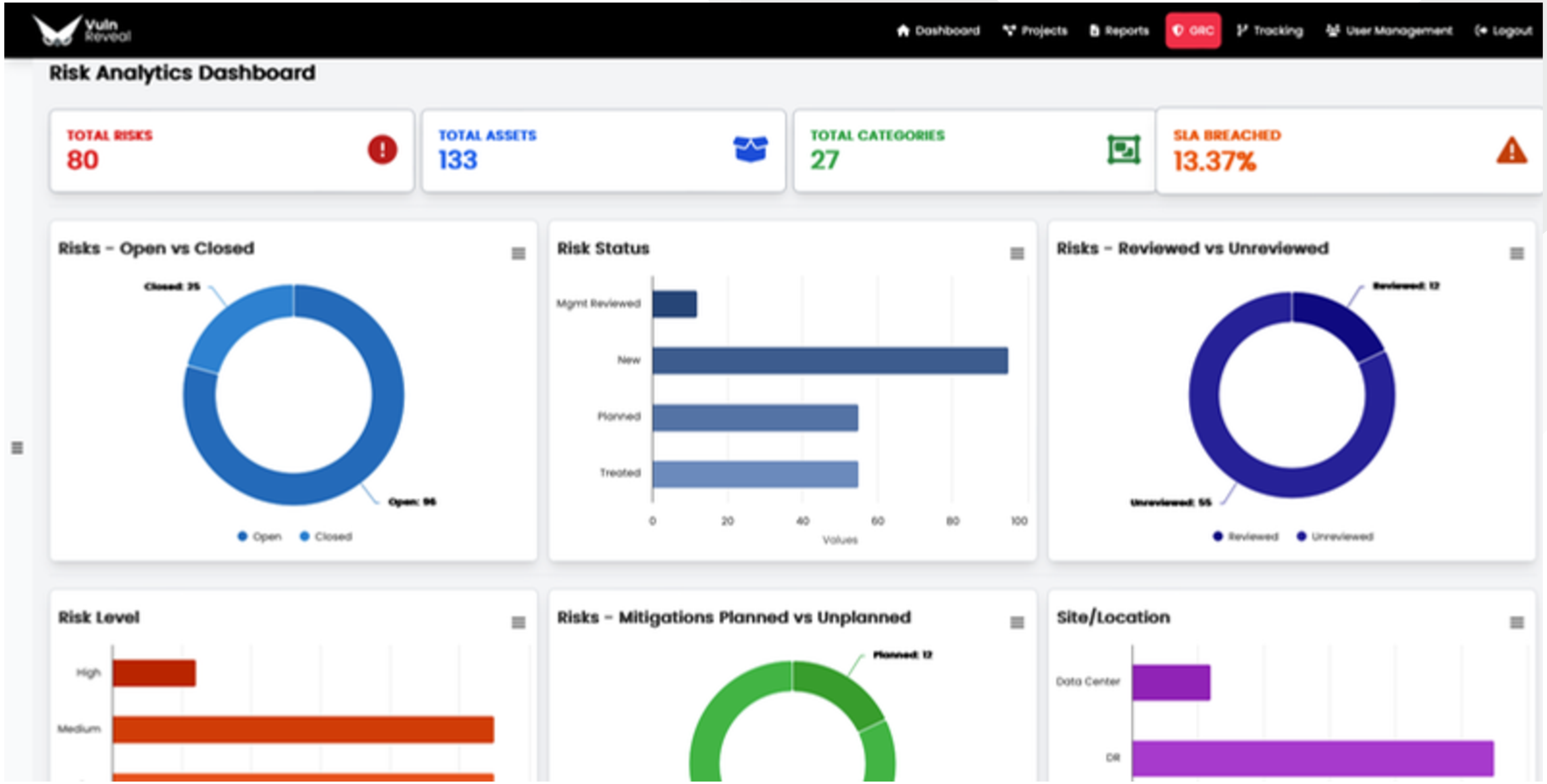
EXPERT INSIGHT

100% VISIBILITY
MANAGEMENT CONSOLE

TRANSPARENT WORKFLOW

Compliance Management

Get the complete visibility of your compliance and quickly manage your organizational requirements.



Risk Analytics Dashboard

TOTAL RISKS 80

TOTAL ASSETS 133

TOTAL CATEGORIES 27

SLA BREACHED 13.37%

Risks - Open vs Closed

Risk Status

Risks - Reviewed vs Unreviewed

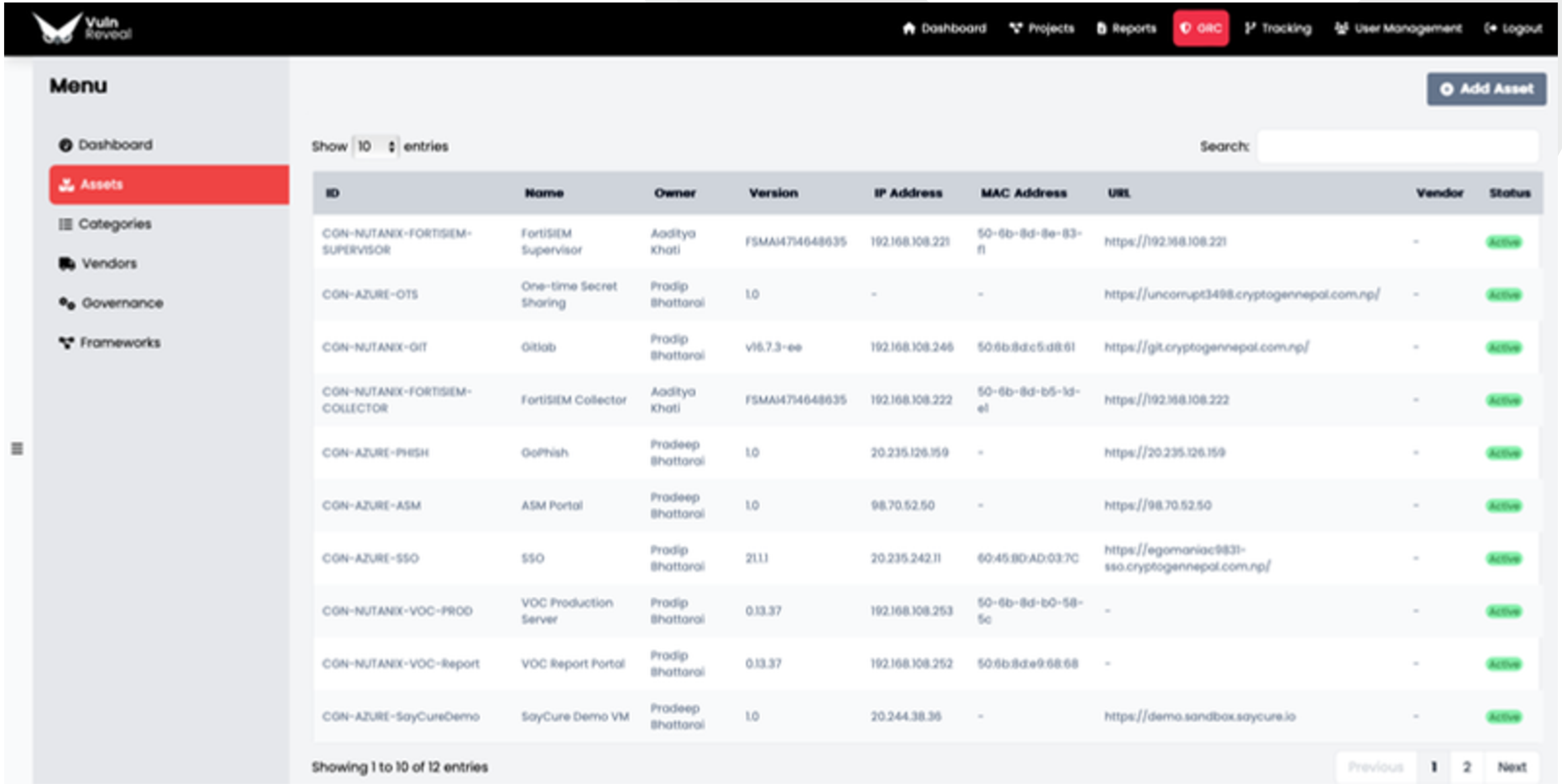
Risk Level

Risks - Mitigations Planned vs Unplanned

Site/Location

Asset Management

Track assets residing in the organization for richer visibility.

