



**elogics**

**Systems**

The technology solutions architects



**systems**

---

**Information Security  
Services Offerings**

systems x  **elogics**  
Systems  
The technology solutions architects

Driving **innovation**  
**and technological**  
**advancement**  
in Kuwait together





Delivering Seamlessly  
for a Digital Tomorrow

**\$154 M+**

Annual  
Turnover

**8500+**

Employees  
Globally

**233+**

Global Active  
Clients

**46+**

Years In Business

Systems Limited is a premier global SI company with a team of over 8500+ brilliant minds who continue to innovate in building leading enterprise solutions that ensure a promising future of our customers' digital footprint for sustainable growth and profitability. We are passionate about solving our customers' challenges using customized, scalable, and efficient products and services across 16+ countries. Our ability to improve, accelerate, and generate key competencies is driven by our investment in our people.



**Subsidiaries and Affiliates:**

- **Elogics Systems – Partner for Kuwait**
- Systems MEA
- Systems KSA
- Systems APAC
- **NdcTech – Banking & FI – TEMENOS Partners**
- EP Systems
- Systems Ventures
- Visionet (North America, Europe & UK)



Digital Transformation,  
Cloud Enablement & Data-  
Driven Service Portfolio



Success-Proof Methodologies



Strong Partner network



Value Offerings and Accelerators

## GRC



Gap Assessment and Readiness Services  
Enterprise IS Strategy Management  
Policies and Procedures  
Risk Management  
ISO 27001, ISO 22301  
ISO 27017, ISO 27018  
COBIT Controls  
PCI-DSS

## Technology Offering



Unified Cloud Security Management  
Cloud Security Controls

Digital Fraud Protection  
X/EDR – Endpoint & Server Security  
Mobile Device Management  
Privilege Access Management  
Data Loss Prevention  
API Security  
Micro segmentation

SIEM Deployment & Support  
SOAR Deployment & Support  
Playbook Creation and Deployment  
Use Case Creation and Deployment

## Managed Security



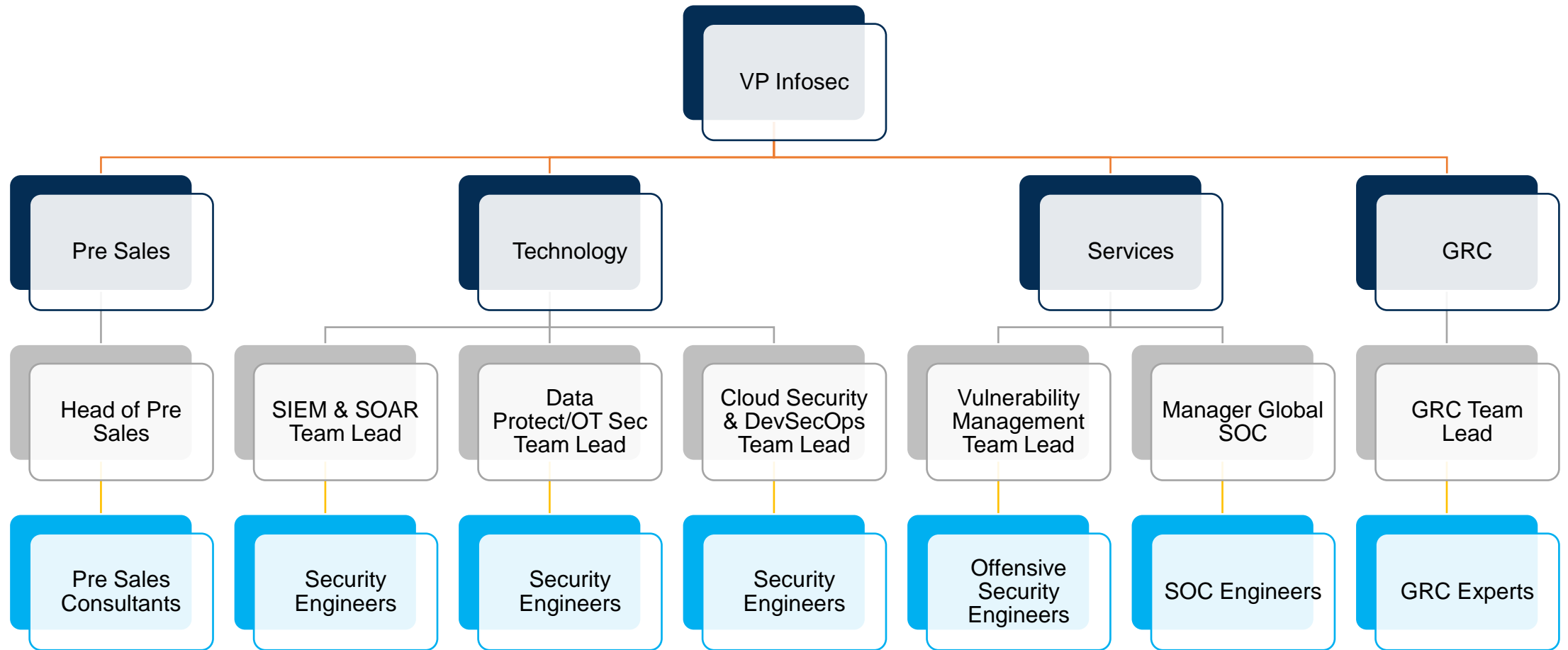
Managed Vulnerability Assessment  
Penetration Testing  
Red Team Operations

Compromise Assessment

24x7 Managed SOC Services  
Digital Forensics & Incident Report  
Advance Treat Hunting  
Managed Security Operations

**Managed Security Services Provider**

# Infosec Department Structure



## PAM – People Management



## Digital Fraud Protection



## Email & Web Security



## Data Security



## API Security & Micro segmentation



## SIEM



## X/E DR



## Deep Security



## SOAR



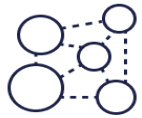
## OT Security



# API Security Challenges

## A Massive New Attack Surface

The nature of today's API landscape makes them very attractive to threat actors



APIs are everywhere

APIs are growing more than 200% per year\*



APIs are changing constantly

28% developers say they deploy APIs into production once a week\*



API vulnerabilities are easy to exploit

76% of organizations have had an API-related breach in the past year\*

## Existing Approaches Aren't Enough



Web Application Firewalls



API Gateways



Bug Bounties



Red Teams



API Inventories

Contextless and Limited Effectiveness & Scope

Expensive and Infrequent

Manual, Difficult and Incomplete

By 2025, less than 50% of enterprise APIs will be managed, as explosive growth in APIs surpasses the capabilities of API management tools – Gartner`

# Noname Security -API Security

## The Pillars of API Security

Complete API security covers the entire lifecycle of an API



### Posture Management

API asset inventory, change detection, configuration control and vulnerability.



