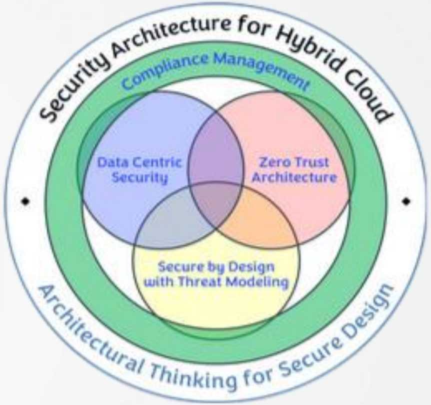
Architectural Thinking for Security

Crested Eagle Finance

Team: 04

Team Members: 05


Security Architecture for Hybrid Cloud
Compliance Management
Data Centric Security
Zero Trust Architecture
Secure by Design with Threat Modeling
Architectural Thinking for Secure Design

Team: 04

Team Members:

- Marc Reinl
- Marciej Duda
- Mukesh Kumar
- Pramod Kumar
- Yash Rajendra Hajare

Table of Contents

Overall Business and IT Context

System Context

Requirements and Constraints

Application Security

Infrastructure Security

Architecture Patterns and Decisions

Security Development and Assurance

Closing Remarks

Business Overview

Business Goals

To develop and implement a secure, integrated **Customer Relationship Management (CRM)** system for **Crested Eagle Finance's** sales partners using the **OneRelationship SaaS** application to track financial history and ensure compliance with regulatory requirements (including PCI-DSS and anti-money laundering regulations), protects client data, and improves operational efficiency by leveraging a scalable hybrid cloud architecture and advanced technologies.

Team Objective

Our team's objective is to integrate the Managed Security Services Provider (MSSP) into Crested Eagle Finance's hybrid cloud infrastructure effectively and securely. This integration involves coordinating with the MSSP, which operates in a different cloud environment, to implement comprehensive threat management detection and response services across our new application and associated systems.

Crested Eagle Finance

IT Context Overview

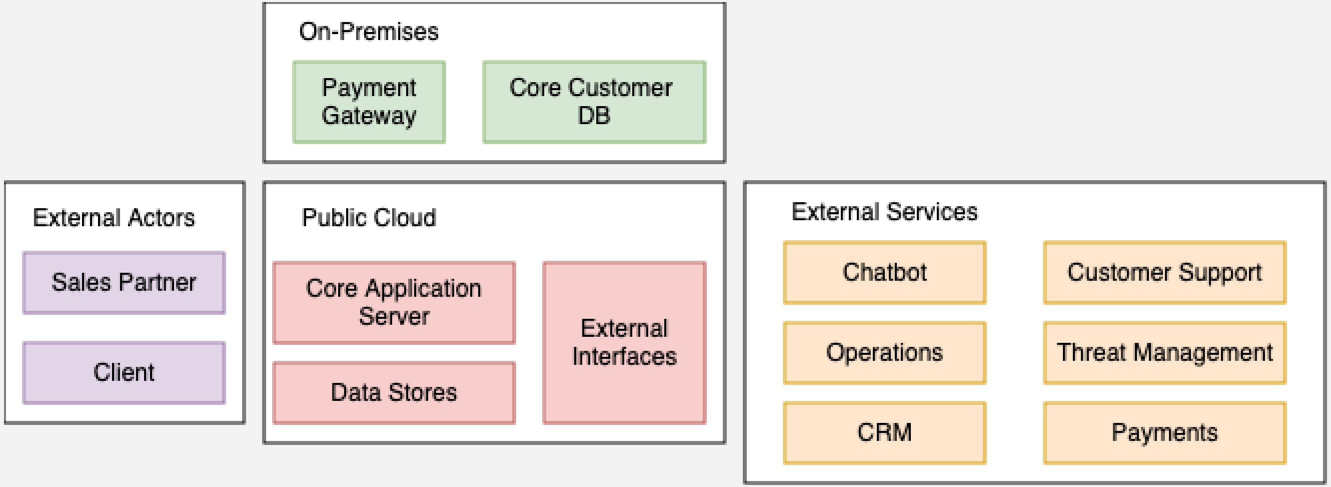
Marc Reinl

Challenges: ***Security & Compliance***

- Sparely documented security architecture.
- Concerns over PCI-DSS compliance and cyber resilience.
- The UK financial services regulator is reviewing the project with a focus on client data protection.
- **Crested Eagle Finance does not have any in-house threat detection team, and needs one**

IT Architecture: ***Hybrid Cloud***

- On-Premises.
- External Actors.
- Public Cloud.
- External Services



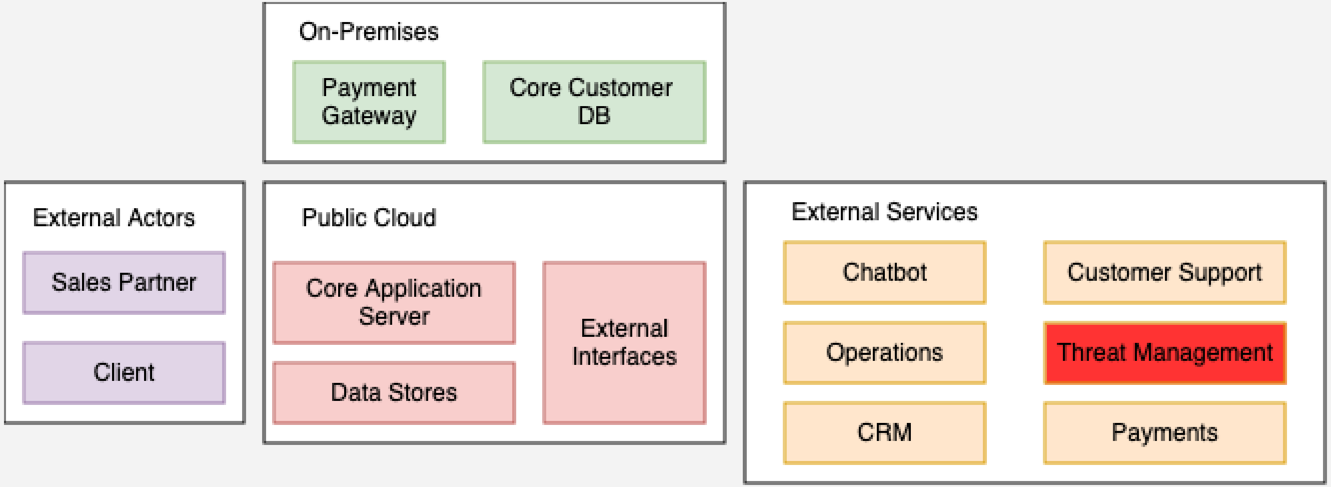
IT Context Overview

Challenges: ***Security & Compliance***

- Sparely documented security architecture.
- Concerns over PCI-DSS compliance and cyber resilience.
- The UK financial services regulator is reviewing the project with a focus on client data protection.
- **Crested Eagle Finance does not have any in-house threat detection team, and needs one**

IT Architecture: ***Hybrid Cloud***

- On-Premises.
- External Actors.
- Public Cloud.
- External Services



On-Premises

Payment Gateway

Core Customer DB

External Actors

Sales Partner

Client

Public Cloud

Core Application Server

Data Stores

External Interfaces

External Services

Chatbot

Customer Support

Operations

Threat Management

CRM

Payments

Table of Contents

Overall Business and IT Context

System Context

Requirements and Constraints

Application Security

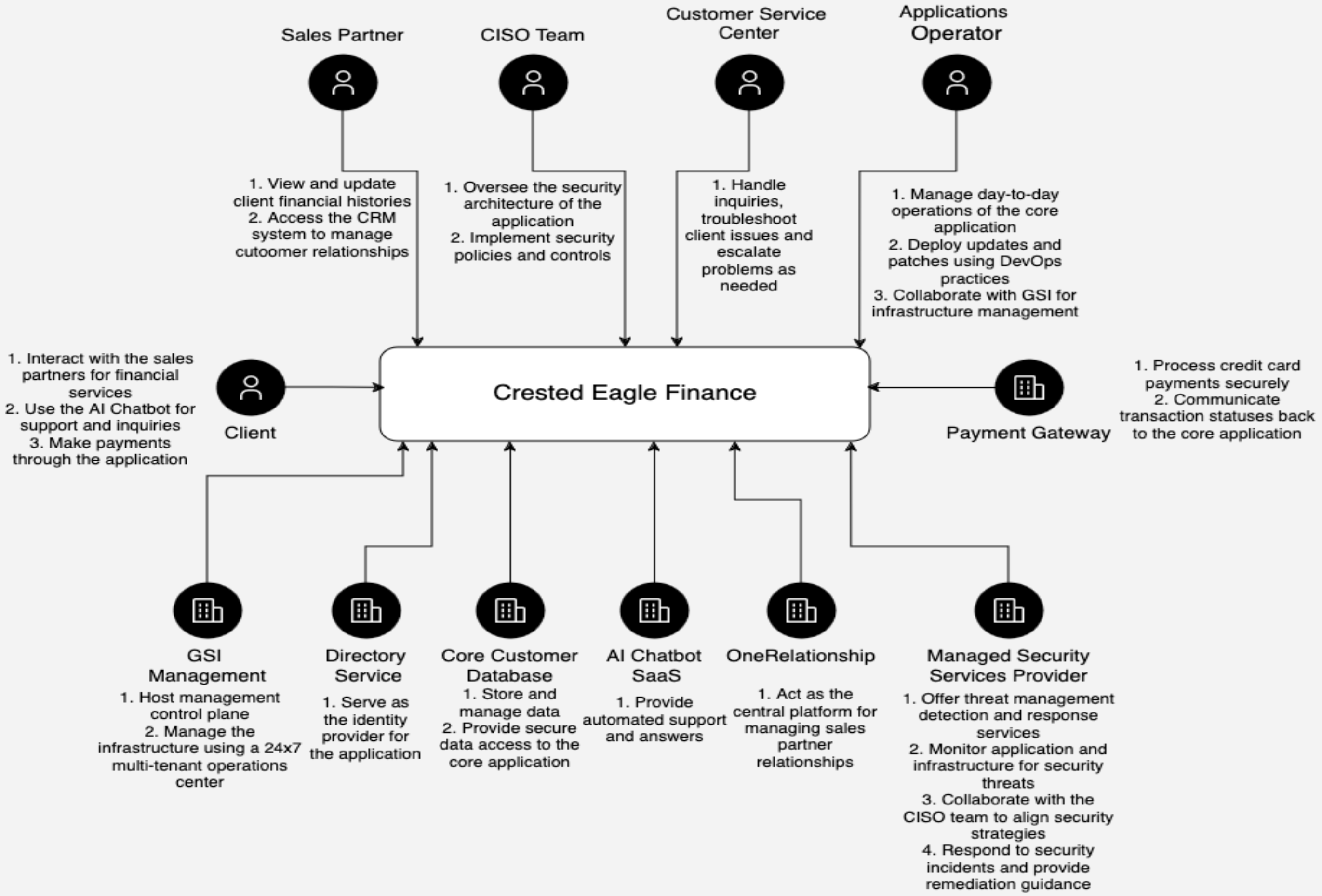
Infrastructure Security

Architecture Patterns and Decisions

Security Development and Assurance

Closing Remarks

System Context Diagram



Sales Partner

1. View and update client financial histories
2. Access the CRM system to manage cutoomer relationships

CISO Team

1. Oversee the security architecture of the application
2. Implement security policies and controls

Customer Service Center

1. Handle inquiries, troubleshoot client issues and escalate problems as needed

Applications Operator

1. Manage day-to-day operations of the core application
2. Deploy updates and patches using DevOps practices
3. Collaborate with GSI for infrastructure management

