Newstar Auto Threat Model

Owner: Pooya Molai
Reviewer:
Contributors:
Date Generated: Tue Oct 22 2024

Executive Summary

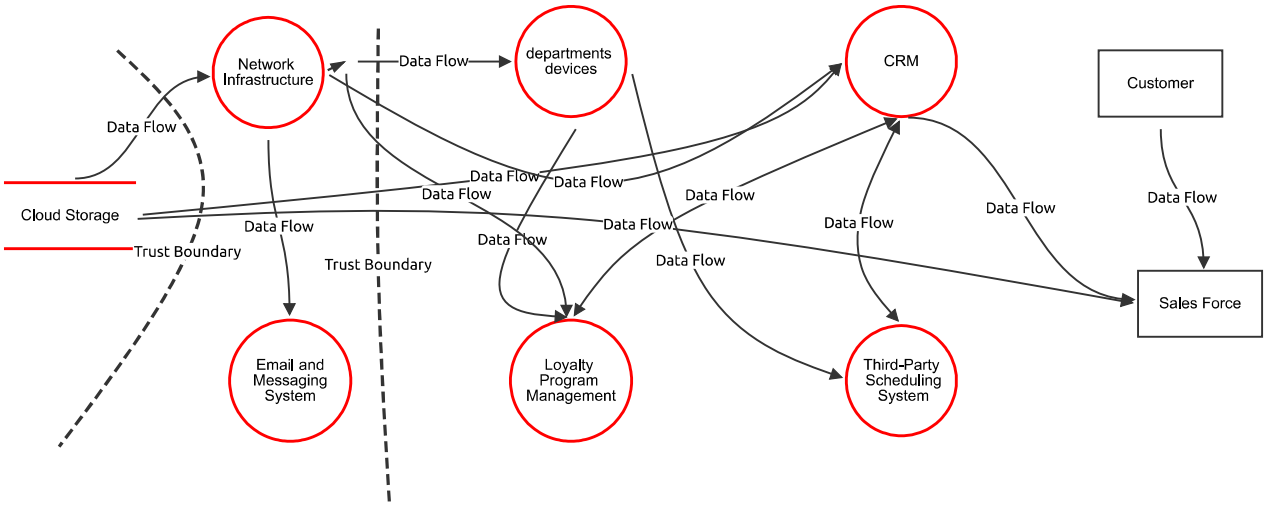
High level system description

Not provided

Summary

Total Threats	42
Total Mitigated	0
Not Mitigated	42
Open / High Priority	28
Open / Medium Priority	14
Open / Low Priority	0
Open / Unknown Priority	0

New STRIDE diagram



New STRIDE diagram

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

CRM (Process)

Stores and manages customer data, including personal details, sales pipeline, and service interactions.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	New STRIDE threat	Spoofing	High	Open	8/10	An attacker impersonates an authorized user to gain access to the CRM.	Implement strong user authentication mechanisms, such as Multi-Factor Authentication (MFA) and Single Sign-On (SSO). Regularly review user access rights.
2	New STRIDE threat	Tampering	High	Open	8/10	An attacker modifies customer data within the CRM, such as altering sales records or customer information.	Use data integrity checks, digital signatures, and role-based access control (RBAC) to prevent unauthorized data changes. Implement logging and alerting for any unauthorized data modification attempts.
3	New STRIDE threat	Repudiation	Medium	Open	6/10	A user denies having performed a particular action within the CRM, such as modifying customer records.	Enable logging and auditing within Salesforce to track user actions. Use non-repudiation techniques such as maintaining secure, immutable logs to provide proof of actions.
4	New STRIDE threat	Information disclosure	High	Open	9/10	Sensitive customer data (e.g., PII, purchase history, preferences) is disclosed to unauthorized users.	Ensure data encryption both at rest and in transit. Enforce least privilege access, meaning only authorized users can access sensitive information. Monitor data access with alerts for unusual activity.
5	New STRIDE threat	Denial of service	Medium	Open	5/10	An attacker could overload the CRM system, causing it to become unresponsive or unavailable.	Implement rate limiting, request throttling, and ensure Salesforce's cloud infrastructure has DoS protection measures. Utilize cloud-based distributed denial of service (DDoS) protection services.
6	New STRIDE threat	Elevation of privilege	High	Open	8/10	An attacker or unauthorized user exploits a vulnerability to gain higher-level privileges in the CRM system.	Use RBAC to ensure users have only the permissions required for their roles. Regularly conduct security assessments and patch management to mitigate vulnerabilities.