### Runtime Protection

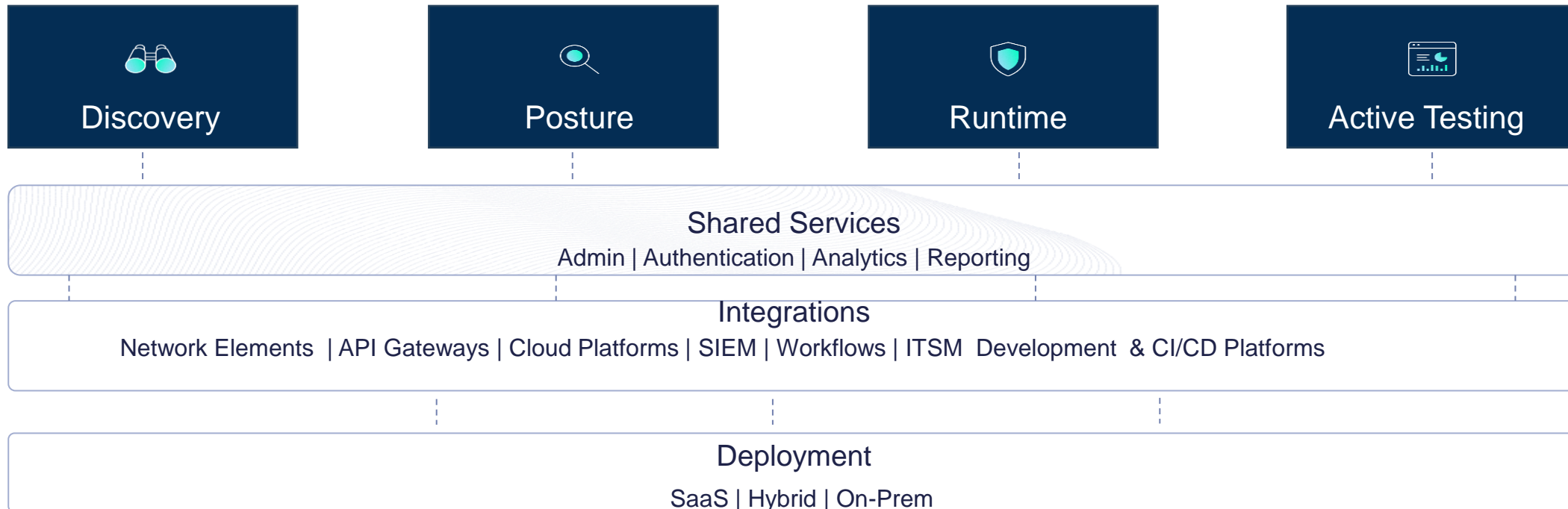
Detection and prevention of attackers and suspicious behavior in real time.



### API Security Testing

Securing your APIs during development and before they hit production.

## The Noname API Security Platform





# Micro segmentation

## Reduce your attack surface

Reduce risk without the need for costly security hardware with a software-based micro segmentation approach.

## Prevent lateral movement

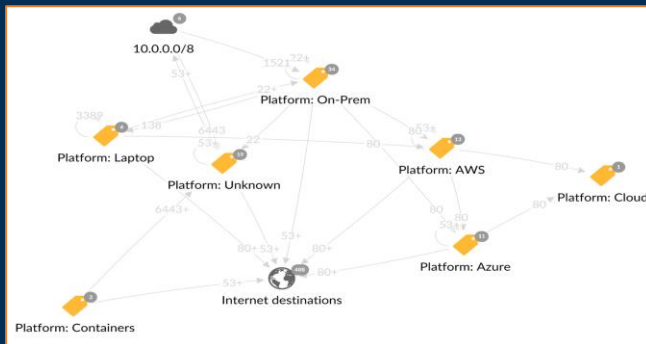
Detect lateral movement and real-time threats across the entire cyberattack kill chain with a single platform.

## Secure IT Assets

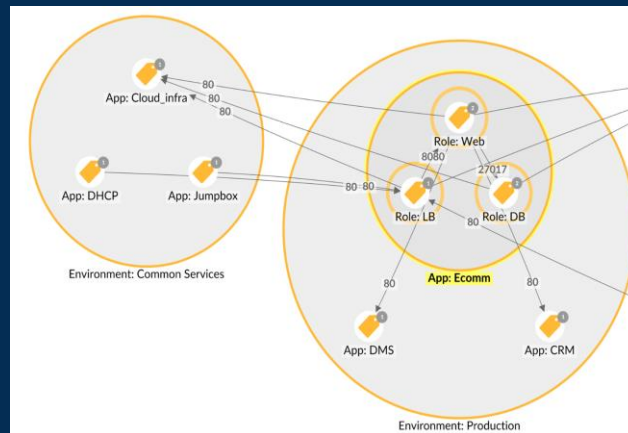
Protect critical assets from ransomware by easily enforcing Zero Trust principles across hybrid cloud ecosystems.

## Akamai Approach to Micro-Segmentation

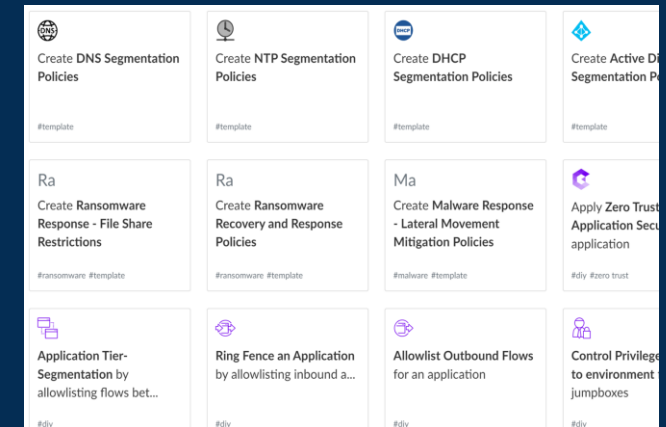
### Visualization



### Mapping

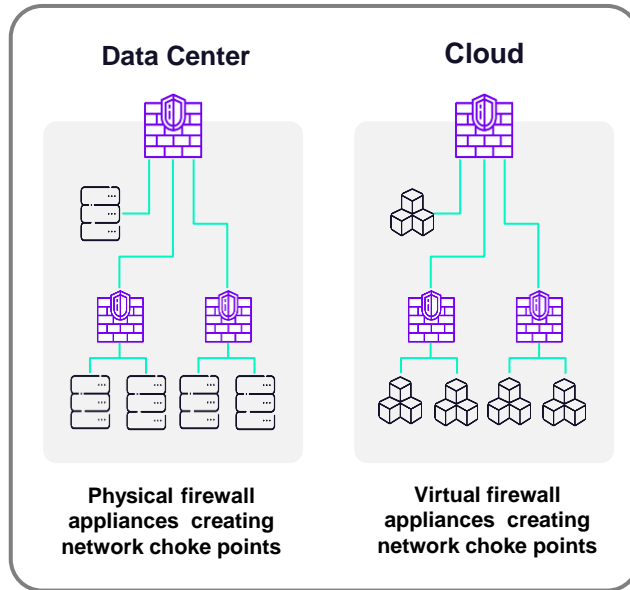


### Policy

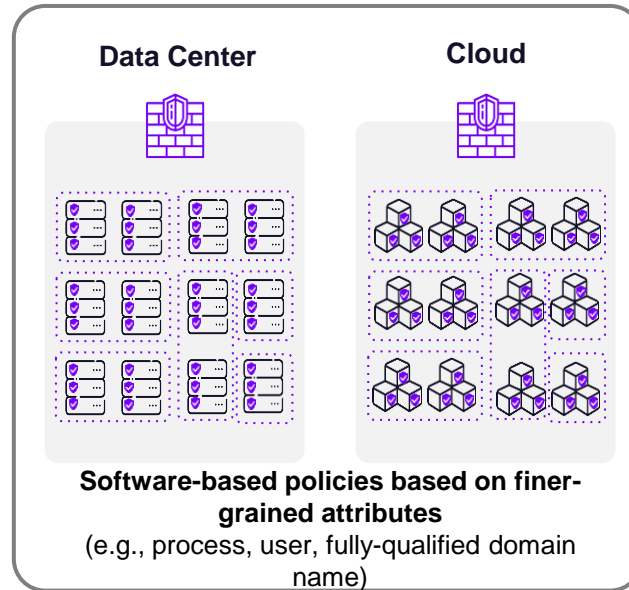


# Micro segmentation

## The Old Way



## The New Way



**Faster  
Lower Risk  
Lower Costs**

Minimize hardware refresh cycles and overhead


- Tied to environment and network
- Different approaches for different environments / technologies
- Slow and difficult to change
- Network-centric policies


- Software-only approach
- One set of security policies that work everywhere
- Easy to visualize and change
- Workload-centric policies


# Threat and Vulnerability Management

Allow us to Battle-Test your security by assessing how well your security program performs under pressure with active attacks against critical assets.

 Remediate Risk Smarter

 Advanced tools and techniques

 Experienced and certified team

 Human Context based Comprehensive Reporting



## Standards

Open Web Application Security Project (OWASP)

Penetration Testing Execution Standard (PTES)

NIST SP 800-115

The Open Source Security Testing Methodology Manual (OSSTMM)



# Security Operation Center

We assist you in designing a security management platform that meets the needs and priorities of your organization.



**On-Prem  
SOC**



**Hybrid  
SOC**



**Managed  
SOC**



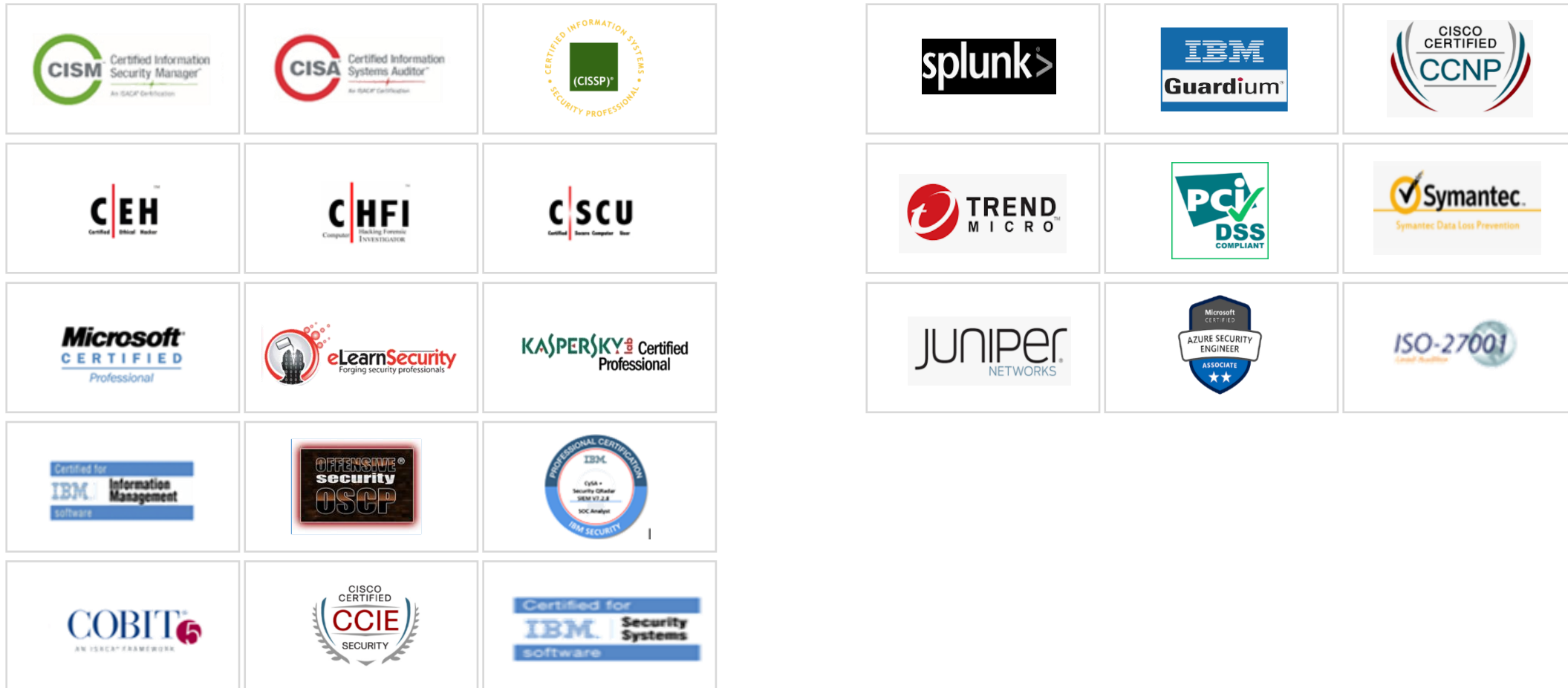


# Managed SOC(Security Operation Center)



# Security Technology expertise

## Infosec --Individual Technology and vendor Certifications



# Our Global Security Clienteles

 <b>Bank Alfalah</b>	<p>DOONEY &amp; BOURKE</p>	 <b>Fatima Group</b>	<p>VINCE.</p>	 <b>MIB</b> <small>MCB Islamic Bank Ltd</small>
 <b>IGI</b>	<p>ERICSSON </p>	 <b>Getz</b> <small>pharma</small>	 Wolters Kluwer	<p>TALBOTS</p>
<p>HBL <small>HABIB BANK</small>  <small>حبيب بینک</small></p>	 <b>Sciensus</b> <small>The new name for Healthcare at Home</small>	 <b>ALLOCATE</b>	 telenor	 <b>Pak Oman</b> <small>Microfinance Bank Limited</small> <small>بانك عمان مائیکرو فنانس بینک لمیٹڈ</small>
<p>Jubilee  <small>INSURANCE</small></p>	 <b>Meezan Bank</b> <small>The Premier Islamic Bank</small>	 <b>khushhali</b> <small>MICROFINANCE BANK</small>	<p>faysabank </p>	



---

# Global Customer Case Studies



Deployment of OpenShift Container Platform, Cloud Pak for Security (CP4S), Resilient and Major QRadar Upgrade

**CASE STUDY**

**Problem Statement**

Meezan Bank needed a solution that could transform their SOC in Next Gen SOC with the help of automation and orchestration for efficient incident analysis and resolution, as well as a single unified interface for incident investigation and search capabilities across the integrated assets and environment. Along with they want to upgrade their SIEM solution to gain complete Infrastructure visibility in terms of Security Incidents.