Client

1. Interact with the sales partners for financial services
2. Use the AI Chatbot for support and inquiries
3. Make payments through the application

Crested Eagle Finance

Payment Gateway

1. Process credit card payments securely
2. Communicate transaction statuses back to the core application

GSI Management

1. Host management control plane
2. Manage the infrastructure using a 24x7 multi-tenant operations center

Directory Service

1. Serve as the identity provider for the application

Core Customer Database

1. Store and manage data
2. Provide secure data access to the core application

AI Chatbot SaaS

1. Provide automated support and answers

OneRelationship

1. Act as the central platform for managing sales partner relationships

Managed Security Services Provider

1. Offer threat management detection and response services
2. Monitor application and infrastructure for security threats
3. Collaborate with the CISO team to align security strategies
4. Respond to security incidents and provide remediation guidance

Actor/Use Case/Interface

Actors	Description	Interface
Customer Service Centre	Acting as the primary interface between the clients and the security service provider.	Web application accessible over a secure TLS 1.3 session Telephony Integration System (VoIP system)
Chief Information Security Officer (CISO)	Ensures that the MSSP management activities comply with regulatory requirements and industry standards	Compliance Management Interface-ServiceNow Governance, Risk, and Compliance (GRC) frameworks like Power BI with backend data sourced from Splunk
Applications Operator	Applications function smoothly, meet business needs, and are secure and updated	Backup and Disaster Recovery Management-Azure Backup Incident Management Interface -Zendesk, ServiceNow
Sales Partner	External organization that helps the company extend its market reach, increase sales, and grow its customer base	Integration with External Stakeholders- mutual TLS and OAuth 2.0 Sales and Commission Tracker- Xactly or custom solutions
Program Executive	Ensure that the various projects are aligned with the organization’s strategic goals and are delivered on time.	Collaboration and Communication Tools- Microsoft Teams, Zoom Program Management Dashboard (Microsoft Project)
Client	Individual or company that receives services or products from another business	Web application accessible over a secure TLS 1.3 session PCI DSS-compliant payment gateway
Payment Gateway	Secure and seamless transfer of payment information between a client and the financial institutions involved	RESTful API with support for OAuth 2.0 authentication and TLS 1.3 encryption. Customer Payment Portal like React or Flutter
Core Customer Database	Maintains accurate, up-to-date records of their customer base, transactional history, and marketing preferences.	data stored in MongoDB and Redis cloud-native databases Customer Data Security and Encryption-AES-256 encryption
Managed Security Service Provider (MSSP)	monitoring and management of security systems and devices to organizations	Incident and Event Management System- ServiceNow Security Information and Event Management- IBM QRadar
GSI Management	integrate and manage the client’s IT infrastructure and security systems	Integrated CRM (e.g., Salesforce), SharePoint, or custom vendor management tools
AI Chatbot SaaS	Customer service and support to sales and marketing	Chatbot and Live Chat Interface secured with TLS 1.3 Integration with messaging platforms like Freshchat for human support handover
One Relationship	Maintains the financial history for all business performed with their sales partners	Integration with External Stakeholders- mutual TLS and OAuth 2.0 Web application accessible over a secure TLS 1.3 session

Actor/Use Case/Data Mapping

Mukesh Kumar

Actors	Use Case	Data Type processed
Customer Service Centre	Assist and support customers before, during, and after they purchase a service	Contact details, Email, Payment details
Chief Information Security Officer (CISO)	Identify Roles, Look into different Strategy and Policies, Budget and Resource Allocation	Policy and Compliance Data, Risk Management Data, and Audit report
Applications Operator	Application Monitoring, Check Logs, Incident Management, Documentation and Reporting	Incident Response Data and Security Tools Data
Sales Partner	Promotion and Marketing by doing research, campaigns Tracking sales and execution	Customer Data, Sales Performance Data, and Marketing Campaign Data
Program Executive	Program Planning and Strategy Coordinate with various departments and stakeholders Program Execution Review	Resource Allocation Data, Communication Data, Project and Task Data, and Budget and Financial Data
Client	Register with the Crested Eagle Finance, Browser a product or service, confirm payment	Contact details, type of service and payment details
Payment Gateway	Initiate Payment Request and Redirect to Payment Gateway, Authorize Payment and Send Confirmation to Customer	Identification and Authentication info, and Payment details
Core Customer Database	Request Customer Information Store, Updates and Delete Profile	Login details, Service details, Contact info
Managed Security Service Provider(MSSP)	Real-Time Threat Monitoring Incident Response and Mitigation Compliance and Reporting	Log and Network Traffic Data, Cloud Activity Data, User Behavior Data
GSI Management	Incident Response and Remediation Regular System Maintenance and Optimization	Project and Task Management Data, Client Requirements and Specifications data, and Financial and Budget Data
AI Chatbot SaaS	Understanding Query and Providing Response	User Input Data, Natural Language Processing (NLP) Data, and User Behavior and Interaction Data
One Relationship	Customer Management, Sales Partner Collaboration and Reporting and Analytics	Customer Data, Sales Partner Data, Financial Data

Data Classification Scheme

Mukesh Kumar

Public	Information which is available to public and don’t have a bigger impact to the organization or the users. An instance of this can be seen with the Web UI which is available to the public which would serve as the access point.
Internal	The information which is made available only to the employees, it is not made available to the public nor on the public website. This can be seen as internal memos or information on the application development.
Confidential	This pertains to information that could potentially harm the organization if disclosed but does not violate any laws or regulations. This could include financial history of client transactions, client names and addresses.
Highly Confidential	This is information which can have a bigger impact on the organization and its users. This could include legal or regulatory consequences. We could consider artifacts such as the encryption and API Keys of the system to secure customer and payment data, as well as the API keys which are used to integrate services like the hybrid cloud architecture.

Asset Inventory

Data Type	Data Fields	Data Classification	Legal and Regulatory
Identification Information	Username	Internal	GDPR, PI
	Password	Highly Confidential	GDPR, PI
Contact Details	Name	Internal	GDPR, PI
	Address	Internal	GDPR, PI
	Phone Number	Internal	GDPR, PI
Customer Data	Financial History	Confidential	GDPR
	AML Check Results	Confidential	GDPR
	Linked Account Numbers	Confidential	GDPR
Payment Details	Card Number	Highly Confidential	PCI-DSS
	Expiry Date	Confidential	PCI-DSS
	Security Code	Highly Confidential	PCI-DSS
	Billing Address	Confidential	PCI-DSS, GDPR
Payment Transactions	Payment Log Events	Confidential	PCI-DSS
	Transaction Amounts	Confidential	PCI-DSS
Operational Data	Source Code (GitHub)	Internal	
	Deployment Scripts (GitHub)	Confidential	
	Project Management (Airtable)	Internal	
API Data	Partner IDs	Confidential	GDPR
	Session Tokens	Confidential	GDPR
	API Usage Logs	Confidential	GDPR
Threat Management Data	Security Alerts	Confidential	UK Financial Services Regulator
	Anomaly Reports	Confidential	UK Financial Services Regulator
Identity Data	MFA Credentials	Highly Confidential	GDPR
	User Roles	Confidential	GDPR

Table of Contents

Overall Business and IT Context

System Context

Requirements and Constraints

Application Security

Infrastructure Security

Architecture Patterns and Decisions

Security Development and Assurance

Closing Remarks

Overview of Functional Requirements – MoSCoW

NFR	Domain	Category	Prio	Requirement	Ext. Ref.	Solution	Service Owner
SEC	**Secure Data Transmission**	**SDT_001**	**MUST**	The system **MUST** securely transmit security logs, events and alerts from Crested Eagle Finance's infrastructure to the MMSP's infrastructure in real-time or near real-time using encrypted communication channels.	001	Implement a secured SIEM integration using TLS 1.3 encryption and dedicated VPN tunnels for log transmission, with real-time streaming capabilities.	Security Operations Lead
SEC	**Data Encryption**	**DA_002**	**MUST**	The system **MUST** encrypt all data sent and stored by the MSSP in transit and at rest utilizing industry-standard encryption algorithms	002	Deploy enterprise-grade encryption using AES-256 for data at rest and TLS 1.3 for data in transit, with centralized key management system.	Cloud Architect (GSI)
SEC	**Authentication and Authorisation**	**AA_003**	**MUST**	The system **MUST** implement robust authentication mechanisms to authenticate and authorize communication between Crested Eagle Finance's systems and the MSSP's systems	003	Implement OAuth 2.0 with SAML for SSO, coupled with multi-factor authentication and role-based access management.	Identity and Access Management Lead
SEC	**Access Control**	**AC_004**	**MUST**	The MSS provider **MUST** be granted least-privilege access to only the necessary data and systems required for threat detection and response, enforced through role-based access control (RBAC).	004	Deploy RBAC system with Just-In-Time access provisioning regular access reviews with an integrated PAM solution	Identity and Access Management Lead
SEC	**Compliance and Regulations**	**CR_005**	**MUST**	The integration **MUST** comply with all relevant data protection and privacy regulations, including GDPR and PCI-DSS, ensuring no sensitive customer data is unlawfully shared or processed	005	Implement automated compliance and monitoring tools with regular audits, data classification, and DLP solutions to ensure compliance.	Compliance Officer
SEC	**Real-time Incident Notification**	**RIN_006**	**MUST**	The MSS provider **MUST** be able to notify Crested Eagle Finance's security team in real-time upon detection of threats or incidents, using predefined communication channels and protocols.	006	Deploy SIEM with automated alert routing, integrated incident response playbooks, and multiple notification channels (emails, SMS, ticketing system)	Security Operations Lead

Overview of Functional Requirements – MoSCoW

NFR	Domain	Category	Prio	Requirement	Ext. Ref.	Solution	Service Owner
SEC	**Secure Data Transmission**	**SDT_001**	**MUST**	The system **MUST** securely transmit security logs, events and alerts from Crested Eagle Finance’s infrastructure to the MMSP’s infrastructure in real-time or near real-time using encrypted communication channels.	001	Implement a secured SIEM integration using TLS 1.3 encryption and dedicated VPN tunnels for log transmission, with real-time streaming capabilities.	Security Operations Lead
SEC	**Data Encryption**	**DA_002**	**MUST**	The system **MUST** encrypt all data sent and stored by the MSSP in transit and at rest utilizing industry-standard encryption algorithms	002	Deploy enterprise-grade encryption using AES-256 for data at rest and TLS 1.3 for data in transit, with centralized key management system.	Cloud Architect (GSI)
SEC	**Authentication and Authorisation**	**AA_003**	**MUST**	The system **MUST** implement robust authentication mechanisms to authenticate and authorize communication between Crested Eagle Finance’s systems and the MSSP’s systems	003	Implement OAuth 2.0 with SAML for SSO, coupled with multi-factor authentication and role-based access management.	Identity and Access Management Lead
SEC	**Access Control**	**AC_004**	**MUST**	The MSS provider **MUST** be granted least-privilege access to only the necessary data and systems required for threat detection and response, enforced through role-based access control (RBAC).	004	Deploy RBAC system with Just-In-Time access provisioning regular access reviews with an integrated PAM solution	Identity and Access Management Lead
SEC	**Compliance and Regulations**	**CR_005**	**MUST**	The integration **MUST** comply with all relevant data protection and privacy regulations, including GDPR and PCI-DSS, ensuring no sensitive customer data is unlawfully shared or processed	005	Implement automated compliance and monitoring tools with regular audits, data classification, and DLP solutions to ensure compliance.	Compliance Officer
SEC	**Real-time Incident Notification**	**RIN_006**	**MUST**	The MSS provider **MUST** be able to notify Crested Eagle Finance’s security team in real-time upon detection of threats or incidents, using predefined communication channels and protocols.	006	Deploy SIEM with automated alert routing, integrated incident response playbooks, and multiple notification channels (emails, SMS, ticketing system)	Security Operations Lead

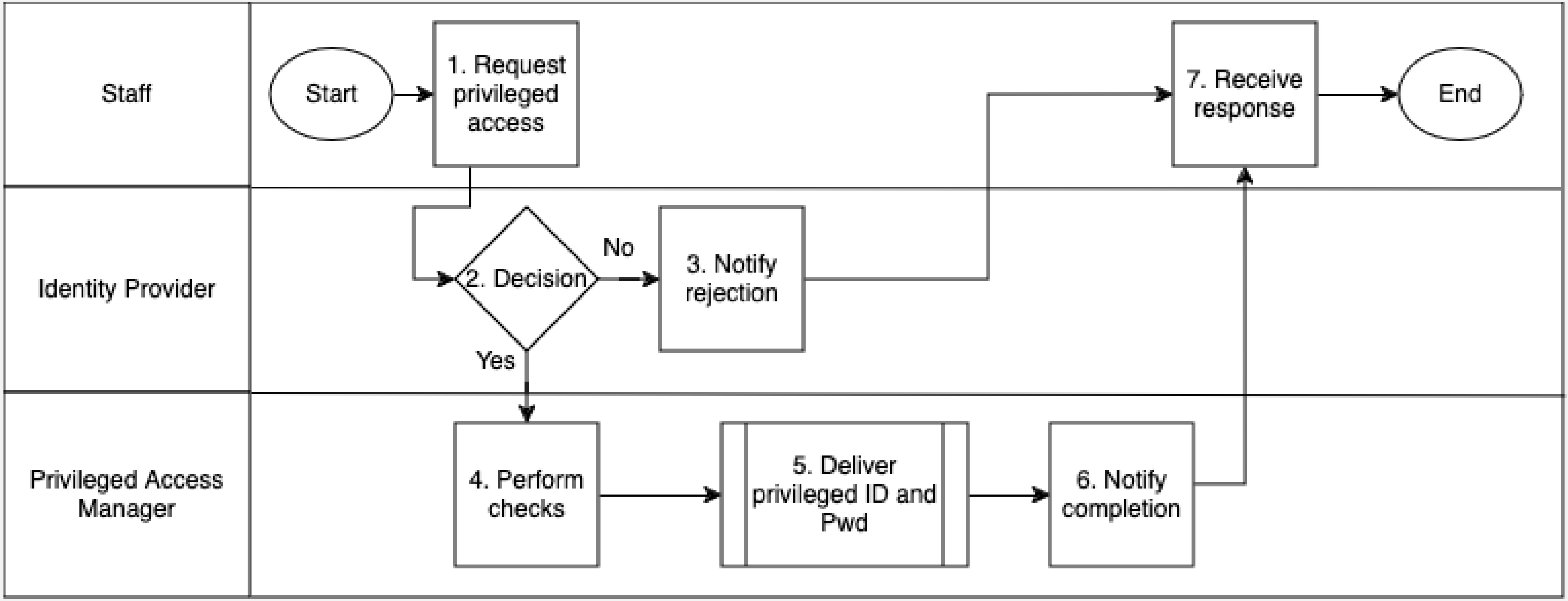
Overview of Non-functional Requirements - MoSCoW

NFR	Domain	Category	Prio	Requirement	Ext. Ref.	Solution	Service Owner
SEC	Scalability	SC_001	MUST	The system **MUST** support both horizontal and vertical scaling for increasing data volumes and applications.	001	Design architecture with auto-scaling features in cloud environments and ensure seamless addition of resources when thresholds are reached.	Cloud Service Provider
SEC	Maintainability	UPD_002	MUST	The system **MUST** have the ability to upgrade components with minimal disruption to services.	002	Plan upgrades during low-usage windows, leverage canary deployments for minimal downtime.	Global Systems Integrator
SEC	Latency	LAT_003	SHOULD	Network communication with the MSS provider **SHOULD** maintain acceptable latency (<100ms round-trip) to support real-time operations.	003	Optimise network routes and ensure high-speed interconnectivity with MSS providers for real-time operations.	Network Operations
SEC	Cost Efficiency	BGT_004	MUST	The Project **MUST** meet allocated budgets for implementation and ongoing operations.	004	Plan a cost-optimized infrastructure using reserved instances, discounts, and cost tracking tools.	Finance Manager
SEC	Training	KB_005	COULD	Eagle Finance **COULD** Maintain an up-to-date repository of knowledge articles and FAQs.	005	Host knowledge base with search capabilities, ensuring all documentation is easily accessible and periodically reviewed.	Knowledge Management Specialist
SEC	Adaptability	POL_006	WOULD	The system **WOULD** have the ability to quickly implement new security policies or compliance requirements.	006	Centralise policy management with tools like a security policy engine and automate compliance checks.	Compliance Officer

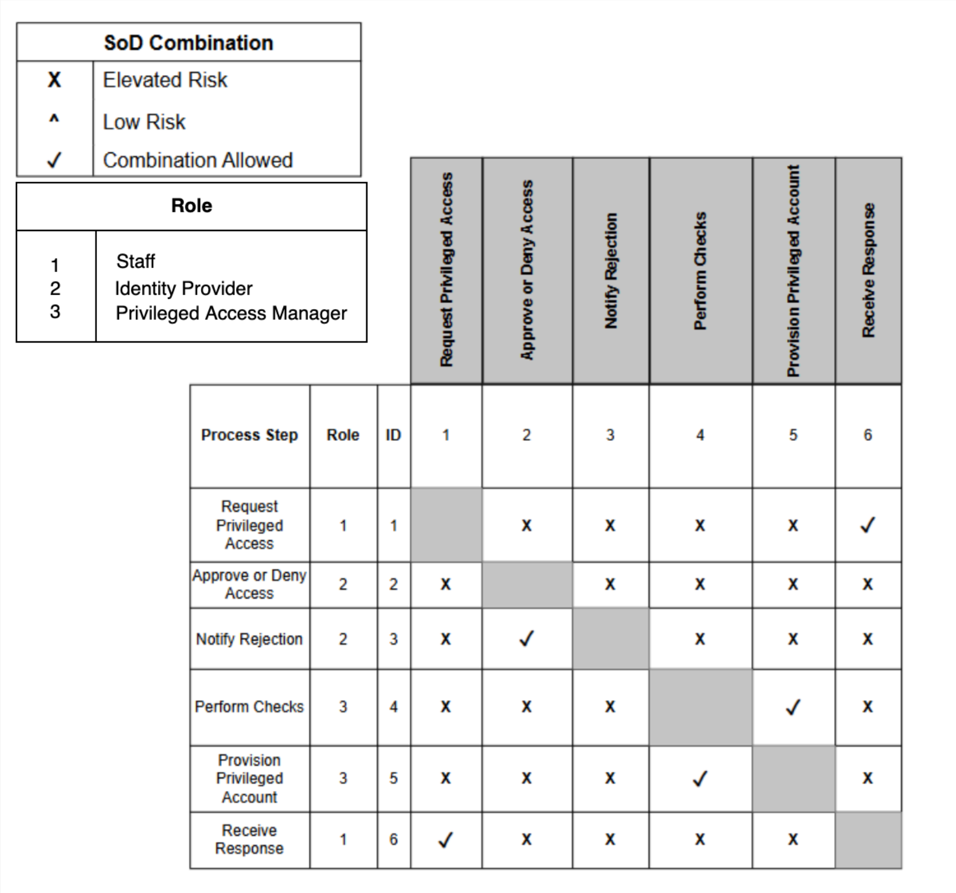
Overview of Non-functional Requirements - MoSCoW