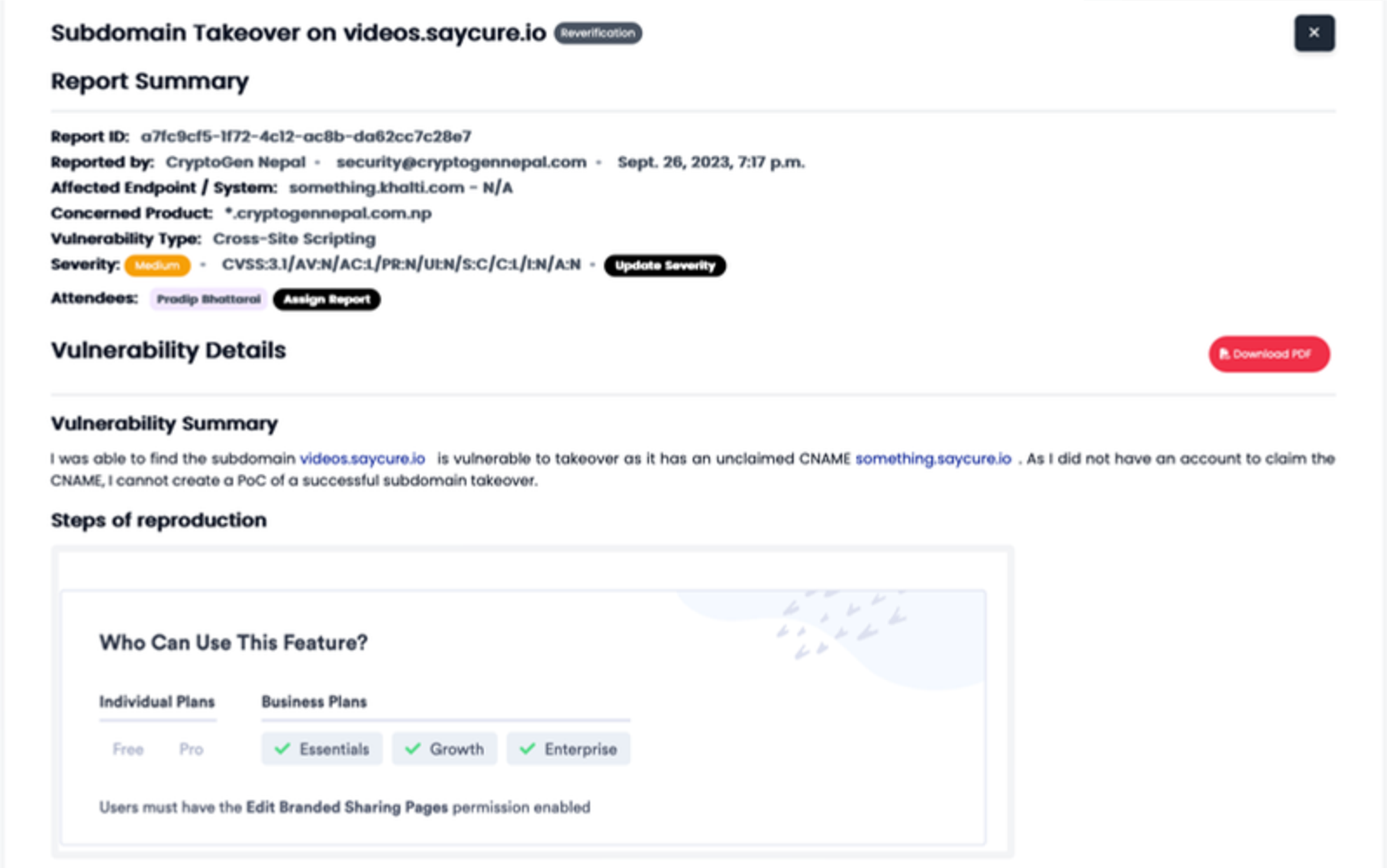


Show 10 entries

ID	Name	Owner	Version	IP Address	MAC Address	URL	Vendor	Status
CGN-NUTANIX-FORTISIEM-SUPERVISOR	FortiSIEM Supervisor	Aaditya Khati	FSMAI4714648635	192.168.108.221	50-6b-8d-8e-83-f1	https://192.168.108.221	-	Active
CGN-AZURE-OTS	One-time Secret Sharing	Pradip Bhattarai	1.0	-	-	https://uncorrupt3498.cryptogennepal.com.np/	-	Active
CGN-NUTANIX-GIT	Gitlab	Pradip Bhattarai	v16.7.3-ee	192.168.108.246	50:6b:8d:c5:d8:61	https://git.cryptogennepal.com.np/	-	Active
CGN-NUTANIX-FORTISIEM-COLLECTOR	FortiSIEM Collector	Aaditya Khati	FSMAI4714648635	192.168.108.222	50-6b-8d-b5-1d-e1	https://192.168.108.222	-	Active
CGN-AZURE-PHISH	GoPhish	Pradeep Bhattarai	1.0	20.235.126.159	-	https://20.235.126.159	-	Active
CGN-AZURE-ASM	ASM Portal	Pradeep Bhattarai	1.0	98.70.52.50	-	https://98.70.52.50	-	Active
CGN-AZURE-SSO	SSO	Pradip Bhattarai	21.1.1	20.235.242.11	60:45:BD:AD:03:7C	https://egomaniac9831-sso.cryptogennepal.com.np/	-	Active
CGN-NUTANIX-VOC-PROD	VOC Production Server	Pradip Bhattarai	0.13.37	192.168.108.253	50-6b-8d-b0-58-5c	-	-	Active
CGN-NUTANIX-VOC-Report	VOC Report Portal	Pradip Bhattarai	0.13.37	192.168.108.252	50:6b:8d:e9:68:68	-	-	Active
CGN-AZURE-SayCureDemo	SayCure Demo VM	Pradeep Bhattarai	1.0	20.244.38.36	-	https://demo.sandbox.saycure.io	-	Active

Showing 1 to 10 of 12 entries

Report Management



Subdomain Takeover on videos.saycure.io

Report Summary

Report ID: a7fc9cf5-1f72-4c12-ac8b-da62cc7c28e7
Reported by: CryptoGen Nepal · security@cryptogennepal.com · Sept. 26, 2023, 7:17 p.m.
Affected Endpoint / System: something.khalti.com - N/A
Concerned Product: *.cryptogennepal.com.np
Vulnerability Type: Cross-Site Scripting
Severity: Medium · CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N · Update Severity
Attendees: Pradip Bhattarai Assign Report

Vulnerability Details

Vulnerability Summary

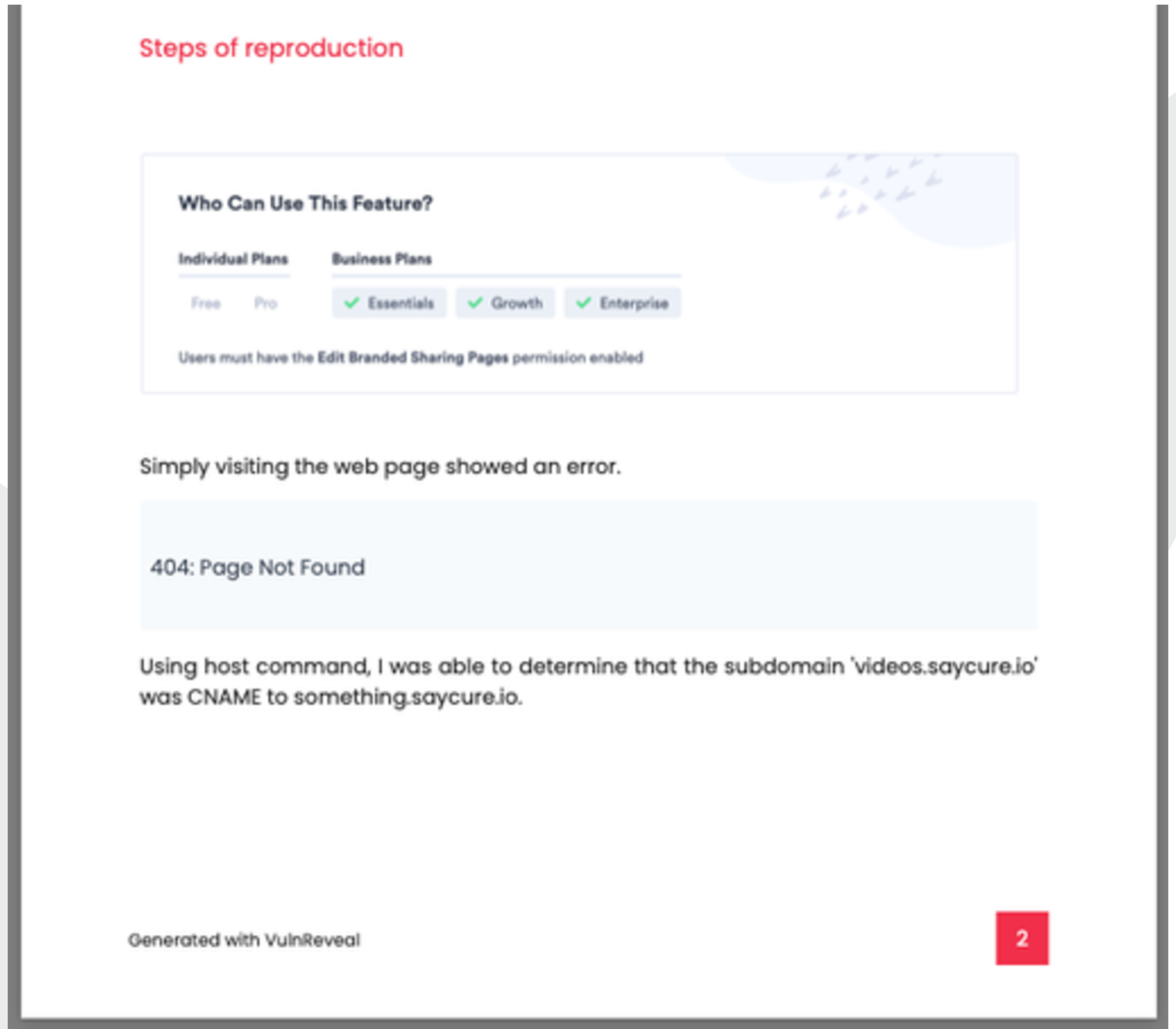
I was able to find the subdomain videos.saycure.io is vulnerable to takeover as it has an unclaimed CNAME something.saycure.io . As I did not have an account to claim the CNAME, I cannot create a PoC of a successful subdomain takeover.