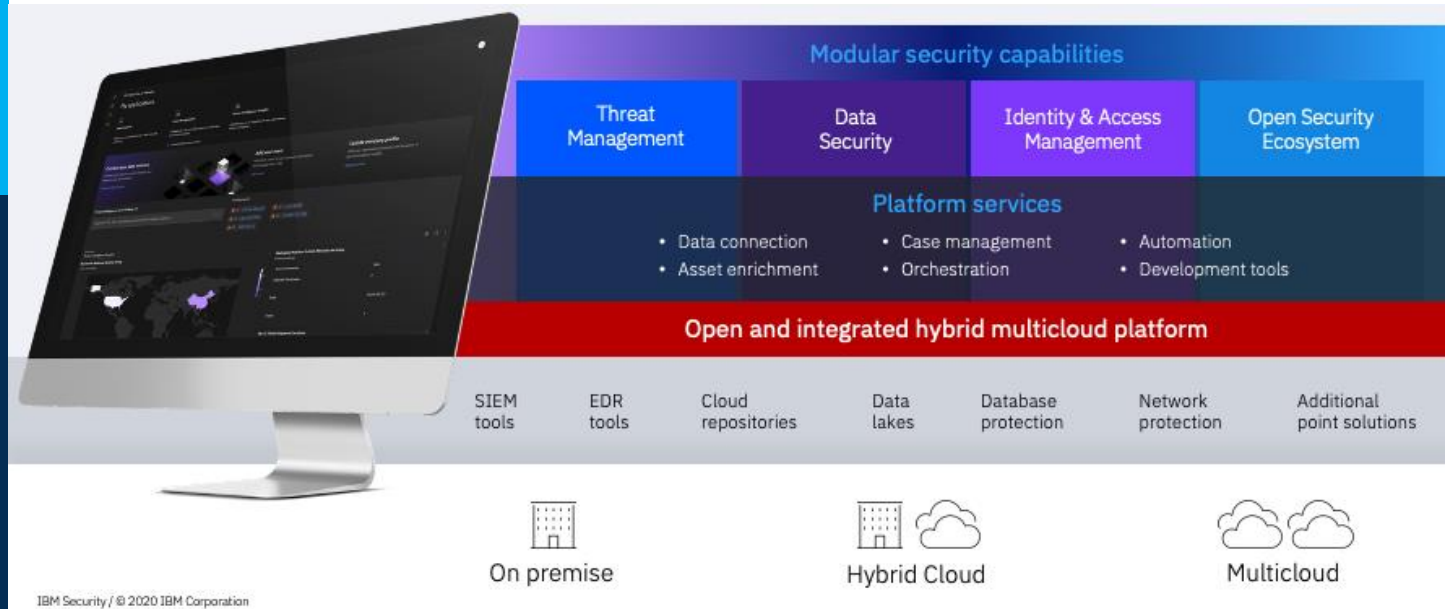
**Proposed Solution**

To meet the needs of customer, Systems Limited suggested IBM Cloud Pak for Security, which includes federated searches, SOAR, and threat intelligence

IBM Cloud Pak for Security is a platform that integrates your existing security tools to offer deeper insights into threats across overall infrastructure, using an infrastructure-independent common operating environment that runs anywhere.

**How Systems team help Bank in order to achieve the desired Goal**

1. Systems Limited team have deployed an underline **data lake** using **RedHat OpenShift container platform** for enablement of microservices infrastructure.
2. On top of **OpenShift Container platform**, our team have deployed IBM Cloud Pak for Security Platform and enable following services in the platform
  1. **Data Federated Search** – with the help of this feature, now analyst can search the data from any connected source while keeping the data at rest. MBL SOC team can add any artifact from the federated search to either new case or existing case on which SOC team is investigating.
  2. **Case Management** – investigate incidents, or cases, faster due to federated search capabilities, which enables searching across multiple data sources while keeping the data at rest. With Automation capabilities, we have reduced their investigation and root cause analysis activities so that their Analyst can focus on incident investigation.
  3. With the threat intelligence platform, MBL SOC team was able to identify the potential impact of any IOC within their environment and in case of any indicator found, their team is able to further investigate using the federated search option and can add the details as an artifact in either existing case or create new case.
3. Automation and Orchestration
  1. Systems Limited team have deployed multiple playbooks with respect to NIST and SANS standards in accordance with banking use cases.



IBM Security / © 2020 IBM Corporation

**Integrations and Customization:**

Systems Limited team have successfully integrated following technologies

1. Integrated QRadar SIEM, IBM Guardium as data source and QRadar Proxy for UBA. Configure STIX bundle to run STIX federated query across multiple data sources.
2. Configure automatic escalation of offenses to case management and automatic closure of offence upon incident closure.
3. Created the SOAR playbooks, workflows, incident task, functions etc. in CP4S case management.
4. We have involved our python developer for parsing the email send to monitored mailbox by case management for Phishing playbook in order to extract the required artifacts.

**Result/Outcome**

1. We have successfully able to deploy, implement, configure and integrate RedHat OpenShift Container Platform, Cloud Pak for Security, Federated Searches, Case management, Resilient and performed major QRadar upgrade.
2. We have successfully able to deploy, implement and integrate the solution with customer environment.
3. We have successful to gain the customer confidence on the product and services.

**Managed Security Services**

**Problem Statement**

Customer suffered some attacks in 2021. They have a limited team to cater all security related things like GRC function, security technology area and services area. Due to non-availability of Security Tools and Security Team, Customer IT had no security visibility over their infrastructure.