NFR	Domain	Category	Prio	Requirement	Ext. Ref.	Solution	Service Owner
SEC	**Scalability**	**SC_001**	**MUST**	The system **MUST** support both horizontal and vertical scaling for increasing data volumes and applications.	001	Design architecture with auto-scaling features in cloud environments and ensure seamless addition of resources when thresholds are reached.	Cloud Service Provider
SEC	**Maintainability**	**UPD_002**	**MUST**	The system **MUST** have the ability to upgrade components with minimal disruption to services.	002	Plan upgrades during low-usage windows, leverage canary deployments for minimal downtime.	Global Systems Integrator
SEC	**Latency**	**LAT_003**	**SHOULD**	Network communication with the MSS provider **SHOULD** maintain acceptable latency (<100ms round-trip) to support real-time operations.	003	Optimise network routes and ensure high-speed interconnectivity with MSS providers for real-time operations.	Network Operations
SEC	**Cost Efficiency**	**BGT_004**	**MUST**	The Project **MUST** meet allocated budgets for implementation and ongoing operations.	004	Plan a cost-optimized infrastructure using reserved instances, discounts, and cost tracking tools.	Finance Manager
SEC	**Training**	**KB_005**	**COULD**	Eagle Finance **COULD** Maintain an up-to-date repository of knowledge articles and FAQs.	005	Host knowledge base with search capabilities, ensuring all documentation is easily accessible and periodically reviewed.	Knowledge Management Specialist
SEC	**Adaptability**	**POL_006**	**WOULD**	The system **WOULD** have the ability to quickly implement new security policies or compliance requirements.	006	Centralise policy management with tools like a security policy engine and automate compliance checks.	Compliance Officer

Privileged Access Management (Process Flow)



Separation of Duties Matrix



SoD Combination	
X	Elevated Risk
^	Low Risk
✓	Combination Allowed

Role	
1	Staff
2	Identity Provider
3	Privileged Access Manager

			Request Privileged Access	Approve or Deny Access	Notify Rejection	Perform Checks	Provision Privileged Account	Receive Response
Process Step	**Role**	**ID**	1	2	3	4	5	6
Request Privileged Access	1	1		X	X	X	X	✓
Approve or Deny Access	2	2	X		X	X	X	X
Notify Rejection	2	3	X	✓		X	X	X
Perform Checks	3	4	X	X	X		✓	X
Provision Privileged Account	3	5	X	X	X	✓		X
Receive Response	1	6	✓	X	X	X	X	

Table of Contents

Overall Business and IT Context

System Context

Requirements and Constraints

Application Security

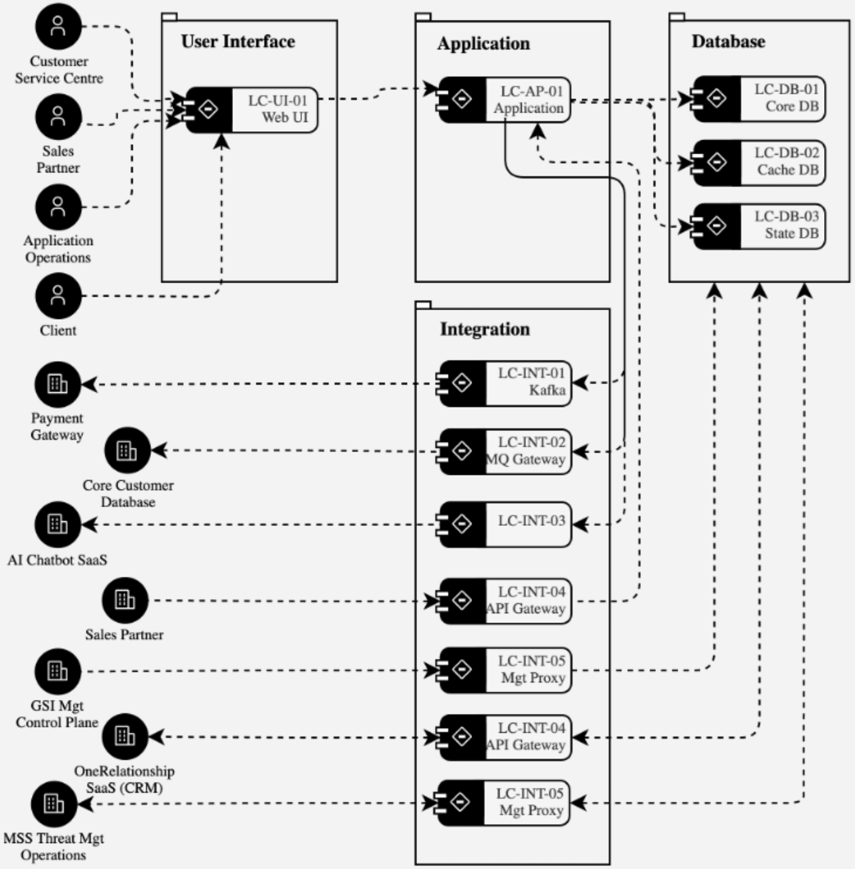
Infrastructure Security

Architecture Patterns and Decisions

Security Development and Assurance

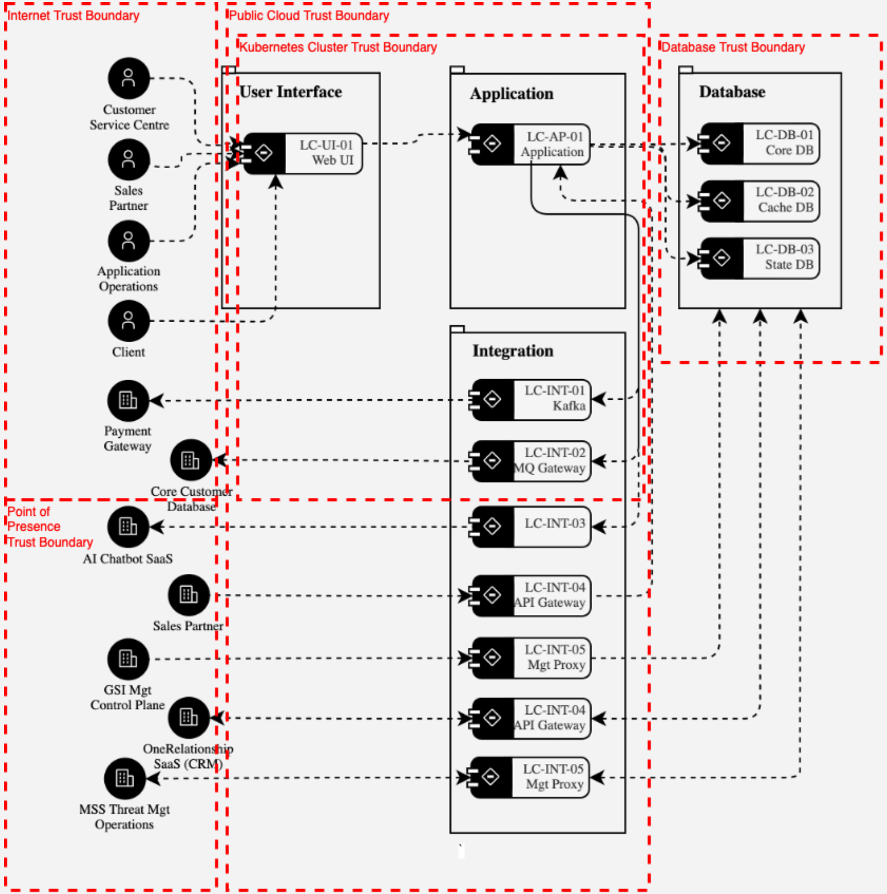
Closing Remarks

Component Architecture Model



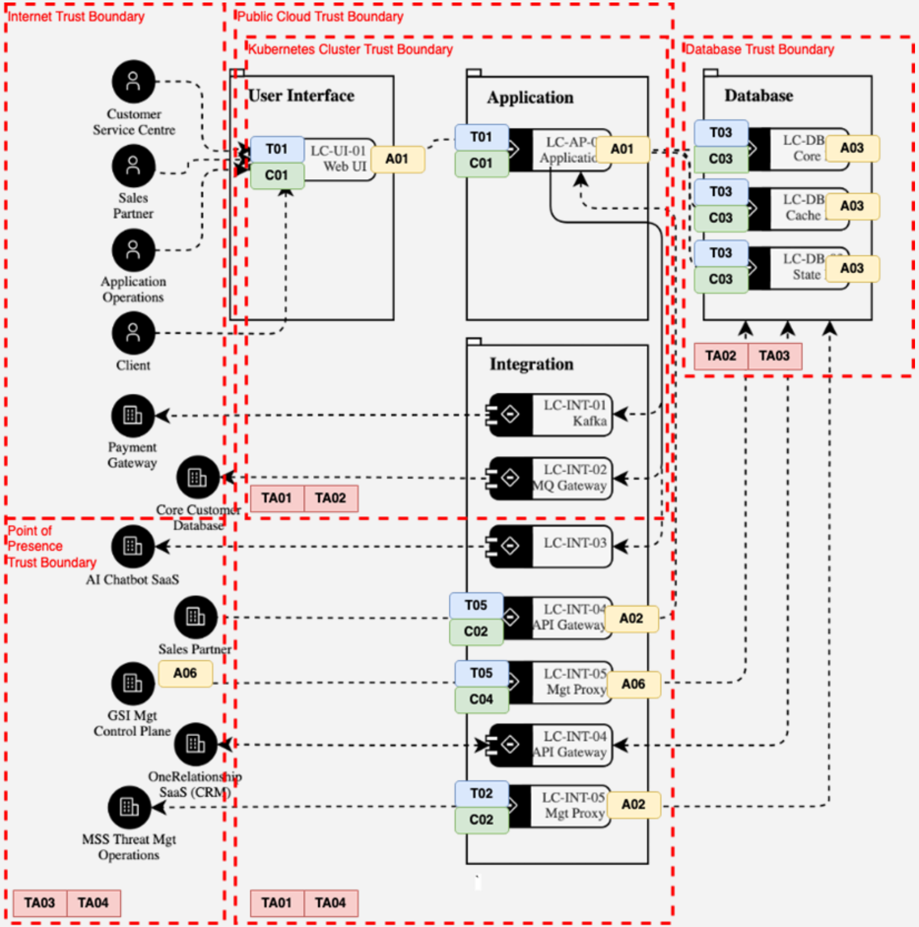
Component Architecture Model

Pramod Kumar

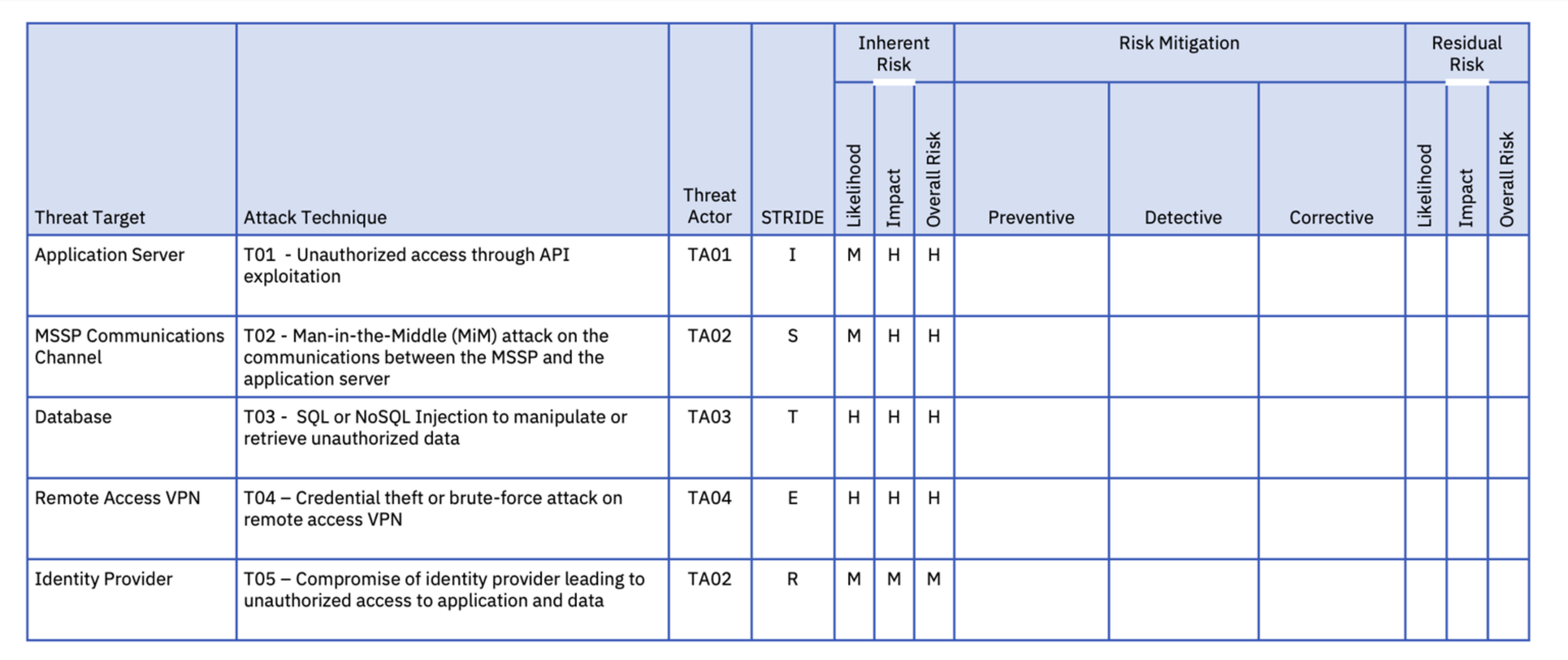


Component Architecture Model

ASSETS	THREATS
A01: Application Server A02: MSSP Communication Channel A03: Databases A04: Identity Provider A05: Remote Access VPN A06: Global System Integrator (GSI)	T01: Unauthorized API access T02: MSSP Man-in-the-Middle Attack T03: SQL/NoSQL Injection T04: Compromised Identity Provider T05: Credential theft T06: Insider threat
THREAT ACTORS	**CONTROLS**
TA01: External Authorized TA02: External Unauthorized TA03: Internal Authorized TA04: Internal Unauthorized	C01: Secure API Gateway and Rate Limiting C02: TLS Encryption and Mutual Auth C03: Input Validation and Parametrized Queries C04: Multi-Factor Authentication

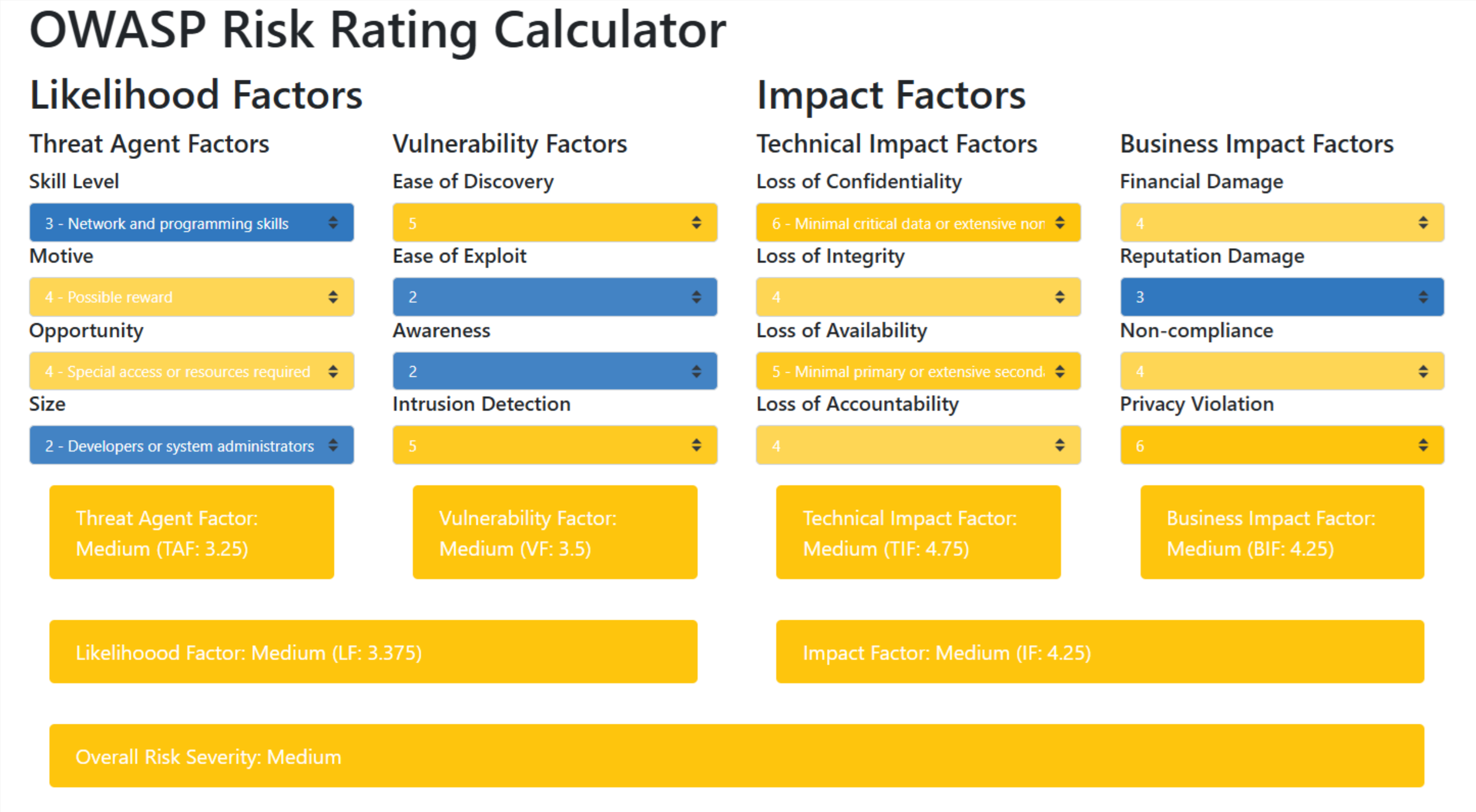


Threat, Vulnerability and Risk Matrix



Threat Target	Attack Technique	Threat Actor	STRIDE	Inherent Risk			Risk Mitigation			Residual Risk		
				Likelihood	Impact	Overall Risk	Preventive	Detective	Corrective	Likelihood	Impact	Overall Risk
Application Server	T01 - Unauthorized access through API exploitation	TA01	I	M	H	H						
MSSP Communications Channel	T02 - Man-in-the-Middle (MiM) attack on the communications between the MSSP and the application server	TA02	S	M	H	H						
Database	T03 - SQL or NoSQL Injection to manipulate or retrieve unauthorized data	TA03	T	H	H	H						
Remote Access VPN	T04 – Credential theft or brute-force attack on remote access VPN	TA04	E	H	H	H						
Identity Provider	T05 – Compromise of identity provider leading to unauthorized access to application and data	TA02	R	M	M	M						

Inherent Risk Calculation



OWASP Risk Rating Calculator

Likelihood Factors

Threat Agent Factors

Skill Level
3 - Network and programming skills

Motive
4 - Possible reward

Opportunity
4 - Special access or resources required

Size
2 - Developers or system administrators

Vulnerability Factors

Ease of Discovery
5

Ease of Exploit
2

Awareness
2

Intrusion Detection
5

Impact Factors

Technical Impact Factors

Loss of Confidentiality
6 - Minimal critical data or extensive non

Loss of Integrity
4

Loss of Availability
5 - Minimal primary or extensive second

Loss of Accountability
4

Business Impact Factors

Financial Damage
4

Reputation Damage
3

Non-compliance
4

Privacy Violation
6

Threat Agent Factor: Medium (TAF: 3.25)

Vulnerability Factor: Medium (VF: 3.5)

Technical Impact Factor: Medium (TIF: 4.75)

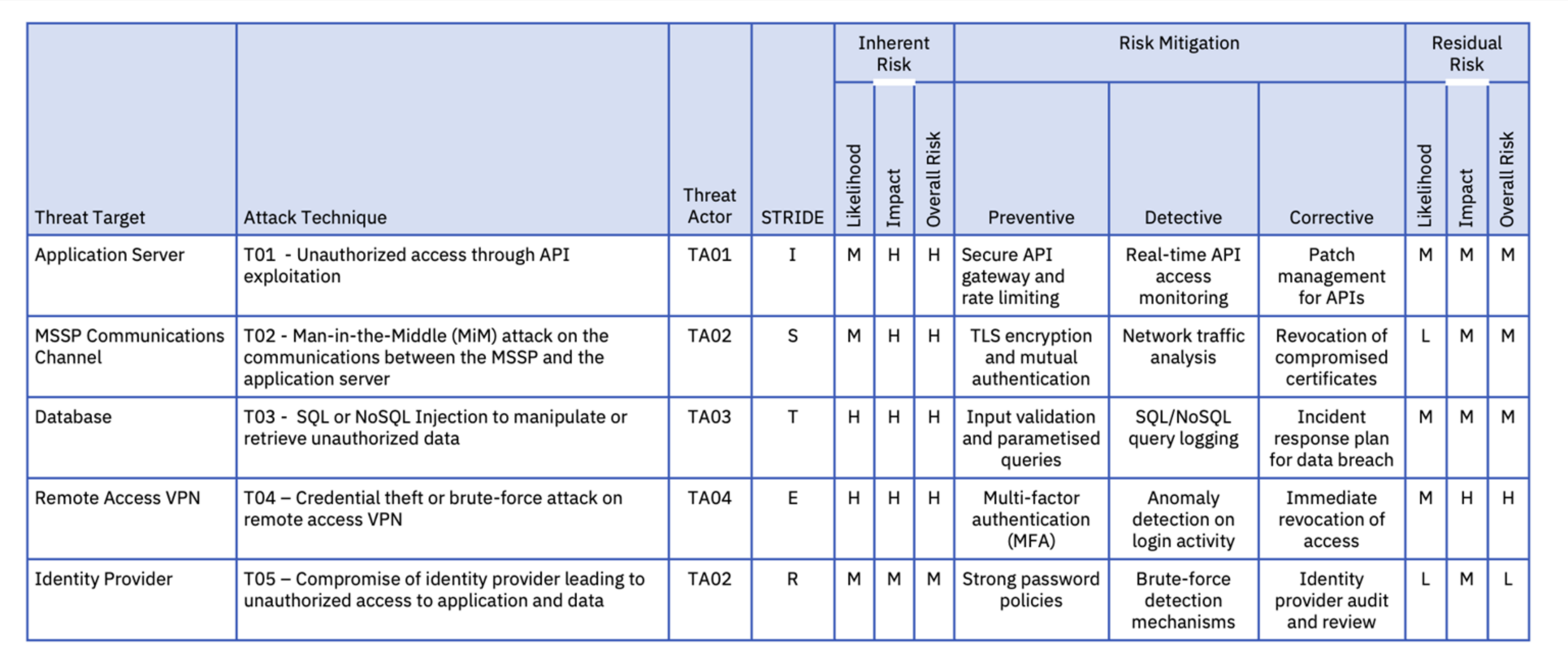
Business Impact Factor: Medium (BIF: 4.25)

Likelihoood Factor: Medium (LF: 3.375)

Impact Factor: Medium (IF: 4.25)

Overall Risk Severity: Medium

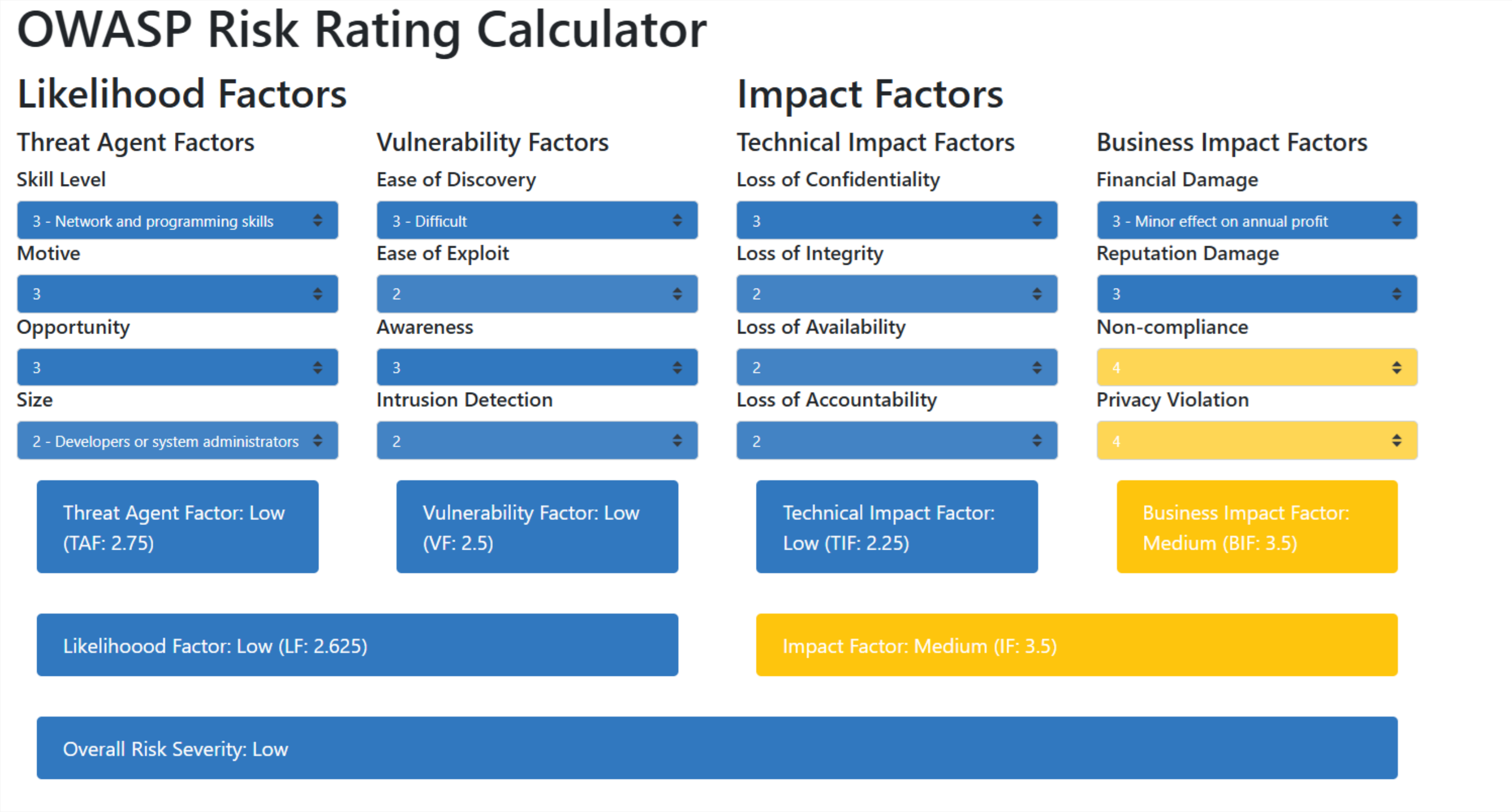
Threat, Vulnerability and Risk Matrix (continued)



Threat Target	Attack Technique	Threat Actor	STRIDE	Inherent Risk			Risk Mitigation			Residual Risk		
				Likelihood	Impact	Overall Risk	Preventive	Detective	Corrective	Likelihood	Impact	Overall Risk
Application Server	T01 - Unauthorized access through API exploitation	TA01	I	M	H	H	Secure API gateway and rate limiting	Real-time API access monitoring	Patch management for APIs	M	M	M
MSSP Communications Channel	T02 - Man-in-the-Middle (MiM) attack on the communications between the MSSP and the application server	TA02	S	M	H	H	TLS encryption and mutual authentication	Network traffic analysis	Revocation of compromised certificates	L	M	M
Database	T03 - SQL or NoSQL Injection to manipulate or retrieve unauthorized data	TA03	T	H	H	H	Input validation and parametised queries	SQL/NoSQL query logging	Incident response plan for data breach	M	M	M
Remote Access VPN	T04 – Credential theft or brute-force attack on remote access VPN	TA04	E	H	H	H	Multi-factor authentication (MFA)	Anomaly detection on login activity	Immediate revocation of access	M	H	H
Identity Provider	T05 – Compromise of identity provider leading to unauthorized access to application and data	TA02	R	M	M	M	Strong password policies	Brute-force detection mechanisms	Identity provider audit and review	L	M	L

Residual Risk Calculation

Pramod Kumar



OWASP Risk Rating Calculator

Likelihood Factors

Threat Agent Factors

Skill Level: 3 - Network and programming skills

Motive: 3

Opportunity: 3

Size: 2 - Developers or system administrators

Vulnerability Factors

Ease of Discovery: 3 - Difficult

Ease of Exploit: 2

Awareness: 3

Intrusion Detection: 2

Impact Factors

Technical Impact Factors

Loss of Confidentiality: 3

Loss of Integrity: 2

Loss of Availability: 2

Loss of Accountability: 2

Business Impact Factors

Financial Damage: 3 - Minor effect on annual profit

Reputation Damage: 3

Non-compliance: 4

Privacy Violation: 4

Threat Agent Factor: Low (TAF: 2.75)

Vulnerability Factor: Low (VF: 2.5)

Technical Impact Factor: Low (TIF: 2.25)

Business Impact Factor: Medium (BIF: 3.5)

Likelihoood Factor: Low (LF: 2.625)

Impact Factor: Medium (IF: 3.5)

Overall Risk Severity: Low

Table of Contents

Overall Business and IT Context

System Context

Requirements and Constraints

Application Security

Infrastructure Security

Architecture Patterns and Decisions

Security Development and Assurance

Closing Remarks

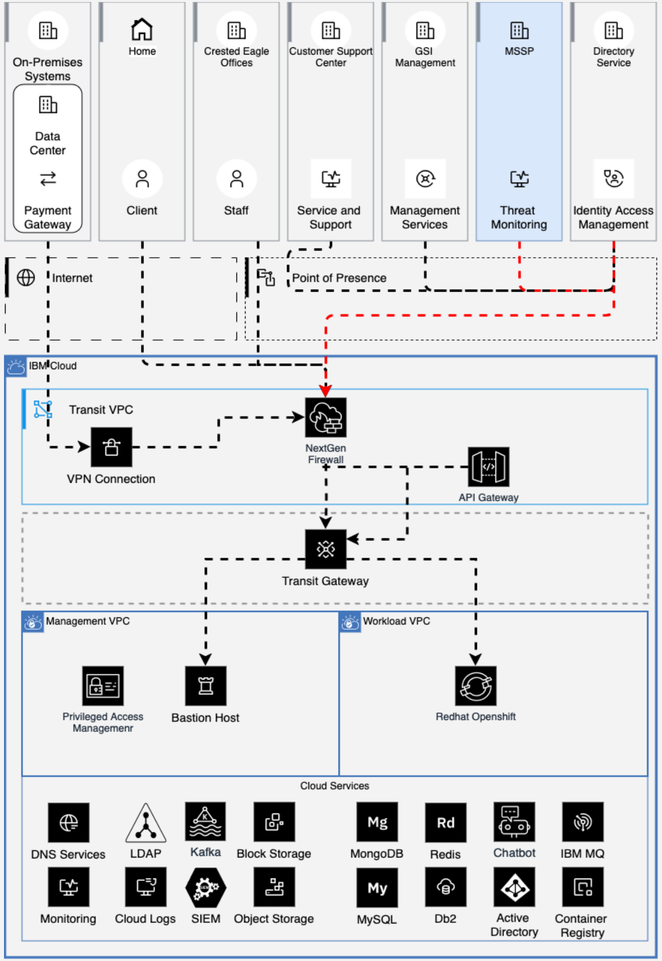
Cloud Deployment Model

Marciej Duda

- External systems and on-premises resources communicate securely with cloud services through the Transit VPC and PoP.

- Administrative access is tightly controlled using the Management VPC with tools like PAM and the Bastion Host

- Logs and security events from across the infrastructure are analyzed externally by the MSSP to maintain strong security posture.



Threat Detection Use Case

Threat detection use case: NoSQL Injection						
Description	An attacker attempts to exploit vulnerable MongoDB queries by injecting malicious operators and syntax into user-supplied input fields. This could allow bypassing authentication, accessing unauthorized data, or manipulating database operations					
Rationale	MongoDB applications are vulnerable to NoSQL injection attacks through unvalidated user input					
Requester	Security Operations Center					
Rule	**Description**	**Event sources**	**Event fields**	**Exceptions**	**Dimensions**	**Notes**
Query Parameterization	Monitor for suspicious in query parameters	MongoDB audit logs, application logs	Query_type, query_content, user_ID, source_IP	Queries from approved admin IPs/subnets, Index management operations	MongoDB	High priority alert - requires immediate investigation
JavaScript Execution Detection	Monitor for JavaScript code in queries	MongoDB system logs	Query_content, js_code	Approved map-reduced operations	MongoDB	Block unauthorized JavaScript execution
Data Exfiltration Detection	Monitor for unusual data volume or pattern retrieval	MongoDB audit logs, network logs	Query_size, result_size, database_name	Scheduled backups, data migrations	MongoDB	High priority alert on large result sets from unusual sources

Incident Response Runbook

Marciej Duda

Incident response runbook:

Description		**Respond to successful NoSQL Injection on Database**				
Detection Use Case		**NoSQL Injection**				
	Activity	**Description**	**Tier 1**	**Tier 2**	**Tier 3**	**Tier 4**
Identification	1.	1. Review MongoDB audit logs, system logs, and application logs for suspicious query parameters or JavaScript execution. 2. Correlate unusual activities with SIEM alerts or other detection tools. 3. Identify affected systems and users and flag affected systems and events.	✓			
	2.	1. Validate the flagged events by analyzing source IPs, user IDs, and query patterns. 2. Cross-reference suspicious activity with threat intelligence feeds. 3. Escalate confirmed incidents to Tier 3 for detailed incident report.		✓		
	3.	1. Prepare a detailed incident report summarising identified indicators of compromise. 2. Notify the client’s internal IT/security team. 3. Escalate validated incidents to the client’s CSIRT for action.			✓	
Containment	1.	1. Disable unauthorized JavaScript execution at database level. 2. Request MSSP to block malicious IP addresses or domains through firewalls and Website Application Firewall rules. 3. Monitor network traffic to confirm the reduction of unusual activity.			✓	✓
	2.	1. If unusual activity continues, temporarily disable vulnerable REST API endpoints as advised by MSSP. 2. MSSP enforces access restrictions on databases to prevent unauthorised queries. 3. Collaborate with MSSP to segment affected components in the hybrid cloud environment.			✓	✓
Eradication	1.	1. Identify and fix Application-Level Vulnerabilities, that caused the injection. 2. Update NoSQL Database Configuration 3. Verify affected systems are patched.	✓	✓	✓	
	2.	1. Advise client to change exposed credentials, keys and tokens. 2. Audit the database to ensure that Malicious Artifacts and backdoors are removed. 3. Verify that step 2 by doing follow-up scans and a logging review.	✓	✓	✓	
Recovery	1.	1. Develop a recovery plan. 2. Propose measure to restore Database integrity, and submit recovery plan.	✓			
	2.	1. Monitor restored systems that use the recovery plan and record anomalies. 2. Validate System Functionality and Restore Database from Clean Backups and ensure security. 3. Apply Long-Term Security Enhancements and Monitor for Recurrence of the Attack	✓	✓		
Post-Incident Review	1.	1. Conduct a Detailed Incident Analysis and Effectiveness and its Impact 2. Identify Vulnerability, Security Gaps and Policies. 3. Strengthen Incident Response Runbook with logs of the incident and preventions.	✓	✓	✓	✓
	2.	1.Through the new Incident Response Runbook, conduct Training and Awareness Sessions 2.Communicate Findings to Stakeholders, and the higher ups of the company.	✓	✓	✓	✓

Table of Contents

Overall Business and IT Context

System Context

Requirements and Constraints

Application Security

Infrastructure Security

Architecture Patterns and Decisions

Security Development and Assurance

Closing Remarks

Security Architectural Decision Record

Pramod Kumar

Decisions	Motivation (or Rationale)	Implication
Use of SIEM for Threat Monitoring (e.g., Splunk or IBM QRadar)	To centralize threat data collection, log management, and real-time monitoring, enabling faster detection and response to incidents.	Improved detection of anomalies across hybrid cloud and on-premises environments.
Implement IDS/IPS (e.g., Snort, Zeek)	To identify and block malicious traffic at both network and application layers, ensuring secure data transmission and protection from external threats.	Strengthened network security with proactive threat prevention. However, high false-positive rates can increase.
Enforce Encrypted Communication Channels (TLS 1.2+)	To ensure secure data transmission between Crested Eagle Finance and MSSP infrastructure, reducing the risk of man-in-the-middle (MITM) attacks.	Enhanced data security during transmission, meeting regulatory standards like GDPR.
Use Role-Based Access Control (RBAC) for MSSP Access	To limit the MSSP provider's access to only necessary resources, ensuring compliance with the principle of least privilege and safeguarding sensitive information.	Reduced attack surface and minimized risk of data breaches. Though, access management policies need to updated frequently.
Integration of SOAR (e.g., IBM Resilient)	Automating incident response processes to reduce response times and improve efficiency.	Increased efficiency in responding to threats.

Security Architectural Decision Record

Subject Area	Threat Management by Managed Security Service Provider (MSSP)	**Topic**	MSSP Integration
Architectural Decision	Should Crested Eagle Finance integrate MSSP technologies for proactive threat management?	**AD ID**	MSSP-AD-0001
Issue or Problem	Crested Eagle Finance requires robust threat detection and response mechanisms while ensuring secure and compliant integration of MSSP services with their hybrid cloud infrastructure.		
Assumptions	1. Crested Eagle Finance's infrastructure supports integration with MSSP tools. 2. MSSP operates its infrastructure in a different cloud environment. 3. Compliance with GDPR, PCI-DSS, and UK financial regulations is mandatory		
Motivation	1. Enhance threat detection and response capabilities. 2. Leverage MSSP expertise to reduce operational burden. 3. Comply with regulatory requirements and secure customer data effectively.		
Alternatives	1. Build an in-house Security Operation Center (SOC) 2. Use multiple vendors for individual security tools instead of MSSP. 3. Maintain status quo with existing systems.		
Decision	Crested Eagle Finance will integrate MSSP technologies, including SIEM, IDS/IPS, SOAR, and Threat Intelligence platforms, while ensuring secure data transmission, role-based access, and compliance with regulations.		

Security Architectural Decision Record

Justification	1. MSSP provides a unified and scalable approach to managing threats across hybrid cloud environments. 2. MSSP provides a unified and scalable approach to managing threats across hybrid cloud environments. 3. Compliance with industry standards is achievable.
Implications	1. Improved security posture with proactive threat management. 2. Increased initial setup and operational costs. 3. Dependence on MSSP for threat management operations and data security.
Derived Requirements	1. Implement TLS 1.2+ for data encryption. 2. Secure API's for cross-cloud integration. 3. Role-based Access Control (RBAC) for MSSP systems. 4. Real-time notification system for incident response.
Related Decisions	1. Use SIEM for centralized threat monitoring. 2. Integrate EDR tools for endpoint protection. 3. Ensure secure communication between hybrid cloud and MSSP integration.

Table of Contents

Overall Business and IT Context

System Context

Requirements and Constraints

Application Security

Infrastructure Security

Architecture Patterns and Decisions

Security Development and Assurance

Closing Remarks

Risks

Statement	Action(s)	Owner & Date
Data Breaches: Sensitive customer data (10M+ records) in the core customer database or CRM system might be exposed due to misconfigured access or unpatched vulnerabilities.	1: Implement Zero Trust Architecture (ZTA) to enforce least privilege access across all systems. 2: Regularly conduct penetration testing on APIs, databases, and public-facing interfaces. 3: Deploy a Web Application Firewall (WAF) to detect and block suspicious activities.	<CISO and Security Architect> + <5 weeks>
Non-Compliance with PCI-DSS: The handling of credit card transactions may fail to meet compliance standards, leading to fines or reputational damage.	1: Ensure end-to-end encryption of payment data (TLS 1.3 in transit, AES-256 at rest). 2: Conduct quarterly audits and vulnerability assessments to verify compliance. 3: Enforce data tokenization to minimize exposure of payment details.	<Compliance Officer and CISO> + <6 weeks>
MSSP Integration Risks: Threat management services operated by MSSP in another cloud may face connectivity or policy misalignment issues.	1: Establish Service Level Agreements (SLAs) with clear escalation procedures for outages or breaches. 2: Use encrypted communication channels (e.g., VPN, IPsec) between the MSSP and core systems. 3: Perform periodic third-party risk assessments of MSSP infrastructure.	<MSSP Manager and Infrastructure Lead> + <5 weeks>
Regulatory Audit Failure: Insufficient documentation or unaddressed risks may fail to satisfy the UK financial regulator’s focus on cyber resilience.	1: Maintain a comprehensive audit trail for all security-related decisions and changes. 2: Use compliance automation tools to align configurations with PCI-DSS and GDPR standards. 3: Conduct mock regulatory audits with internal and external reviewers.	<Compliance Officer and Documentation Lead> + <8 weeks>

Assumptions

Statement	Action(s)	Owner & Date
Crested Eagle Finance assumes that the MSSP will ensure consistent backup and disaster recovery processes for all logs and configurations, including automated failover capabilities during MSSP infrastructure outages.	1. Audit MSSP’s disaster recovery capabilities during annual incident response simulations. 2. Verify MSSP log backups through monthly retention reports generated by Splunk and AWS Security Hub. 3. Ensure MSSP infrastructure is compliant with multi-region redundancy standards for critical systems.	<MSSP Manager> + <2 weeks>
Crested Eagle Finance assumes that the MSSP will handle insider threat scenarios with precision, especially for high-risk systems like the payment gateway (Apache Kafka) and sales partner APIs, minimizing disruption to legitimate activities.	1. Require MSSP to develop behavior-based monitoring specifically for insider threats using tools like Microsoft Defender for Endpoint. 2. Test MSSP response accuracy through simulated insider threat incidents biannually. 3. Maintain a centralized repository in Airtable for reporting and tracking insider-related anomalies escalated by MSSP.	<Chief Information Security Officer> + <4 weeks>
Crested Eagle Finance assumes the MSSP will provide transparent escalation paths for non-critical incidents, ensuring operational priorities are not delayed due to over-escalation of minor alerts.	1. Establish a tiered escalation framework within IBM Resilient, categorizing incident severity and required actions. 2. Train internal teams to independently resolve minor incidents flagged by MSSP with guidance from documented playbooks. 3. Review incident escalation logs quarterly to identify patterns of unnecessary escalations and adjust thresholds.	<Incident Response Manager> + <3 weeks>
Crested Eagle Finance assumes that the MSSP will ensure consistent backup and disaster recovery processes for all logs and configurations, including automated failover capabilities during MSSP infrastructure outages.	1. Test MSSP’s disaster recovery capabilities during annual incident response simulations. 2. Verify MSSP log backups through monthly retention reports generated by Splunk and AWS Security Hub. 3. Ensure MSSP infrastructure is compliant with multi-region redundancy standards for critical systems.	<MSSP Manager> + <2 weeks>

Issues

Statement	Action(s)	Owner & Date
MSSP provided reports lack clarity, often missing actionable details, making it difficult for Crested Eagle Finance's security team to respond effectively.	1. Work with the MSSP to define a competent reporting template that uses Splunk and IBM QRadar to highlights risks specific to critical assets like the on-premises IBM DB2 database and cloud-native MongoDB. 2. Configure automated data aggregation and reporting dashboards within the IBM Resilient (SOAR) platform to generate actionable, real-time insights. 3. Schedule bi-weekly meetings to review reports, ensuring alignment with Crested Eagle Finance’s hybrid cloud security needs.	<Security Operations Team> + <2 weeks>
The MSSP lacks contextual knowledge of Crested Eagle Finance business operations, such as routine API traffic between the One Relationship SaaS (CRM) and on-premises DB2 could be flagged unnecessarily, slowing operations	1. Share business asset classifications with the MSSP, mapping systems such as the One Relationship CRM and Kubernetes services to critical business processes using AWS Security Hub. 2. Calibrate CrowdStrike threat intelligence feeds to prioritise potential risks associated with financial services, ensuring MSSP alert configurations align with Crested Eagle’s priorities. 3. Conduct quarterly calibration exercises to fine-tune detection rules in Snort and Zeek, reducing noise from low-priority or known safe activities.	<Security Monitoring Lead> + <3 weeks>
Incident response times are inconsistent due to delays occurring when incidents involving endpoints managed by Microsoft Defender are not escalated to the internal team in time to mitigate potential breaches	1. Develop and document an incident response playbook within IBM Resilient (SOAR) that maps clear escalation paths, including roles for the MSSP and Crested Eagle’s Application Operations and CISO teams. 2. Integrate Microsoft Teams notifications into the SOAR platform for multi-channel alerts to response teams. 3. Establish SLA dashboards within Splunk to monitor and enforce agreed response times, ensuring accountability for MSSP and internal team performance.	<Incident Response Manager> + <2 weeks>
The insufficient retention of MSSP logs and monitoring data fails to meet PCI-DSS compliance requirements, hindering forensic investigations into incidents involving critical systems like the Apache Kafka payment gateway, thereby increasing regulatory and operational risks.	1. Implement a log retention policy across Splunk and AWS Security Hub, ensuring compliance with PCI-DSS requirements by retaining critical logs for at least 12 months. 2. Utilise Microsoft Purview to manage and encrypt all retained logs, ensuring data integrity and protection. 3. Schedule monthly retention audits to verify that MSSP is maintaining proper storage practices for logs related to hybrid cloud transactions and threat management operations.	<Compliance Manager> + <4 weeks>

Dependencies

Yash Rajendra Hajare

Statement	Action(s)	Owner & Date
The MSSP depends on Crested Eagle Finance's Global Systems Integrator (GSI) to maintain continuous infrastructure availability and ensure that key systems, like Red Hat OpenShift and Apache Kafka, are operational for seamless integration.	1. Define and enforce Service Level Agreements with the GSI for minimum uptime requirements, explicitly covering systems critical to MSSP operations. 2. Implement a real-time status dashboard for GSI-managed systems using tools like Splunk or AWS Security Hub. 3. Schedule quarterly alignment meetings between the MSSP, GSI, and Crested Eagle Finance to discuss operational risks and upcoming infrastructure changes.	<Infrastructure & Operations Team> + <3 weeks>
The MSSP requires a structured change management process from Crested Eagle Finance to receive updates on modifications to systems such as Kubernetes,Apache Kafka, and public cloud databases.	1. Use a centralised change management repository (e.g., Airtable) to track and share all infrastructure, software, and network updates with MSSP. 2. Automate notifications for MSSP using tools like GitHub Actions, ensuring they are informed about updates to systems like MongoDB or Kubernetes. 3. Perform quarterly impact assessments with MSSP teams to evaluate whether recent changes have affected detection rules or system integrations.	<Operations & DevOps Team> + <2 weeks>
The MSSP depends on Crested Eagle Finance's customer support center to provide context on user-reported anomalies and potential insider threats for improved threat intelligence correlation.	1. Train customer support staff on recognizing and reporting potential security anomalies, using standardized templates shared with MSSP. 2. Integrate an anomaly tracking system, such as a shared workflow in IBM QRadar, to log reports and forward them to MSSP for analysis. 3. Conduct biannual joint training sessions between MSSP analysts and customer support teams to improve collaboration and threat context understanding.	<Customer Support Manager> + <4 weeks>
The MSSP relies on Crested Eagle Finance to provide comprehensive incident response permissions to critical systems, such as firewalls (Fortinet FortiGate) and endpoint protection (Microsoft Defender), to execute remediation actions.	1. Implement a role-based access control framework via Azure Active Directory, granting MSSP access to only necessary resources during incident response. 2. Regularly audit MSSP permissions using Microsoft Purview to ensure they align with organizational policies and are not overly permissive. 3. Define and share a remediation authorization workflow with MSSP through IBM Resilient, clarifying escalation procedures and pre-approved actions for urgent incidents.	<Security Operations Team> + <3 weeks>

Table of Contents

Overall Business and IT Context

System Context

Requirements and Constraints

Application Security

Infrastructure Security

Architecture Patterns and Decisions

Security Development and Assurance

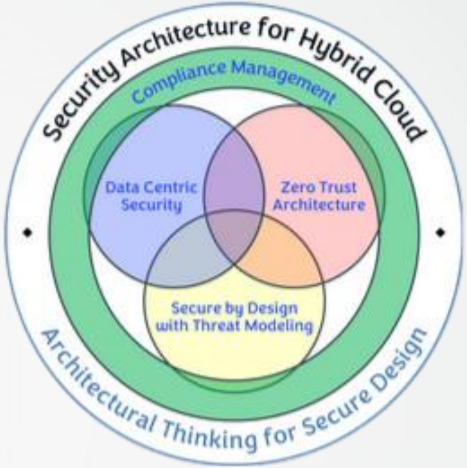
Closing Remarks

Closing Remarks

Summaries

- Identified the business goal of integrated CRM system to enhance collaboration with sales partners while ensuring compliance with PCI-DSS regulations.
- Delivered a scalable and secure hybrid cloud solution integrating Crested Eagle Finance’s systems with the Managed Security Services Provider.
- Assessed threats and vulnerabilities, calculated inherent and residual risks, and provided actionable incident response.
- Leveraged a structured architectural decision-making process to evaluate trade-offs, prioritize security requirements, and align the system design.
- Established a structured approach for risks, issues, and dependencies, ensuring long-term operational efficiency and security.

Thank you for your time!


Security Architecture for Hybrid Cloud
Compliance Management
Data Centric Security
Zero Trust Architecture
Secure by Design with Threat Modeling
Architectural Thinking for Secure Design