Steps of reproduction

Who Can Use This Feature?

Individual Plans: Free, Pro
Business Plans: ✓ Essentials, ✓ Growth, ✓ Enterprise

Users must have the **Edit Branded Sharing Pages** permission enabled



Steps of reproduction

Who Can Use This Feature?

Individual Plans: Free, Pro
Business Plans: ✓ Essentials, ✓ Growth, ✓ Enterprise

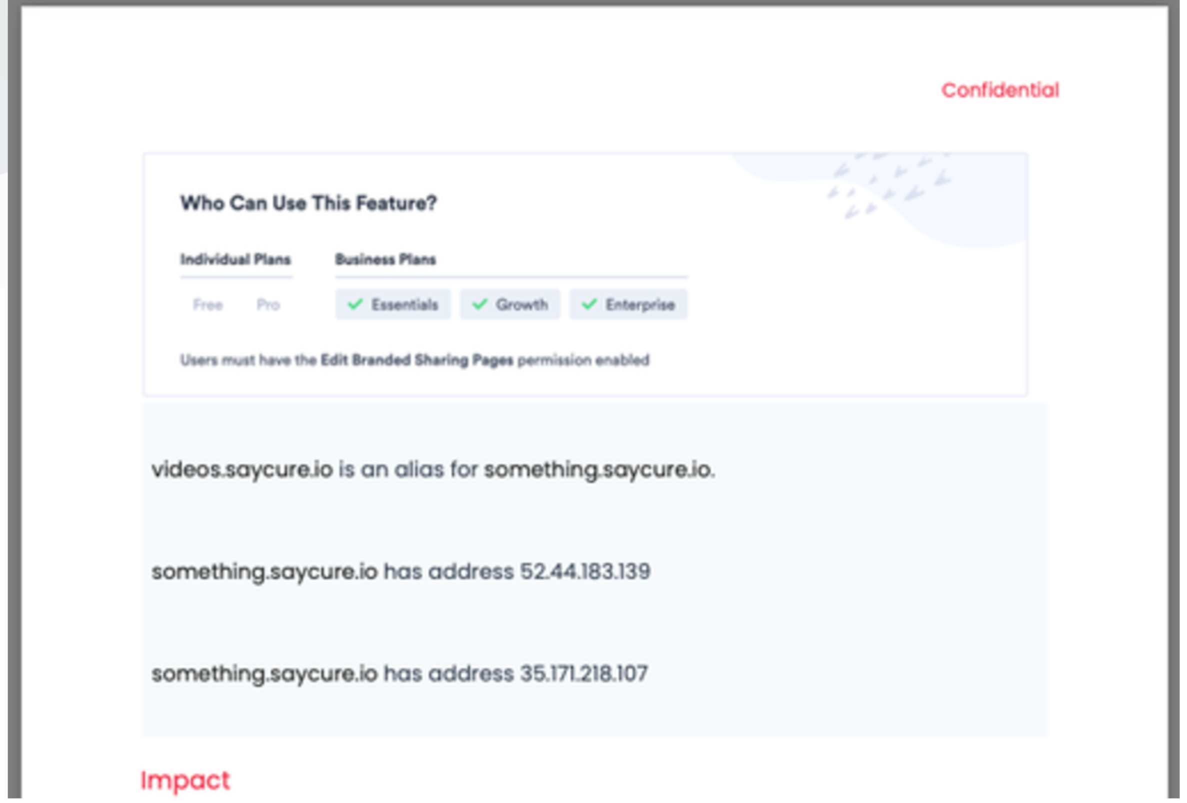
Users must have the **Edit Branded Sharing Pages** permission enabled

Simply visiting the web page showed an error.

```
404: Page Not Found
```

Using host command, I was able to determine that the subdomain 'videos.saycure.io' was CNAME to something.saycure.io.

Generated with VulnReveal 2



Confidential

Who Can Use This Feature?

Individual Plans: Free, Pro
Business Plans: ✓ Essentials, ✓ Growth, ✓ Enterprise

Users must have the **Edit Branded Sharing Pages** permission enabled

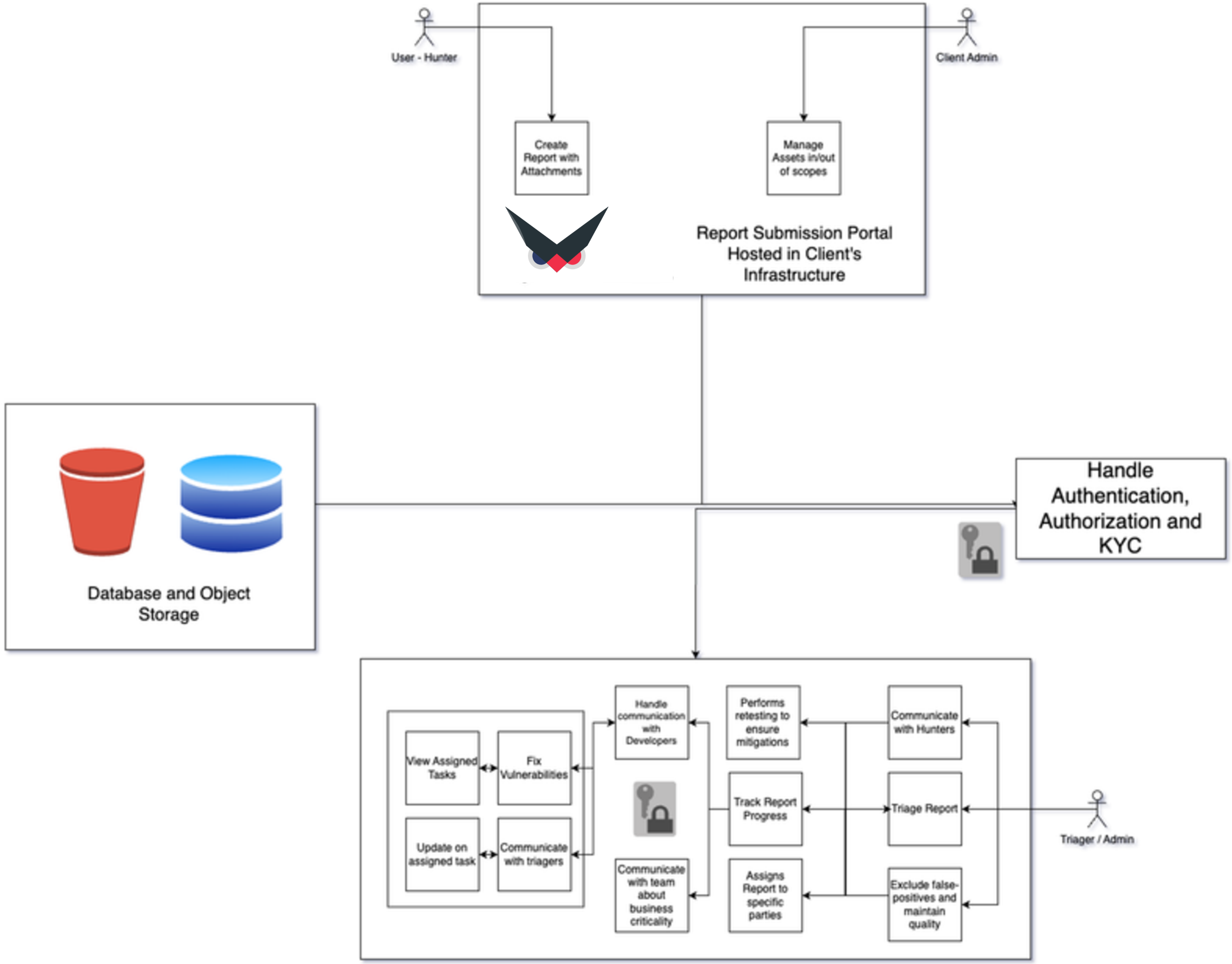
```
videos.saycure.io is an alias for something.saycure.io.

something.saycure.io has address 52.44.183.139

something.saycure.io has address 35.171.218.107
```

Impact

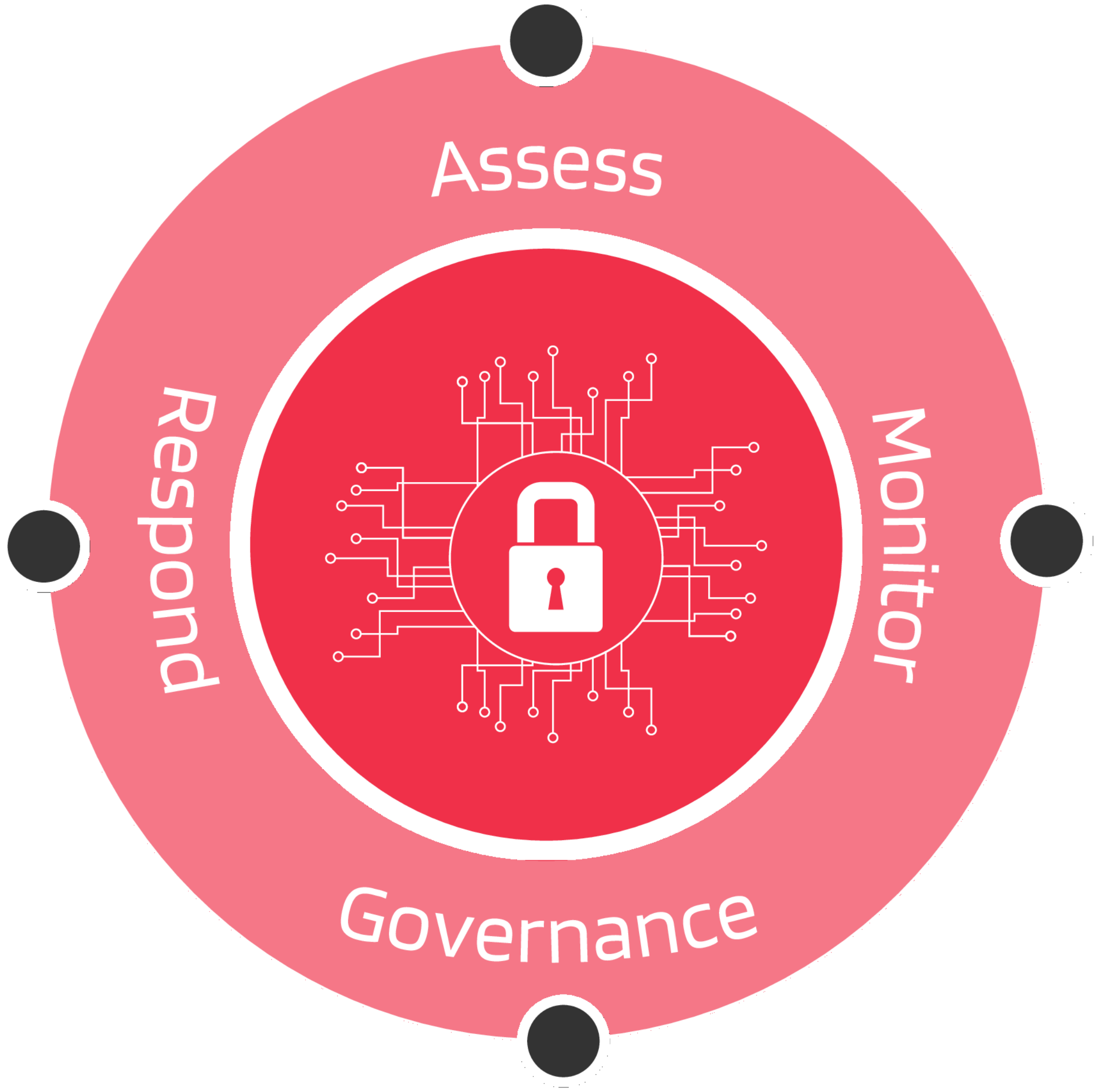
Solution Components


User - Hunter
Client Admin
Create Report with Attachments
Manage Assets in/out of scopes
Report Submission Portal Hosted in Client's Infrastructure
Database and Object Storage
Handle Authentication, Authorization and KYC
View Assigned Tasks
Fix Vulnerabilities
Update on assigned task
Communicate with triagers
Handle communication with Developers
Communicate with team about business criticality
Performs retesting to ensure mitigations
Track Report Progress
Assigns Report to specific parties
Communicate with Hunters
Triage Report
Exclude false-positives and maintain quality
Triager / Admin

Self-assessment

Do you have a continuous visibility to cyber risk and vulnerabilities?

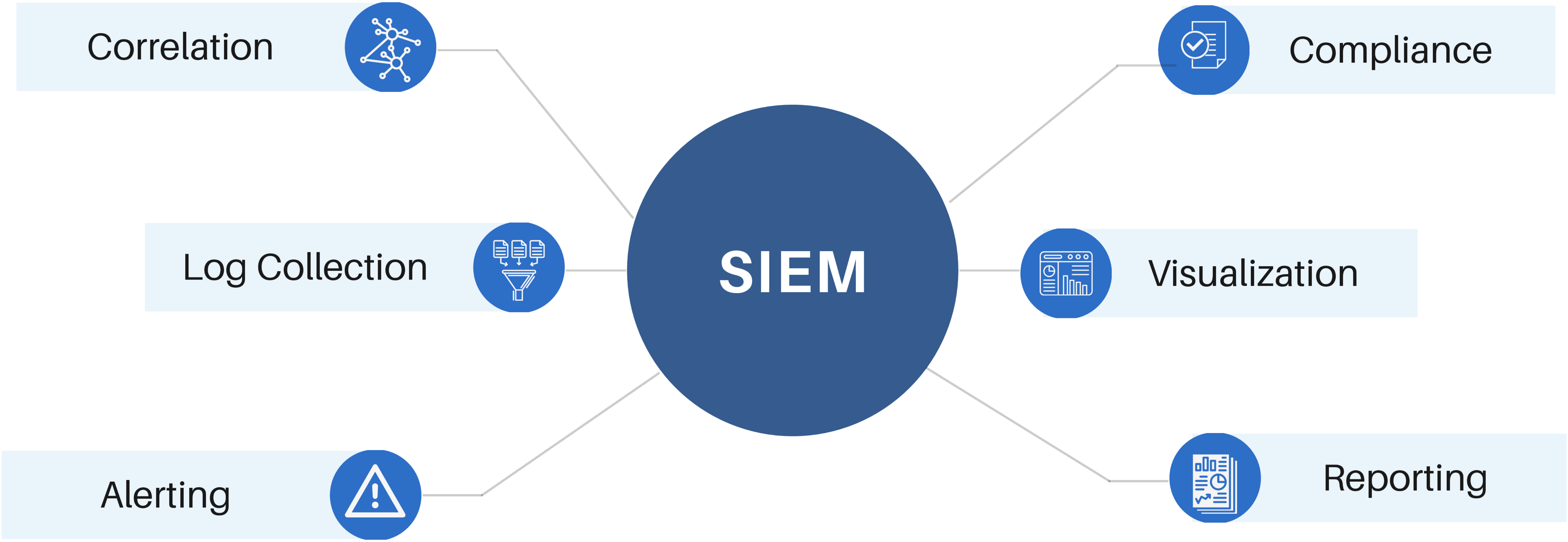
What measures are being taken to mitigate risk expect adding another security product?



Do you have visibility of your internal and external information?

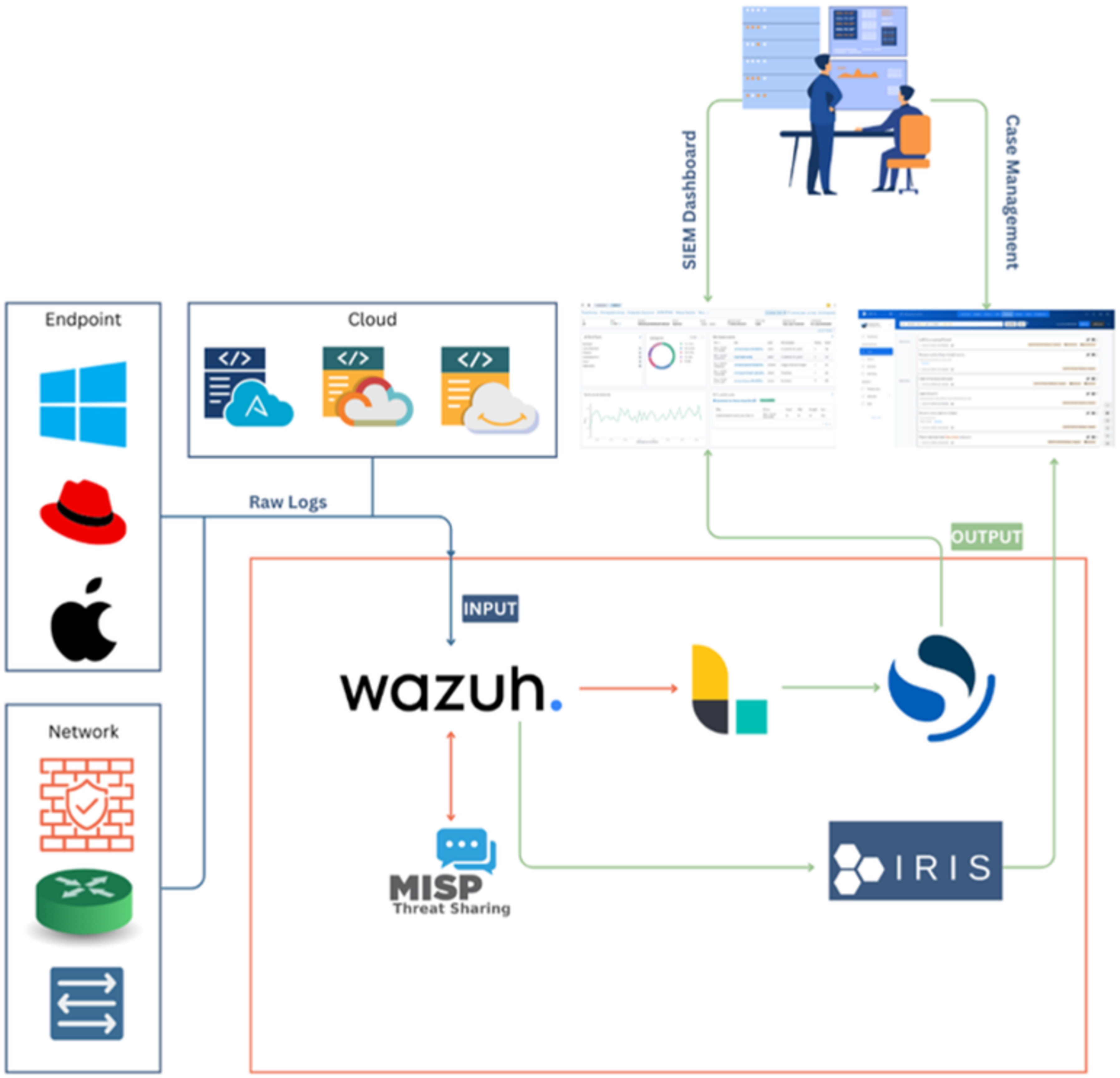
How many compliances do you plan to follow this year?

SIEM as a Product



SayCure as a Product

- Endpoint Detection
- Response Action
- Case Management
- Threat Intelligence Platform
- Endpoint vulnerability detection
- Compliance Monitoring
- Dashboard Customization



SayCure as a Solution

SIEM

- Aggregate Logs
- Generate Alerts
- Event Correlation
- Vulnerability Management
- Compliance

Analytics

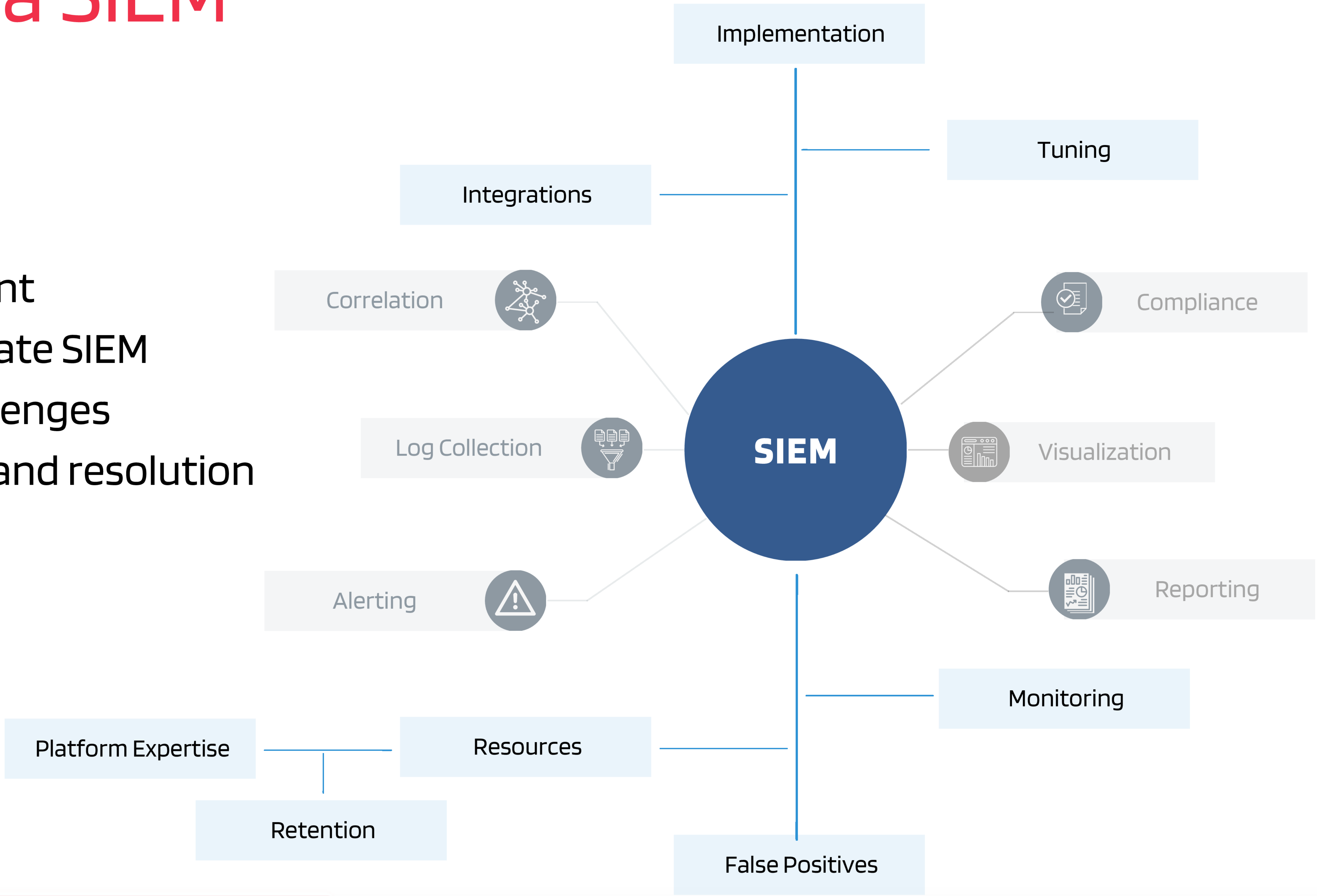
- Consolidate Security Alert
- API Integration
- Case Management
- Automated Response

SOC

- Qualify Anomalies
- Threat Hunt & Incident Response
- Alert Prioritization & response
- Periodic Actionable Report

Complexities of a SIEM

- SIEM Tuning and Management
- Technical Resources to operate SIEM
- Continuous monitoring challenges
- False positive identification and resolution



Security Operations Center

Security Operations Center is a modern necessity for protecting business services by establishing a base identification, continious monitoring and response through, skilled manpower, standard procedures and detection technologies.

SOC is built through three (3) key aspects:

PEOPLE

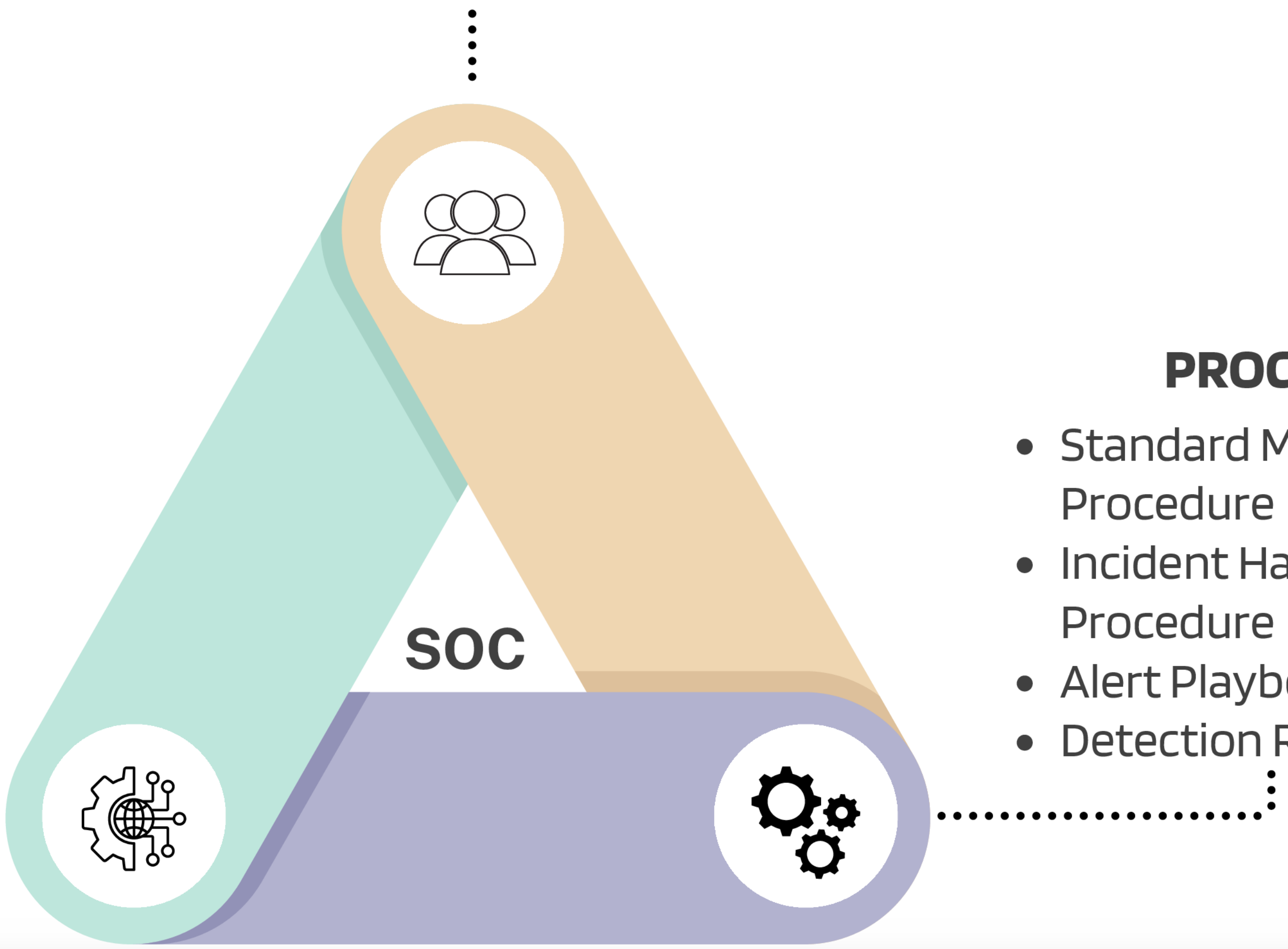
- Skilled Detection Analyst
- Defined Responsibilities
- Qualified Team Lead
- Alert Engineers

TECHNOLOGY

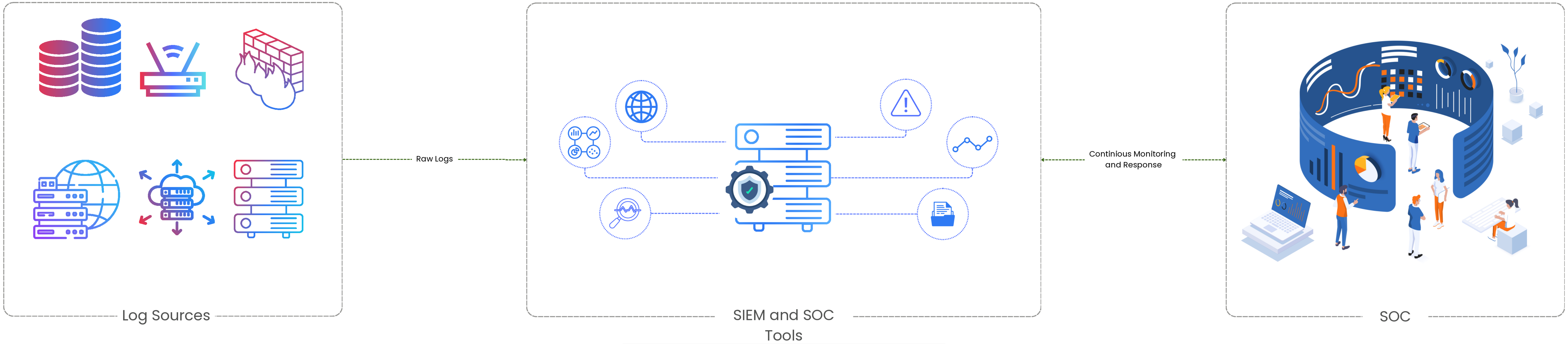
- Security Information and Event Management (SIEM)
- Threat Intelligence
- Incident Management

PROCESS

- Standard Monitoring Procedure
- Incident Handling Procedure
- Alert Playbook
- Detection Runbook



Operational Process of SOC



Log Sources:

- Firewall
- Web Application Firewall (WAF)
- Anti-virus (AV) and End-point Protection (EPP)
- Business Critical Application Servers
- Database Servers
- Identity and Access Management
- Active Directory (AD)
- Privilege Access Management (PAM)

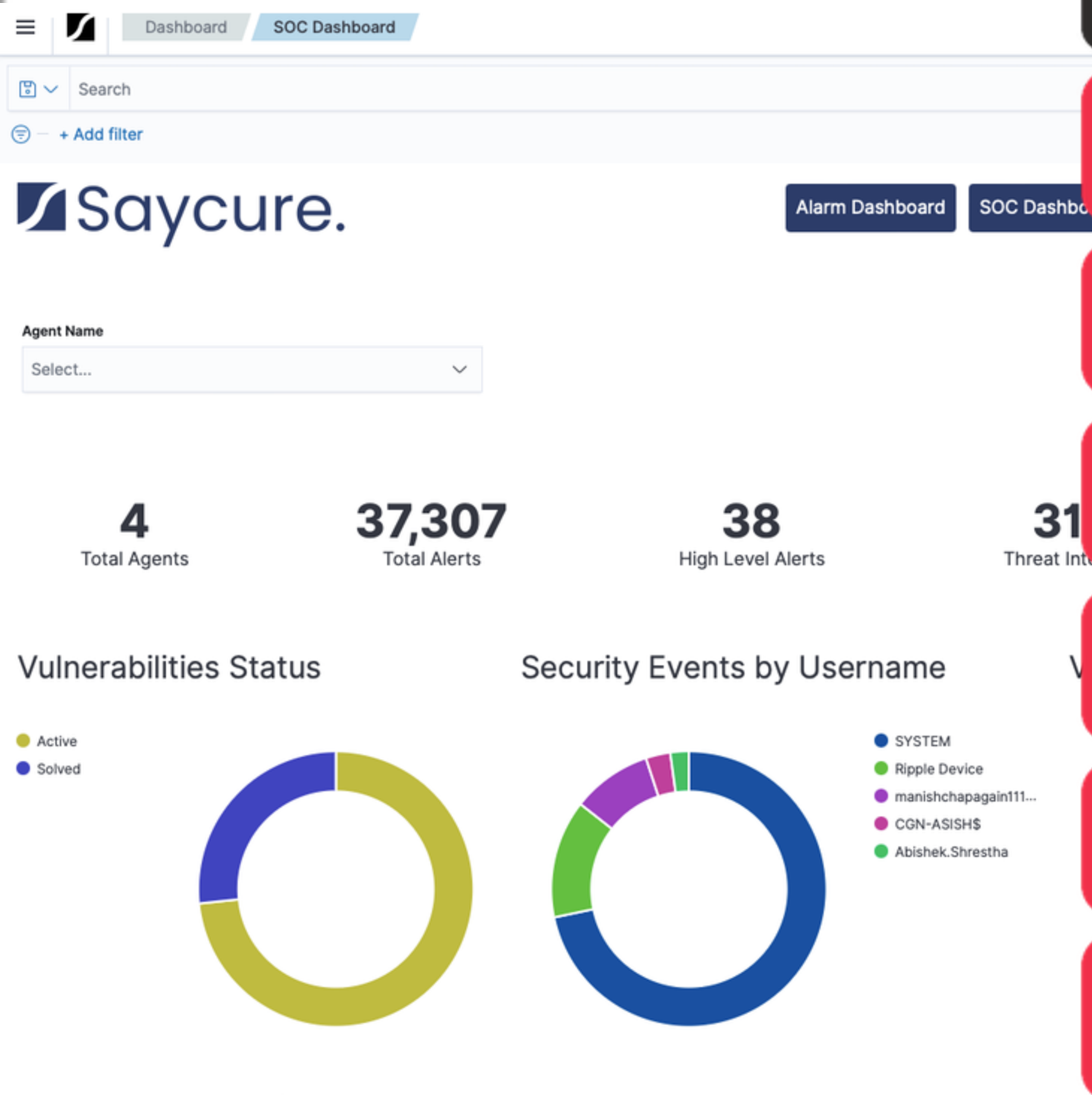
SOC Technologies:

- SIEM
- Case/Incident Management
- Threat Intelligence
- File & Registry Integrity Monitoring
- Vulnerability Management Platform
- Dark Web Scanning Tool

SOC:

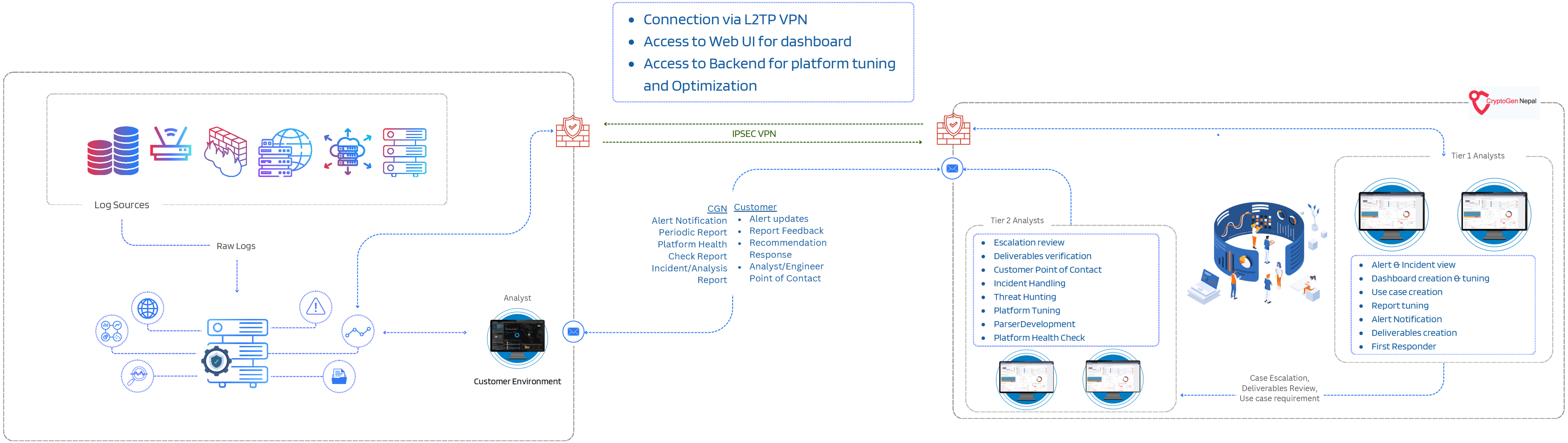
- 24x7 Detection and Response
- Alert Qualification and Escalation
- Incident Handling
- Periodic Vulnerability Assessment
- Compromise Assessment
- Digital Forensics

SayCure as a Solution



Problem	Description	SayCure SOC-as-a-Service
Log Management	SayCure utilizes log management to track, store and analyze security-related data, enabling effective threat detection and response.	SayCure is a comprehensive SIEM solution that assists to retain logs for compliance and forensics purposes.
Threat Monitoring	SayCure monitors for security threats across all endpoints, network traffic, and user behavior to quickly identify and remediate potential risks.	Our SOC team monitors client's infrastructure 24x7 for identifying, qualifying and steps to eradicate threats.
Incident Handling	SayCure assists to timely and effectively respond to security incidents, minimizing damage and ensuring business continuity.	SayCure SOC comprises of security practicionairs to qualify alerts into incidents and analyze for Root Cause.
Vulnerability Assessment	Vulnerability assessment for identifying gaps in systems and applications across your environment	Our team consists of offensive security experts to perform periodic Vulnerability Assessment and report gaps on your environment
Phishing Campaign	Conduct phishing campaigns to simulate attacks and educate employees on how to recognize and avoid them.	Our in-house developed phishing simulation helps clients to determine phishing readiness of the users and provide insight with training.
Compliance Monitoring	Monitor compliance with industry standards and regulations, including HIPAA, PCI DSS, and GDPR, NIST 800-53, etc.	Our SayCure platform has out-of-the-box compliance monitoring and reporting in addition to gap analysis and readiness for your compliance needs

SOC Architecture



- Connection via L2TP VPN
- Access to Web UI for dashboard
- Access to Backend for platform tuning and Optimization

Log Sources

Raw Logs

Analyst

Customer Environment

IPSEC VPN

CGN
Alert Notification
Periodic Report
Platform Health Check Report
Incident/Analysis Report

Customer
- Alert updates
- Report Feedback
- Recommendation Response
- Analyst/Engineer Point of Contact

CryptoGen Nepal

Tier 1 Analysts

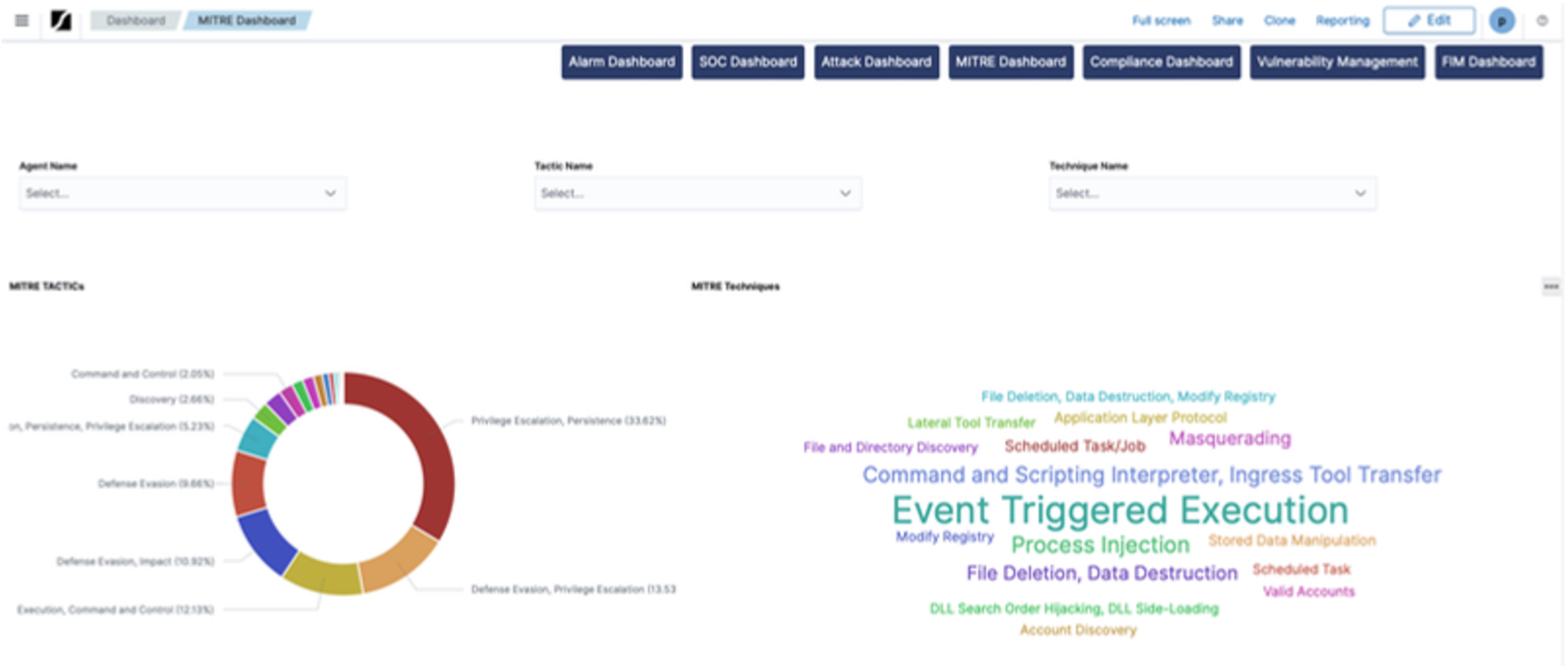
- Alert & Incident view
- Dashboard creation & tuning
- Use case creation
- Report tuning
- Alert Notification
- Deliverables creation
- First Responder

Tier 2 Analysts

- Escalation review
- Deliverables verification
- Customer Point of Contact
- Incident Handling
- Threat Hunting
- Platform Tuning
- ParserDevelopment
- Platform Health Check

Case Escalation,
Deliverables Review,
Use case requirement

SayCure as a Solution


Dashboard
MITRE Dashboard
Full screen
Share
Clone
Reporting
Edit
Alarm Dashboard
SOC Dashboard
Attack Dashboard
MITRE Dashboard
Compliance Dashboard
Vulnerability Management
FIM Dashboard
MITRE TACTICs
Command and Control (2.05%)
Discovery (2.66%)
on, Persistence, Privilege Escalation (5.23%)
Defense Evasion (9.66%)
Defense Evasion, Impact (10.92%)
Execution, Command and Control (12.13%)
Privilege Escalation, Persistence (33.62%)
Defense Evasion, Privilege Escalation (13.53
MITRE Techniques
File Deletion, Data Destruction, Modify Registry
Lateral Tool Transfer
Application Layer Protocol
File and Directory Discovery
Scheduled Task/Job
Masquerading
Command and Scripting Interpreter, Ingress Tool Transfer
Event Triggered Execution
Modify Registry
Process Injection
Stored Data Manipulation
File Deletion, Data Destruction
Scheduled Task
Valid Accounts
DLL Search Order Hijacking, DLL Side-Loading
Account Discovery