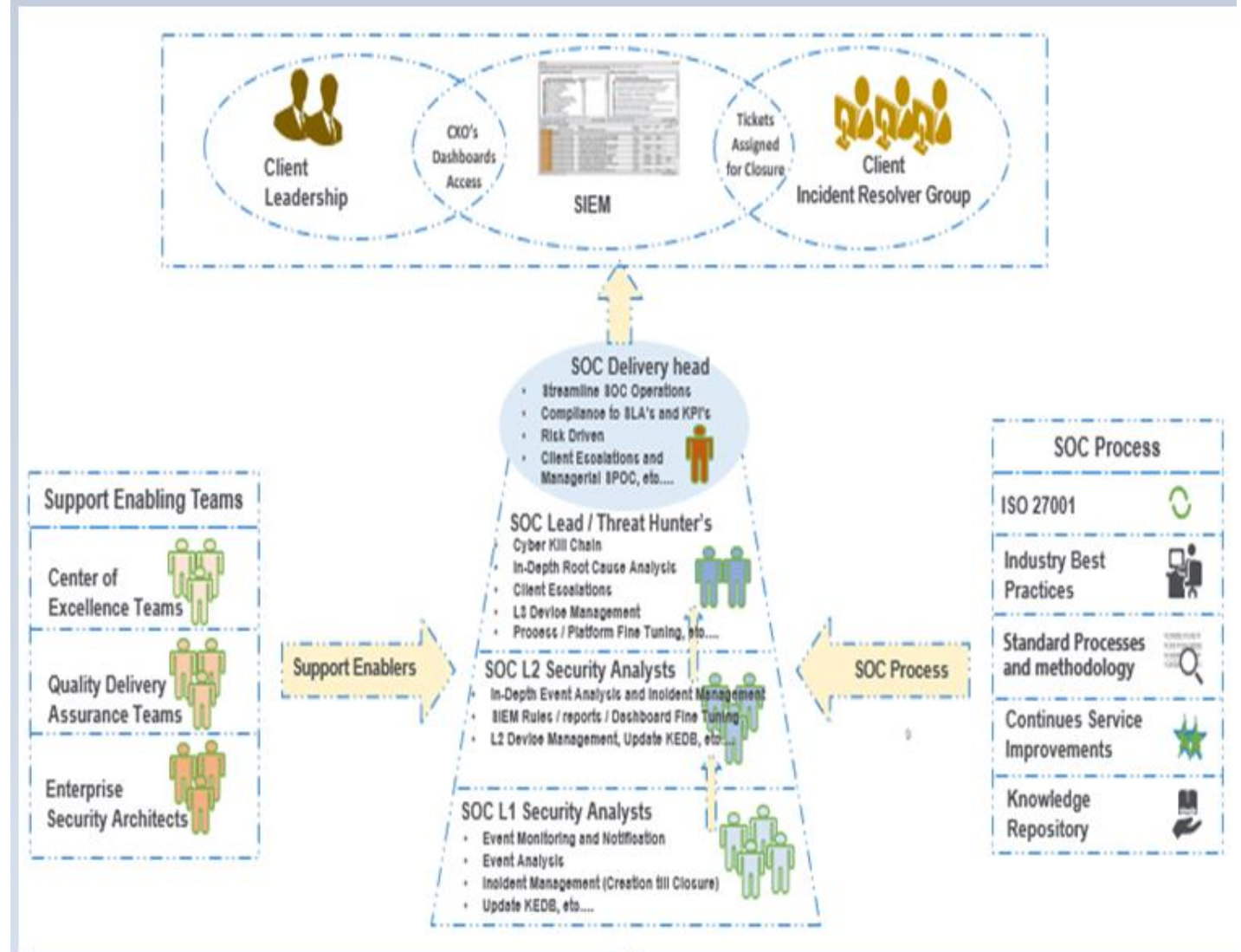
For this reason Customer decided to opt for TVS Managed Security Services including Enterprise GRC, Vulnerability Management, 24/7 SOC Monitoring and Incident Response/ Digital Forensics Services.

**TVS Solution**

When SL was onboarded for the Managed Security Services, SL prioritized to start with GAP Assessment. For this reason, our Enterprise GRC team conducted GAP assessment based on regulatory requirements and ISO controls. Internal & External vulnerability testing of Customer Hybrid (on-premise & on-cloud) environment was conducted. Once we have complete assessment report from GRC & VA teams, we have devised comprehensive plan to for next 3 years to fix GAPS. To start with, start providing its Next GEN SOC services based on cutting edge technologies.

Once we have the complete environment visibility, team deployed Azure Sentinel (SIEM) on Customer's Azure Environment. Specialized use cases and alerts were created relevant to Customer Infrastructure. Critical Network Devices and hosts were integrated with Azure Sentinel to ingest logs for Security Monitoring.

TVS SOC Team now manages Customer's SIEM alongside providing 24/7 Security Monitoring and advance Incident Response Services to Customer.



**Deployment of Open architecture Platform, based on Azure Sentinel**

**Problem Statement**

Customer suffered a Ransomware attack. Due to non-availability of Security Tools and Security Team, Customer IT had no security visibility over their infrastructure.

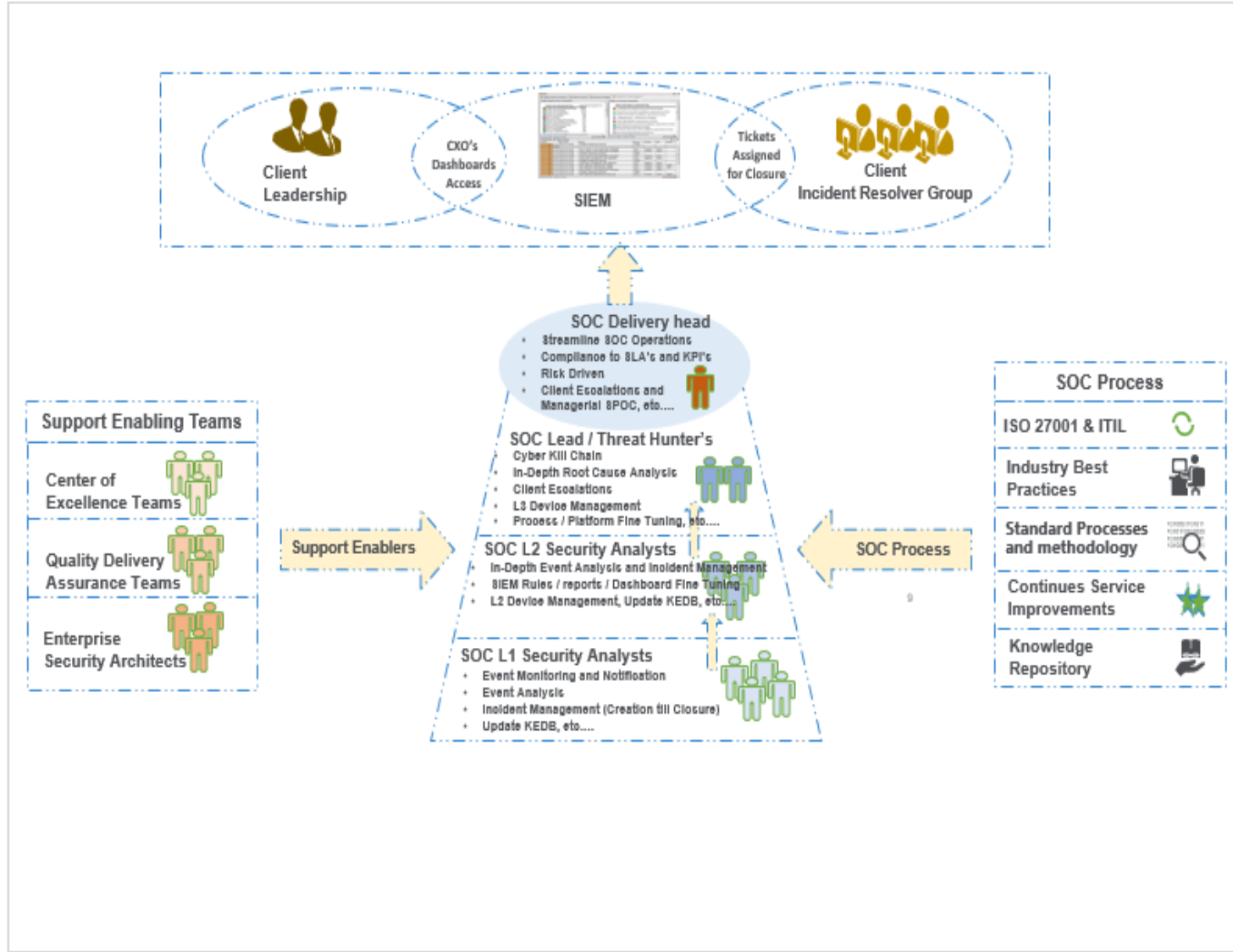
For this reason Customer decided to opt for Managed Security Services including Vulnerability Management, 24/7 SOC Monitoring and Incident Response/ Digital Forensics Services.

**SL Solution**

When Techvista was onboarded for the Managed Security Services, SL prioritized on securing the infrastructure. For this reason, Internal & External Penetration Testing of complete Customer Hybrid (on-premise & on-cloud) environment was conducted. Once these vulnerabilities were fixed, SL Red-Team conducted DFIR activity to detect existing web shells/backdoors and RATs in the environment to ensure no existing attacker is present in infrastructure. Alongside Penetration Testing of Network Devices, Security Configuration Review was also conducted for core Network Devices to ensure fool-proof security.

Once the environment was secured inside out, TVS team deployed Azure Sentinel (SIEM) on Customer's Azure Environment. Specialized use cases and alerts were created relevant to Customer Infrastructure. Critical Network Devices and hosts were integrated with Azure Sentinel to ingest logs for Security Monitoring.

TVS SOC Team now manages Customer's SIEM alongside providing 24/7 Security Monitoring and Incident Response Services to Customer.



**Managed Security Services based on Sentinel SIEM**

**Problem Statement**

Customer suffered 3 targeted Ransomware attacks in Q4 2020. Despite having one of the leading Endpoint Protection solution, they were unable to prevent those attacks from encrypting their data. Customer had no visibility over their Shadow IT.

SL was engaged for DFIR during the third ransomware attack.

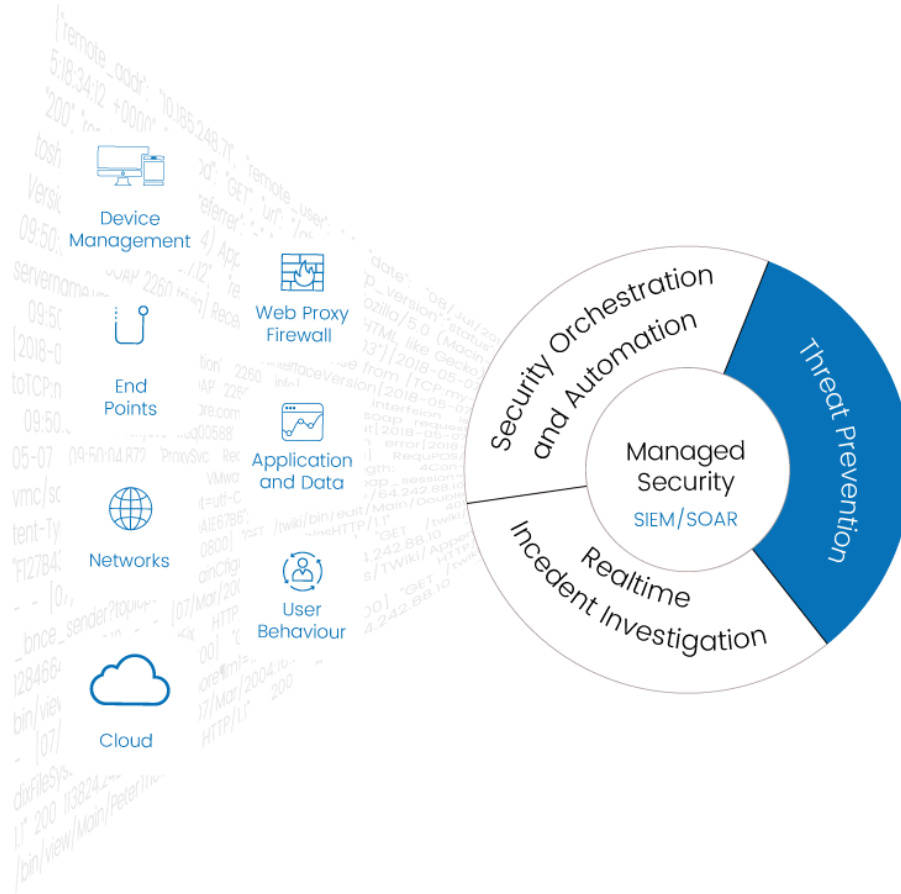
**SL Solution**

During the DFIR, TVS observed that there was no Penetration Testing ever performed on Customer's Infrastructure. Also, it was discovered that there was no centralized platform for Log Management. The Security events generated were not viewed by anyone due to lack of skilled IT Staff.

The forensics findings reveled an unpatched IIS vulnerability which was being exploited by the attacker. The forensics team also found attacker's persistent backdoor on one of the domain controllers.

TVS first performed Internal & External Penetration Testing followed by Compromise Assessment. A CIS Benchmarking was also performed to set a hardening baseline for Servers. Once the Infrastructure was hardened, TVS then deployed Azure Sentinel SIEM and initiated 24x7 SOC monitoring of customer's Infrastructure.

TVS SOC Team now manages Customer's SIEM alongside providing 24/7 Security Monitoring and Incident Response Services to Customer.



**Incident Discovery**

- Advanced Detection Engines
- Automated Threat Intelligence
- Retrospective Analysis
- Event Correlation

**Vulnerability Management**

- Advanced Patching
- Vulnerability Assessment
- License Management
- Remote Tool



Deployment of OpenShift Container Platform, Cloud Pak for Security (CP4S), Resilient and Guardium Data Protection

**CASE STUDY**

**Problem Statement**

Khushali Bank needed a solution that could transform their SOC in Next Gen SOC with the help of automation and orchestration for efficient incident analysis and resolution, as well as a single unified interface for incident investigation and search capabilities across the integrated assets and environment. Along with they want to protect their database servers from any security incident by imposing the policy and implement monitoring controls.

**Proposed Solution**

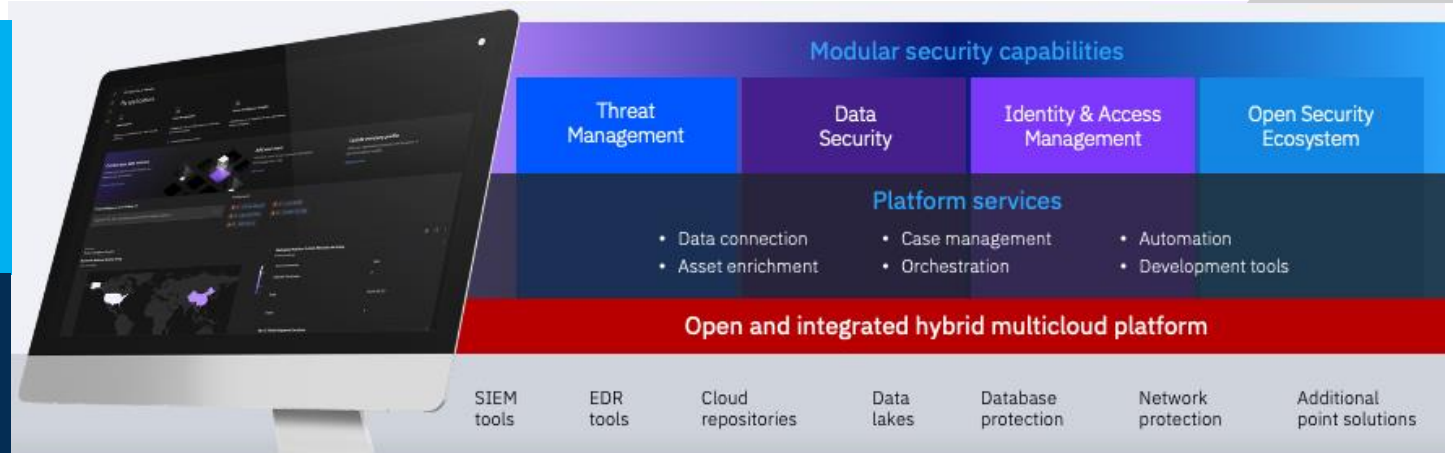
To meet the needs of customer, Systems Limited suggested IBM Cloud Pak for Security, which includes federated searches, SOAR, and threat intelligence along with IBM Guardium (data base security solution).

IBM Cloud Pak for Security is a platform that integrates your existing security tools to offer deeper insights into threats across overall infrastructure, using an infrastructure-independent common operating environment that runs anywhere.

**IBM Guardium provides the simplest, cost effective in terms of resources, most robust solution for assuring the privacy and integrity of trusted information resides in databases, data warehouses, and reducing costs by automating the entire compliance auditing process in heterogeneous environments.**

**How Systems team help Meezan Bank in order to achieve the desired Goal**

1. Systems Limited team have deployed an underline **data lake** using **RedHat OpenShift container platform** for enablement of microservices infrastructure.
2. On top of **OpenShift Container platform**, our team have deployed IBM Cloud Pak for Security Platform and enable following services in the platform
  1. **Data Federated Search** – with the help of this feature, now analyst can search the data from any connected source while keeping the data at rest. MBL SOC team can add any artifact from the federated search to either new case or existing case on which SOC team is investigating.
  2. **Case Management** – investigate incidents, or cases, faster due to federated search capabilities, which enables searching across multiple data sources while keeping the data at rest. With Automation capabilities, we have reduced their investigation and root cause analysis activities so that their Analyst can focus on incident investigation.
  3. With the threat intelligence platform, MBL SOC team was able to identify the potential impact of any IOC within their environment and in case of any indicator



found, their team can further investigate using the federated search option and can add the details as an artifact in either existing case or create new case.

4. Automation and Orchestration - Systems Limited team have deployed multiple playbooks with respect to NIST and SANS standards in accordance with banking use cases.
5. Deployed IBM Guardium a database monitoring & protection solution and integrate it with Oracle Hexa Data, MySQL, MSSQL database server. We have implemented successful policy covering, SQL statement auditing, protection and redaction services.

**Integrations and Customization:**

Systems Limited team have successfully integrated following technologies

1. Integrated QRadar SIEM, IBM Guardium as data source, TrendMicro Vision One and QRadar Proxy for UBA. Configure STIX bundle to run STIX federated query across multiple data sources.
2. Configure automatic escalation of offenses to case management and automatic closure of offence upon incident closure.
3. Created the SOAR playbooks, workflows, incident task, functions etc. in CP4S case management.
4. We have involved our python developer for parsing the email send to monitored mailbox by case management for Phishing playbook in order to extract the required artifacts.

**Result/Outcome**

1. We have successfully able to deploy, implement, configure and integrate RedHat OpenShift Container Platform, Cloud Pak for Security, Federated Searches, Case management, Resilient and performed major QRadar upgrade.
2. We have successfully able to deploy, implement and integrate the solution with customer environment.
3. We have successful to gain the customer confidence on the product and services.

SIEM Disaster Recovery

**CASE STUDY**

**Problem Statement**

HB Bank needed a solution that would allow them to enable a DR site for their existing SIEM solution as well as upgrade the primary site software and hardware by enabling the high availability option to build resiliency into the system.

**Proposed Solution**

To meet the needs of customer, Systems Limited suggested required server hardware and software i.e., IBM QRadar SIEM disaster recovery site deployment and implementation.

Disaster Recovery (DR) is a key aspect to the resiliency of a QRadar deployment. At a high-level, the solution is intended to utilize an enhanced Backup/Recovery API to transfer configuration data from a Main Site to the DR Site, as well as an advanced efficient Ariel Copy mechanism to frequently move event and flow data stored in the Ariel database from any Event Processor in production to a comparable Event Processor in the DR deployment.