Third-Party Scheduling System (Process)

Used for managing service appointments, vehicle deliveries, and maintenance scheduling.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	New STRIDE threat	Spoofing	High	Open	8/10	An attacker impersonates a legitimate user to gain access to the scheduling system.	Implement MFA and secure authentication protocols for all users. Regularly audit access controls to prevent unauthorized access.
8	New STRIDE threat	Tampering	High	Open	8/10	An attacker modifies appointment or vehicle delivery data in the scheduling system.	Enforce data integrity checks, use digital signatures, and employ RBAC to prevent unauthorized data modification. Log and monitor all system changes.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
9	New STRIDE threat	Repudiation	Medium	Open	6/10	A user denies having scheduled or modified appointments.	Maintain secure, immutable logs of all actions taken in the scheduling system to provide proof of actions and enable audits.
10	New STRIDE threat	Information disclosure	High	Open	9/10	Sensitive scheduling information is disclosed to unauthorized individuals.	Encrypt data at rest and in transit, and enforce strict access controls. Monitor data access with alerts for any suspicious activity.
11	New STRIDE threat	Denial of service	Medium	Open	5/10	An attacker overloads the scheduling system, making it unavailable for legitimate users.	Implement rate limiting and request throttling. Ensure the third-party provider has robust DDoS protection measures in place.
12	New STRIDE threat	Elevation of privilege	High	Open	8/10	An attacker exploits a vulnerability to gain higher-level access within the scheduling system.	Implement RBAC to restrict access to administrative functions. Conduct regular security assessments and patch any vulnerabilities promptly.

Cloud Storage (Store)

Stores customer data that has been migrated from on-premise servers for scalability and accessibility.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	New STRIDE threat	Tampering	High	Open	8/10	An attacker impersonates an authorized user to gain access to cloud storage.	Enforce strong user authentication mechanisms, including Multi-Factor Authentication (MFA) and Single Sign-On (SSO). Regularly audit access control policies.
14	New STRIDE threat	Repudiation	High	Open	8/10	An attacker modifies stored data, such as customer information or service records.	Use encryption, data integrity checks, and version control to protect stored data. Implement logging to detect unauthorized modifications.
15	New STRIDE threat	Repudiation	Medium	Open	6/10	A user denies having made changes or accessed cloud-stored data.	Maintain secure, immutable logs of all activities and actions taken in cloud storage. Implement non-repudiation measures to track user activities.
16	New STRIDE threat	Information disclosure	High	Open	9/10	Sensitive customer data stored in the cloud is disclosed to unauthorized individuals.	Encrypt data both at rest and in transit. Enforce strict access controls with least privilege principles. Use monitoring tools to detect unusual access patterns.
17	New STRIDE threat	Denial of service	Medium	Open	5/10	An attacker floods the cloud service, making data inaccessible to legitimate users.	Implement rate limiting, request throttling, and ensure the cloud provider has DDoS protection in place.
18	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

departments
devices (Process)

Laptops, desktops, and tablets used by service staff to access Salesforce, scheduling systems, and loyalty program data.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
19	New STRIDE threat	Spoofing	High	Open	8/10	An attacker impersonates a legitimate user by gaining access to service department devices.	Implement strong user authentication mechanisms, including password protection and Multi-Factor Authentication (MFA). Enforce policies for secure device use.
20	New STRIDE threat	Tampering	High	Open	8/10	An attacker gains physical access to a device and modifies stored data or software.	Use full-disk encryption to protect stored data, enforce secure boot settings, and implement endpoint security software to detect unauthorized changes.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
21	New STRIDE threat	Repudiation	Medium	Open	6/10	A user denies actions taken on a service department device, such as accessing or modifying customer data.	Enable logging and auditing on service department devices. Use tamper-evident logs to provide proof of actions taken.
22	New STRIDE threat	Information disclosure	High	Open	9/10	Sensitive information accessed through service department devices is exposed to unauthorized individuals.	Encrypt data stored locally on devices and ensure that network connections are secured with VPNs. Train staff on proper handling of sensitive data.
23	New STRIDE threat	Denial of service	Medium	Open	5/10	An attacker physically damages or disables a device, rendering it unusable.	Implement device tracking, ensure regular backups of critical data, and have replacement devices readily available.
24	New STRIDE threat	Elevation of privilege	High	Open	8/10	An attacker exploits vulnerabilities in the device or its software to gain elevated privileges.	Keep devices and software up to date with security patches. Use RBAC to limit the privileges of users and enforce least privilege principles.