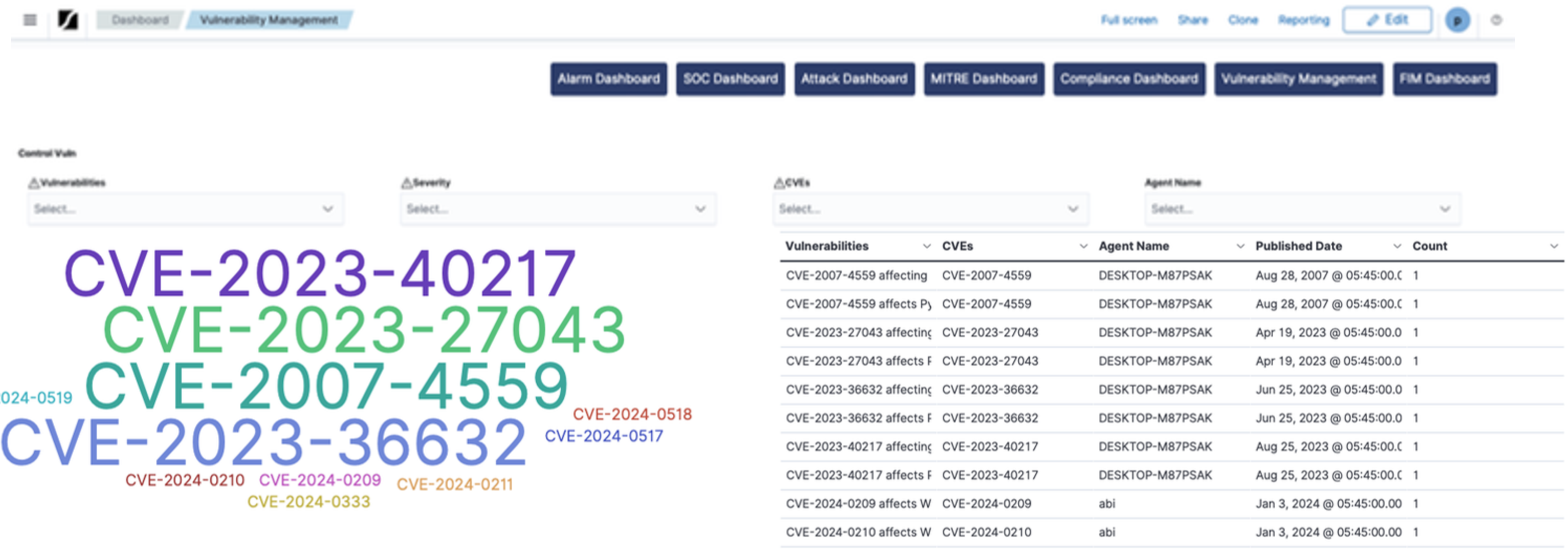
Agent Name: Select...

Tactic Name: Select...

Technique Name: Select...

Mapping MITRE Tactics and Techniques to the logs for threat navigation

SayCure as a Solution

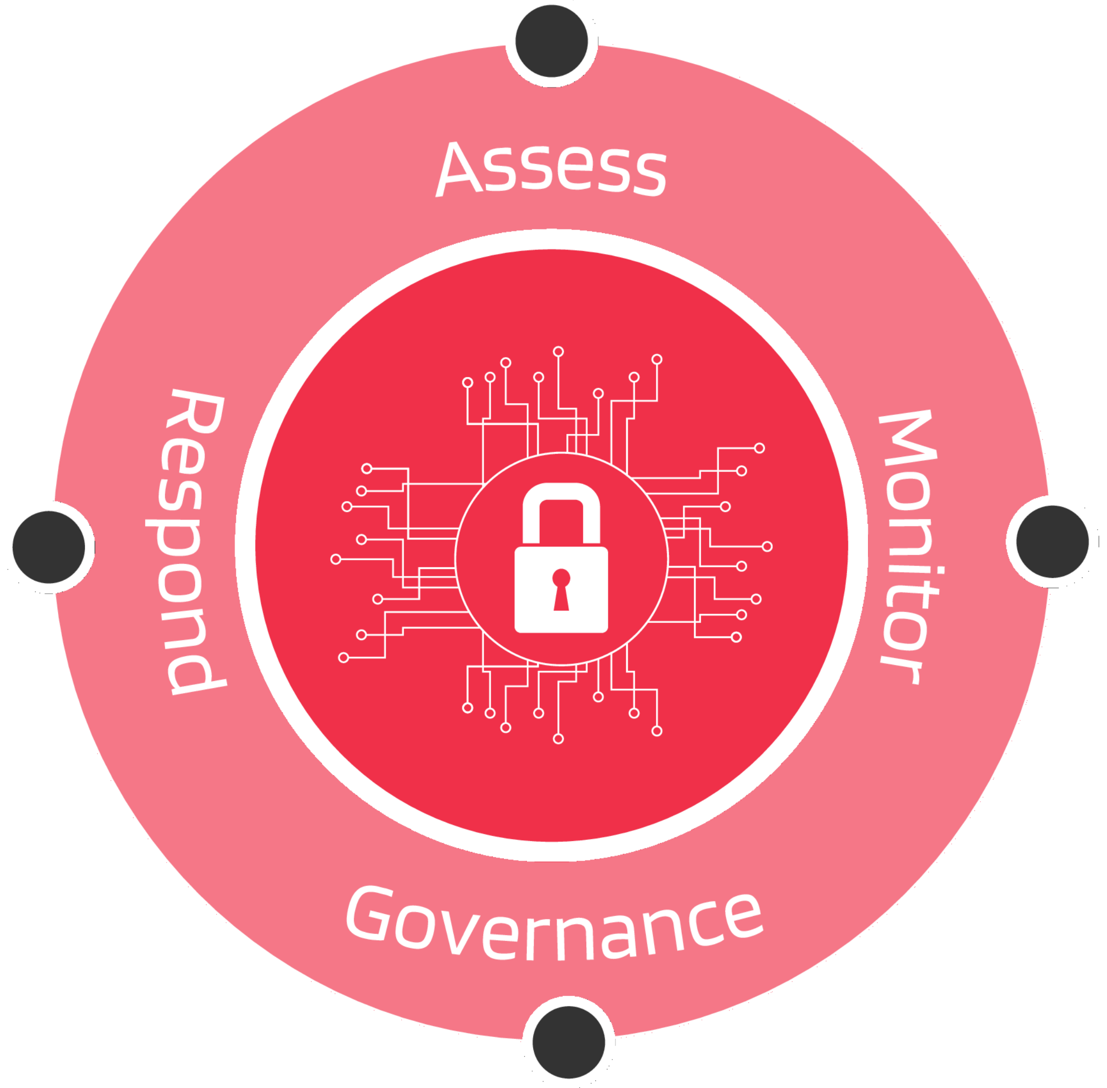


Vulnerabilities	CVEs	Agent Name	Published Date	Count
CVE-2007-4559 affecting	CVE-2007-4559	DESKTOP-M87PSAK	Aug 28, 2007 @ 05:45:00.(	1
CVE-2007-4559 affects Py	CVE-2007-4559	DESKTOP-M87PSAK	Aug 28, 2007 @ 05:45:00.(	1
CVE-2023-27043 affecting	CVE-2023-27043	DESKTOP-M87PSAK	Apr 19, 2023 @ 05:45:00.0	1
CVE-2023-27043 affects F	CVE-2023-27043	DESKTOP-M87PSAK	Apr 19, 2023 @ 05:45:00.0	1
CVE-2023-36632 affecting	CVE-2023-36632	DESKTOP-M87PSAK	Jun 25, 2023 @ 05:45:00.0	1
CVE-2023-36632 affects F	CVE-2023-36632	DESKTOP-M87PSAK	Jun 25, 2023 @ 05:45:00.0	1
CVE-2023-40217 affecting	CVE-2023-40217	DESKTOP-M87PSAK	Aug 25, 2023 @ 05:45:00.(	1
CVE-2023-40217 affects F	CVE-2023-40217	DESKTOP-M87PSAK	Aug 25, 2023 @ 05:45:00.(	1
CVE-2024-0209 affects W	CVE-2024-0209	abi	Jan 3, 2024 @ 05:45:00.00	1
CVE-2024-0210 affects W	CVE-2024-0210	abi	Jan 3, 2024 @ 05:45:00.00	1

Agent based Vulnerability Detection

Cyber Security Coverage

- Vulnerability Assessment
- Penetration Testing
- Phishing Campaign



- Cyber Security Consultation
- CXO training
- Cyber Security Awareness
- Incident Response

- SIEM
- Vulnerability Management
- Dark Web Monitoring
- Brand Protection
- Security Monitoring

- ISO 27001 (ISMS)

- IT Audit
- Ransomware Audit