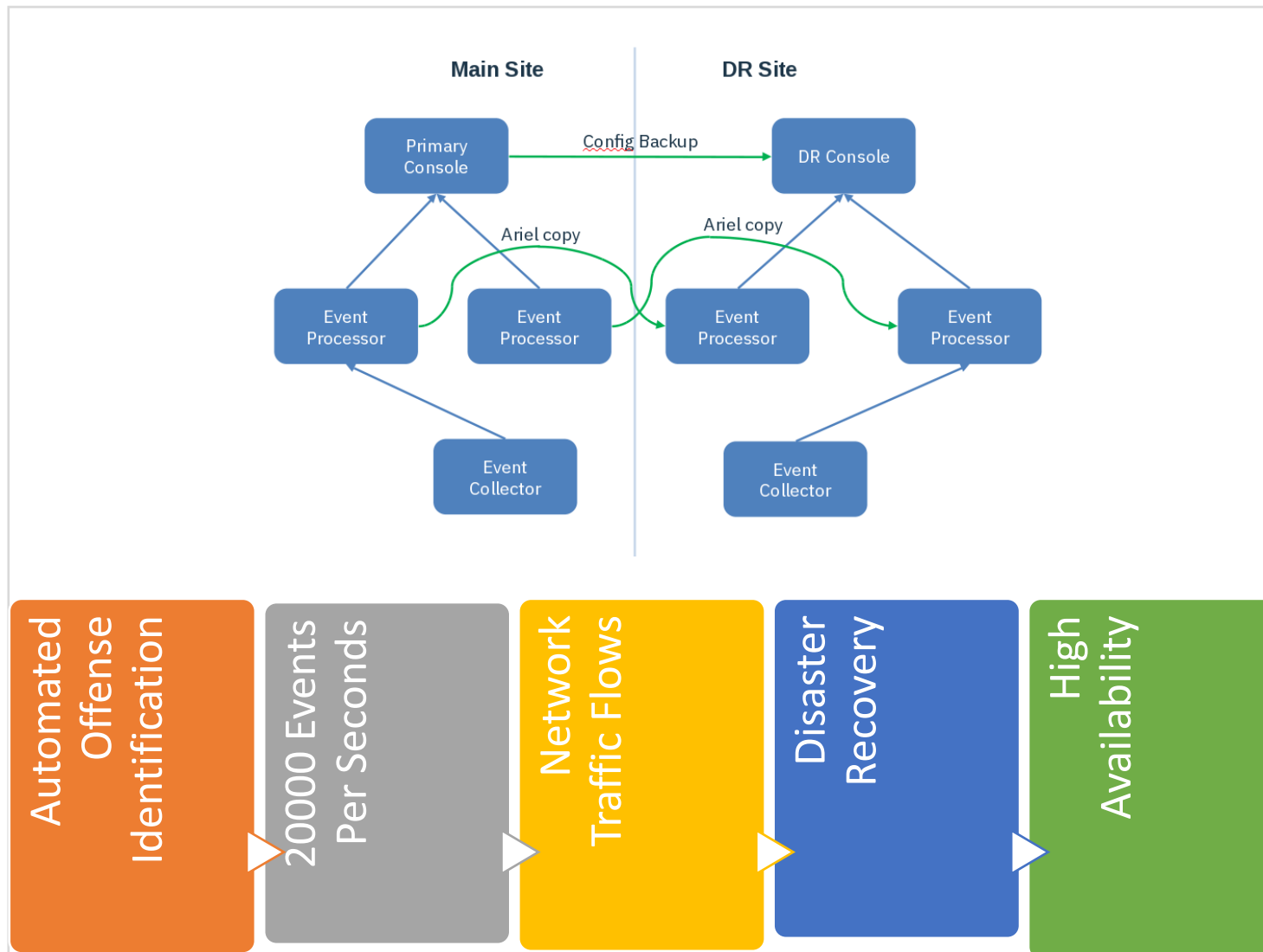
Our team is currently deploying the IBM QRadar systems in parallel to existing QRadar environment by upgrading the hardware and software at both the sites.

Our team is deploying high availability environment in distributed architecture at primary site. In case of any outage on the primary node, secondary node will automatically take over the responsibility.

Data synchronization will be configured between primary and disaster recovery site so that in case of any failure to the primary site, services can be restored from the disaster recovery site.

**Result/Outcome:**

1. Systems Limited team is expecting to complete this deployment without any issues



## Penetration Testing

CASE STUDY

## Problem Statement

Global Telco Vendor and our partner deployed MFS Wallet Platform at TMCEL Mozambique. Our partner wanted Third Party Penetration Testing done for the Wallet Platform. TVS was engaged by Ericsson for the Penetration Test.

## SL Solution

The scope covered Infrastructure, Mobile Applications(iOS & Android) and Web Application Portals. The Infrastructure assessment was Whitebox as it included containerized environment while Infrastructure & Mobile Applications were Blackbox.

The environment was a network segregated environment with very limited access available to Systems Limited's Security engineers. Systems Limited Security Engineers used Network Pivoting techniques to access the in-scope assets. The testing was performed within specified time and critical vulnerabilities were discovered that could have breached the Confidentiality, Integrity and Availability of the platform.

### 1. Pre-engagement



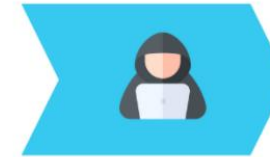
Defining security objectives, & outcomes

### 2. Scope defining



Recognizing assets that would undergo the test

### 3. Exploitation



Simulating attacks on the system

### 4. Reporting & Remediation



Documenting the findings and working on fixing

### 5. Re-Scan & Certification



Testing the fixes and issuing pentest certificate

Managed Vulnerability Management

**Problem Statement**

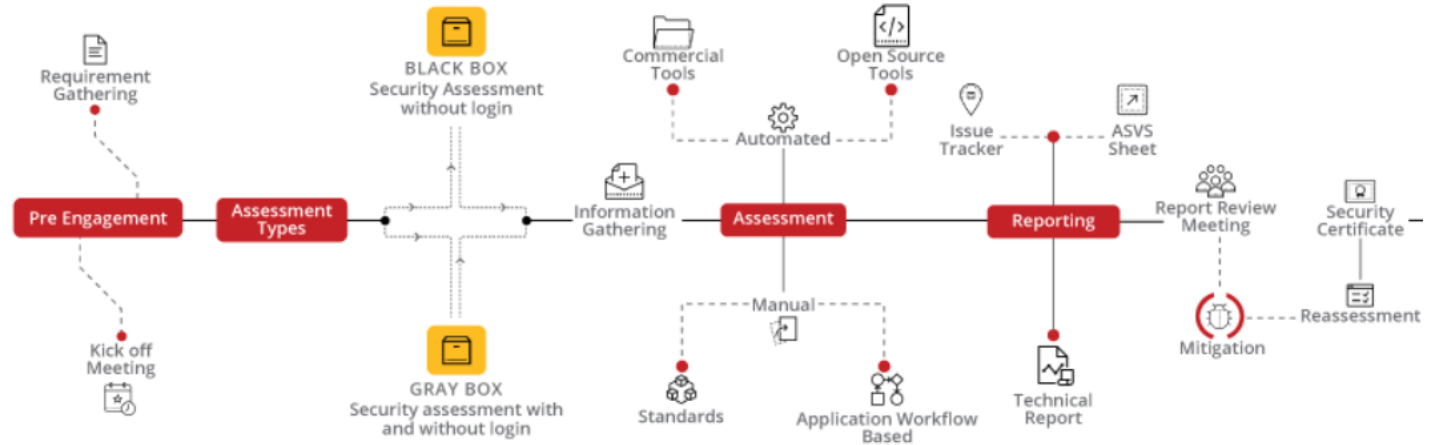
Customer didn't had an Application Security Framework in place. No Active Application Security Testing was being performed on Applications being developed in-house. As a result, Applications were being exploited resulting in loss in terms of financial and reputation.

TVS was engaged as Managed Vulnerability Management Partner.

**SL Solution**

During the initial phase of the engagement, Visionet analyzed the applications and prioritized their scanning based on their criticality, builds roll-out frequency and other aspects. Once the scope was locked, Visionet team ad Customer mutually agreed scan frequency of each application.

Visionet Security Engineers now perform Application Security Testing, Mobile Application Security Testing and Cloud Security Assessment of each application before new build is roll-out.





**elogics**  
Systems

The technology solutions architects

systems

*Please contact us:*



23 Floor, Dar-Al-Awadhi Towers, Sharq

Kuwait City – Kuwait.

Phone: +965 2232 2190

Mobile+WhatsApp: +965 9406-1666 – 9969-6335 - 6566 6607

Email: [sales@elogicssystems.com](mailto:sales@elogicssystems.com)

Website: <https://elogicssystems.com/>

*Thank  
you*