Network Infrastructure (Process)

Internal network that connects service staff devices to the cloud-based CRM, scheduling systems, and loyalty program.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
25	New STRIDE threat	Spoofing	High	Open	8/10	An attacker impersonates a legitimate device or user within the network.	Implement Network Access Control (NAC) to authenticate devices, use strong authentication protocols, and employ encryption for communication.
26	New STRIDE threat	Tampering	High	Open	8/10	An attacker modifies data packets in transit across the network.	Use encryption protocols like TLS to protect data in transit. Implement integrity checks and secure routing mechanisms to prevent tampering.
27	New STRIDE threat	Repudiation	Medium	Open	6/10	A network user denies having performed certain actions, such as accessing resources or modifying network configurations.	Enable logging of all network activities, including access and configuration changes. Use tamper-evident logs and secure storage for audit trails.
28	New STRIDE threat	Information disclosure	High	Open	9/10	Sensitive data transmitted over the network is intercepted by an unauthorized party.	Encrypt all sensitive data in transit using secure protocols (e.g., TLS/IPsec). Implement network segmentation to reduce the risk of data interception.
29	New STRIDE threat	Denial of service	High	Open	8/10	An attacker floods the network with excessive traffic, making it unavailable to legitimate users.	Deploy firewalls, intrusion detection/prevention systems (IDS/IPS), and rate limiting to mitigate DoS attacks. Utilize cloud-based DDoS protection services.
30	New STRIDE threat	Elevation of privilege	High	Open	8/10	An attacker gains elevated privileges within the network by exploiting vulnerabilities.	Use RBAC to limit user privileges. Regularly update network devices with security patches and conduct vulnerability assessments to address potential weaknesses.

Email and Messaging System (Process)

Used by sales and service staff to communicate with customers regarding appointments, loyalty rewards, and follow-up services.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
31	New STRIDE threat	Spoofing	High	Open	8/10	An attacker impersonates a legitimate user to gain access to email or messaging systems.	Implement MFA for email and messaging access. Use email authentication protocols such as SPF, DKIM, and DMARC to prevent spoofing.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
32	New STRIDE threat	Tampering	High	Open	8/10	An attacker modifies the content of emails or messages in transit.	Encrypt emails and messages in transit using secure protocols like TLS. Use digital signatures to verify the integrity of messages.
33	New STRIDE threat	Repudiation	Medium	Open	6/10	A user denies having sent or received a particular email or message.	Use digital signatures and maintain secure, tamper-proof logs of all communication activities.
34	New STRIDE threat	Information disclosure	High	Open	9/10	Sensitive information shared via email or messaging is exposed to unauthorized parties.	Encrypt emails and messages both at rest and in transit. Implement access controls to restrict who can view or send sensitive information.
35	New STRIDE threat	Denial of service	Medium	Open	5/10	An attacker floods the email or messaging systems, making them unavailable to legitimate users.	Implement rate limiting, spam filtering, and ensure that the email service provider has anti-DDoS measures in place.
36	New STRIDE threat	Elevation of privilege	High	Open	8/10	An attacker exploits vulnerabilities in the email or messaging system to gain elevated privileges.	Use RBAC to limit user privileges. Regularly update and patch email and messaging systems to address vulnerabilities.

Loyalty Program Management (Process)

Manages customer loyalty rewards, service credits, milestones, and owner's club benefits.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
37	New STRIDE threat	Spoofing	High	Open	8/10	An attacker impersonates a legitimate customer to gain access to loyalty rewards or manipulate referral credits.	Enforce MFA for customer accounts and use CAPTCHA to prevent automated attacks. Regularly monitor login attempts for unusual activity.
38	New STRIDE threat	Tampering	High	Open	8/10	An attacker modifies loyalty program data, such as rewards balance or referral information.	Use data integrity checks, implement encryption for stored data, and utilize role-based access control (RBAC) to restrict modification rights.
39	New STRIDE threat	Repudiation	Medium	Open	6/10	A user denies performing actions related to loyalty program participation, such as redeeming rewards or referring others.	Maintain secure, tamper-proof logs of all loyalty program transactions. Use digital signatures to verify actions taken.
40	New STRIDE threat	Information disclosure	High	Open	9/10	Sensitive customer data, including service history and loyalty rewards, is disclosed to unauthorized parties.	Encrypt sensitive data both at rest and in transit. Implement access controls to ensure only authorized users can view or modify customer data.
41	New STRIDE threat	Denial of service	Medium	Open	5/10	An attacker overloads the loyalty program system, making it unavailable to legitimate customers and staff.	Implement rate limiting, request throttling, and ensure the loyalty program service provider has anti-DDoS measures in place.
42	New STRIDE threat	Elevation of privilege	High	Open	8/10	An attacker exploits vulnerabilities to gain elevated privileges in the loyalty program system.	Use RBAC to limit user privileges and enforce the principle of least privilege. Regularly conduct security assessments and apply patches promptly.

Data Flow (Data Flow)

Data such as service history and customer interactions flows to/from the Loyalty Program Management System to maintain consistency.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Customer and sales data is stored in Cloud Storage for accessibility and scalability.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Customer service requests (appointments, vehicle deliveries) are sent to the Scheduling System. Updates to appointments are synchronized back to Salesforce.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Service staff use devices to view and update appointments via the scheduling system.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Cloud-stored data is accessed for customer management and reporting purposes.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Any interaction relevant to rewards or loyalty points is also logged into the Loyalty Program System.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Customer (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Sales Force (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations