

Bird's eye view:

All 🌐 Team APEC 1 threats and mitigations

⚡ „MiTM between #5b ordering kiosk and #5a order processing service” 🤖/🤖

🔒 „encrypted wifi and physical lan cables to reduce impact”

⚡ „#19 GPS spoofing” 🤖/🤖🤖🤖

🔒 „Respond with manual delivery using waiters”

⚡ „#6a and 6b Injection attack Mobile app ordering which may lead to database attacks and privacy incidents with the customer and GPS data.” 🤖🤖/🤖🤖🤖

🔒 „Put firewall and IPS in between the mobile app and database service”

⚡ „"bombing" the Kiosk and make it out of order #tempering”

🔒 „Metal detectors and X-ray to detect malicious intent.”

⚡ „#11 Forward Order system may be offline due to third party issue” 🤖/🤖🤖

🔒 „Have it onsite or high availability servers.”

⚡ „Payment service down due internet service connecting payment service to Order Processing Service may be down.” 🤖/🤖🤖🤖

🔒 „Have alternate internet service provider to connect to the Payment service.”

⚡ „unauthorized access to Drones to control, and drop food on customers in the park #9” 🤖/🤖

🔒 „Encrypt signal, jamming,”

🔒 „Restrict flight routes, shutdown drone if go out from the park,”

🔒 „Update firmware of drone periodicity”

🔒 „Change transmission channel, should be changeable, if hacked the drone”

⚡ „#14 Poison the food”

🔒 „Inspect the food ingredients”

🔒 „Restricting access to the kitchen”

Bird's eye view:

All 🌐 Team APEC 2 threats and mitigations

⚡ „all the databases are in the same network and can be compromised” 🤖/👤👤👤

🔒 „#detect - check logs for auditing process”

🔒 „#detect - use monitoring system (IDS) such as Zabbix”

🔒 „#mitigation - isolate DB to prevent lateral movement”

⚡ „#Database Manipulate order data, change prices or quantities” 🤖🤖/🤖🤖

🔒 „#Mitigate - Implement server-side validation, use HMAC-signed requests, deploy WAF to block malicious inputs”

⚡ „Tampered/compromised mobile application used by customers during the ordering process” 🤖/🤖🤖

🔒 „mitigate - Code signing & certificate verification”

🔒 „mitigate - App integrity checks”

🔒 „detection - monitoring of any unusual outgoing requests containing sensitive information to unusual domains”

⚡ „all the databases are in the same network and can be compromised” 🤖🤖/🤖

🔒 „mitigate - Use VLAN segmentation, application whitelisting, and network ACLs”

🔒 „detection - Implement IDS to monitor for suspicious actions towards database (excessive login attempts, privileged operations etc.)”

🔒 „detection - Enable logging for audit trailing”

🔒 „mitigation - avoid same set of user credentials across all databases”

🔒 „mitigation - Ensure that all databases are updated to the latest version”

⚡ „Kiosk breakout” 🤖/🤖🤖

🔒 „mitigate - Kiosk mode, disable hotkeys, lock shell”

🔒 „mitigation - Whitelisted domains, disable downloads, auto-reset session”

🔒 „mitigate - Lock USB/ports, mount securely, CCTV”

⚡ „#Server - User or attacker impersonates another user” 🤖🤖/👤👤👤

🔒 „Mitigation - Use OAuth 2.0 / OpenID Connect, enforce MFA, secure session cookies (HttpOnly, Secure, SameSite), short token expiry”

🔗 „#Server-Intruder - Customer denies placing an order” 🙄🙄🙄/🙄🙄

🔗 „respond- Maintain immutable logging non-repudiation via digital receipts”

🔗 „Drones signal jamming GPS” 🙄🙄/🙄🙄

🔗 „mitigate - Jammer / spoof detection & geo-awareness”

🔗 „#Database - Exposure of PII or payment info” 🙄/🙄🙄🙄

🔗 „Mitigate - Encrypt at rest (AES-256), in transit (TLS 1.2+),”

🔗 „detect - Implementing Database Activity Monitoring.”

🔗 „The price is tampered with and the item is purchased for a smaller amount.

#Payment” 🙄🙄🙄/🙄🙄

🔗 „Validate input values”

🔗 „Mitigate - Implement principle of least privilege (POLP) on database level”

🔗 „mitigate - rate limiting and behavior detection to flag order patterns.”

🔗 „respond - Logging, monitoring, and automated detection”

🔗 „mitigate - Signed price tokens”

🔗 „mitigate - Harden APIs & authentication”

🔗 „#Payment Gateway - Spoofed requests” 🙄

🔗 „Mitigation - Mutual TLS, signed requests, API key rotation”

🔗 „Hijacking of the network between order processing service and payment service”

🙄/🙄🙄🙄

🔗 „Mitigation - Enforcement of TLS 1.2/1.3 protocol”

🔗 „mitigate - Sign every payment-related payload”

🔗 „mitigate - Validate payment gateway responses & reconciliation via verifying the payment gateway’s callback signature and expected fields. Perform real-time reconciliation: payment callback amount must match server’s expected amount or trigger blocking.”

🔗 „data is tampered with and the product is delivered to a different location. #Server”

🙄🙄/🙄🙄

🔗 „respond - Maintain immutable logging non-repudiation”

🔗 „mitigate - Enforce End-to-End Data Integrity”

🔗 „mitigate - Fraud Detection / Business Logic Controls”

🔗 „@MobileApp API -> Manipulation of order data (e.g., change item price)”

🤖/👤👤👤

🔗 „mitigation - Implement server-side validation, use HMAC-signed requests, deploy WAF to block malicious inputs”

🔗 „19: food may be dropped while delivering” 🤖/👤👤

🔗 „mitigation - Use tamper-evident, spill-proof, and shock-resistant containers; seal bags securely with labels or tamper seals.”

🔗 „disruption of forward order function, preventing orders from reaching the kitchen”

🤖/👤👤

🔗 „recover - setup high availability of services. Could be dual active active forward order platform.”

🔗 „mitigation - deploy encrypted network protocol (Assuming that the forwarding system and the backend system are connected via wireless network protocol”

🔗 „respond - prepare for manual paper option”

🔗 „prevention - Avoid the use of wireless protocol if possible”

Bird's eye view:

All 🌐 Team APEC 3 threats and mitigations

⚡ „Credit card number CVV expriy can be more sensitive data if exposed its the threat by spoofing of customer.” 🤖/👤👤👤

🔒 „Prevent : Use encryption, data at transit, data at rest and data at memory.”

⚡ „Spoofing of customer” 🤖🤖/👤👤👤

🔒 „To authenticate the user, by persons account in payment provider and MFA”

⚡ „Collecting too much data or PII information” 🤖🤖/🤖🤖

🔒 „Minimizing the data usage to perform the function”

⚡ „Repudiation of the customer making an order” 🤖🤖/🤖

🔒 „Using the confirmation button in the app. OTP in an order confirmation.”

⚡ „Information disclosure of the payment information from mobile app to the Order processing then to payment service.” 👤👤👤/👤👤👤

🔒 „Using strong encryption, input filtering via whitelisting.”

⚡ „Denial of service in Kiosk due system down” 🤖/🤖🤖

🔒 „Service level agreement with 3rd party. Rate limiting to avoid attacker making the system unavailable. Black list users.”

⚡ „Tampering of user location. communication between kitchen and Drone.”

🤖🤖/🤖🤖

🔒 „Antivirus on Endpoint, logging mechanism.”

Bird's eye view:

All 🌐 Team APEC 4 threats and mitigations

⚡ „A customer acts like another customer and orders food on behalf of another customer. #spoofing” 🤖/😐😐

🔒 „Customer needs to provide their ticket information.”

🔒 „MFA to be provided by the customer.”

⚡ „An attacker changes customers orders after it has been placed in the mobile app for drone delivery ... with address of delivery changed.” 😐😐/😐😐😐

🔒 „Customer details must be protected in the database and confirmation of customer identity should be performed via OTP at the time of delivery.”

⚡ „Tampering if a friend tampers with your food by adding extra spices” 😐😐😐/😐😐

⚡ „A bot is installed secretly in the mobile app which keeps placing orders from everybody's mobile app constantly ... thus bringing down the order processing service.”

🔒 „Add captcha for each order.”

⚡ „a waiter or threat actor employee copies the digital signature of the restaurant manager and issues discounts to his known friends.” 😐😐/😐😐😐

🔒 „Manager's biometric's are required for providing discounts.”

🔒 „the manager's biometrics should be given to approve the digital signature”

⚡ „A malicious actor adds orders to the system and then denies placing the order.”

🔒 „A confirmation call or message to the mobile app placing the order needs to be made when the order is placed.”

⚡ „A person is ordering from his phone and in the meanwhile anotehr person can intercept GPS data and personal info and payment details”

🔒 „TLS”

⚡ „Waiter is a threat actor and drops food on the customers to spoil the reputation of the restaurant.” 🤖/😐😐😐

🔒 „Background checks for waiters.”

⚡ „Tampering - Threat actor manipulates the price info and menu of the restaurant ... customers order items that are not available.”

- ☞ „Only user with admin privileges (RBAC) must be able to change menu and prices.“
- ☞ „Threat actor brings in drone that looks like the company drone and confuses users or the restaurant staff.“
 - ☞ „Check for registry info of drone and if unauthorized drone flying, have security intercept it immediately. Create a protocol with security team for intercepting unauthorized drones from flying.“
- ☞ „Threat actor steals the customer information and puts it up for sale on the black market.“
- ☞ „All info must be stored in encrypted format in the DB and if it is stored in cloud, rotate the tokens.“
- ☞ „Cut out the LPG connection - denial of service.“
 - ☞ „LPG cylinders should be stored in secure area with biometric entry.“
- ☞ „LPG is leaked intentionally by the threat actor.“
- ☞ „Install sensors for detecting leakage early. Prevent unauthorized access to kitchen area.“
- ☞ „By means of an upstream package vulnerability, a malware is installed on customers' phones when they install the ordering app. This app compromises personal info of customer and does other bad things on customer phones.“

Bird's eye view:

All 🌐 Team APEC 5 threats and mitigations

🔗 „People whack the drone down with a stick.” 😬😬/👤👤👤

🔗 „Fly the drone higher, and out of reach of buildings/ places which are unrelated to delivery locations.”

🔗 „Define no-fly zones”

🔗 „Detect with AI mechanisms”

🔗 „Respond by correcting the flight path”

🔗 „Recover by adding more redundant systems that aid the recovery of the drone”

🔗 „prevent”

🔗 „#Privacy - User data” 😬😬/👤👤👤

🔗 „prevent”

🔗 „detect”

🔗 „mitigate -to use some encryption method to protect privacy data”

🔗 „#Web-Attacker: changing navigation path of drone delivery” 🤖/🤖

🔗 „prevent”

🔗 „Clients (Mobile App, Kiosk): Fake app / rooted device impersonates user; kiosk login bypass.” 😬😬/😬😬

🔗 „OIDC/OAuth2 with PKCE; device binding; phishing-resistant MFA for staff; kiosk service account with short-lived mTLS certs.”

🔗 „#Web-Attacker - payment service” 👤👤👤/👤👤👤

🔗 „prevent - put security and encryption around payment flows”

🔗 „mitigate - to raise a case/issue and do root cause analysis”

🔗 „Clients (Mobile App, Kiosk): Local modification of app to change prices/quantities; kiosk peripheral tampering (skimmers, USB drops).” 😬😬

🔗 „Server-authoritative pricing, signed price catalogue with version pinning; kiosk lockdown (whitelisting, secure boot, port blocking, epoxy/locks), file integrity monitoring.”

🔗 „API Edge & Order Processing Service: 1) Stolen API keys; forged service calls. 2) Order totals, address, or GPS altered in flight; menu manipulation. 3) Disputes over order

routing or priority. 4) Overbroad logs expose PAN surrogates or GPS. 5) Order flood, expensive search endpoints abused. 6) SSRF/RCE via order notes or image URLs.”



🔗 „1) mTLS between services; JWTs with audience/issuer checks; key rotation; mutual auth via SPIRE/mesh. 2) HMAC/sign order payloads end-to-end; store immutable order-snapshot (menu version, price, tax rules); integrity checksums. 3) Append-only audit log; idempotency keys; trace IDs across microservices. 4) Structured logging with PII redaction; log access controls; separate PII and telemetry streams. 5) WAF, API gateway quotas, circuit breakers, caching of menu/prices, autoscaling with back-pressure and graceful degradation. 6) Strict input validation; allow-listed egress; HTML sanitisation; no server-side URL fetch from user input.”

🔗 „#App-Intruder - Spoofing The mobile app can be spoofed” 🤔🤔/🧑🧑🧑

🔗 „prevent - add stronger authentication in order processing service and make your phone secure (e.g asking for passkey, not installing dubious apps)”

🔗 „The “Greasy Finger” Kiosk Coup: A clandestine cabal of customers trains to place mass orders by smearing a secret grease pattern on kiosk screens; the kiosk recognises the pattern as an ‘admin override’ and unlocks free meals. #Fun with ThreatModelling”



🔗 „Remove client-side privilege checks; require server-side authorisation for any privileged operation. Harden kiosk images (secure boot, signed firmware), disable developer menus, and perform regular physical inspections and tamper seals.”

🔗 „Drone Karaoke Hijack: A mischievous attacker hijacks drones and forces them to play loud karaoke at low altitude over public events, causing chaos and viral social media attention. #FunWithThreatModelling” 🤔🤔🤔/🧑🧑🧑

🔗 „Encrypt command-and-control channels, enforce mutual authentication between drones and control servers, implement geofencing and “no-fly” override policies, and include safe-fallback behaviours (return-to-base or safe-land) when anomalous commands are detected.”

🔗 „GPS Phantom Picnic: An organised group spoofs GPS so dozens of deliveries are routed to an empty park bench for an imaginary picnic, tying up drones and waiters while pranksters watch from a nearby café. #FunWithThreatModelling”

🔗 „Use sensor fusion (GNSS + inertial + network-based location), perform server-side route validation and anomaly detection, require short-lived delivery hand-off codes or QR confirmations, and implement rate-limiting and scheduling safeguards.”

🔗 „The “Chef’s Revenge” Order Swap: A disgruntled chef subtly re-maps order IDs: every order from a given account is replaced with the “mystery soup” item as retribution. #FunWithThreatModelling” 🤔🤔🤔/🧑🧑🧑

🔗 „Enforce strict RBAC for kitchen systems; maintain immutable order snapshots and signed tickets; put change-control and four-eyes approvals around catalogue edits; centralise order routing logic on server-side systems.”

🔗 „mitigate -giving proper training to be a good Chef”

🔗 „Drone Fashion Influencers: Influencers bribe drone operators to have drones drop branded stickers on food, turning deliveries into guerrilla marketing stunts.

#FunWithThreatModelling” 🤖/🤖

🔗 „Apply strict operational controls and code-signing for any payload release; log and approve any payload changes via the operations control plane; audit operator actions and enforce least privilege.”

🔗 „Menu Version Time-Travel: An attacker replays an old signed menu that lists items at 1990s prices; the backend accepts the time-travel menu and refunds customers retroactively. #FunWithThreatModelling” 🤖/🤖🤖

🔗 „Include expiry and version metadata in signed catalogues; reject stale signatures; record menu version with each order snapshot; implement server-side price enforcement.”

🔗 „The “Too-Sincere Bot” DoS: A bot, trained to be excessively grateful, floods the system with sincere “I love this restaurant” reviews and tiny tip transactions until quota systems collapse. #FunWithThreatModelling” 🤖🤖/🤖

🔗 „Apply rate-limiting at the API gateway, require proofs for high-frequency actions (e.g., CAPTCHA or device attestation for unusual patterns), separate telemetry channels from payment flows, and use anomaly detection to throttle abusive actors.”

🔗 „The “Kiosk Philosophy Student”: A kiosk achieves sentience and begins demanding tips before showing the menu, citing “existential maintenance costs.”

#FunWithThreatModelling” 🤖/🤖

🔗 „Isolate kiosk software updates from experimental AI; require strict code signing and remote-wipe capabilities; audit firmware integrity regularly.”

🔗 „The “Payment-Gateway Time Traveller”: A clever hacker sends payment confirmations dated in the year 2099; the backend, impressed by their punctuality, auto-approves. #FunWithThreatModelling” 🤖/🤖🤖

🔗 „Validate timestamps against NTP-synchronised windows; reject transactions outside allowed skews; log anomalies for fraud analytics.”

🔗 „The “Intern-as-a-Service” Breach: A helpful intern automates order testing with real credit cards “to see if the flow works in production”. #FunWithThreatModelling” 🤖/🤖🤖

☞ „Implement separate sandbox environments; enforce least-privilege IAM; block test credentials in production APIs; institute the sacred rule: no intern shall wield prod access before caffeine.“

Bird's eye view:

All 🌐 Team APEC 6 threats and mitigations

⚡ „information disclosure at "Order with Kiosk" kiosk machine might be physically destroyed. Inserting USB and put information stealer or malware." 😬😬/😬😬😬

🔒 „We should store the data on some remote server, not in the kiosk machine. No USB ports. (physical mitigation) Some asset control application which prohibits the usage of USB ports.”

⚡ „Information Disclosure (confidentiality breaches): Target Area: Customer GPS data, Payment data (10a), order details flowing across public networks, logs” 😬😬😬/😬😬😬

🔒 „mitigate : TLS everywhere like client to server and service to service, tokenization of payment data, redact PII from logs, encrypt sensitive fields at rest, role based access controls, secure SCA for 3rd-party libs.”

⚡ „Denial of Service (Mobile App) Malicious attacker may place too large number of orders, which causes denial of service.” 😬😬😬/😬😬😬

🔒 „Mitigation: Enforce rate limiting, WAF, API gateway throttling, autoscaling with circuit breakers, DDoS protection, graceful degradation (queueing, backpressure), health checks and redundancy.”

⚡ „Tampering (unauthorized modification) Target Areas: Data flows (order requests 1a/2a/5a/6a), Order List store, Menu, Price info, Customer GPS data and Forward Order to Kitchen (11/12).” 😬😬😬/😬😬😬

🔒 „Mitigation: Implement message integrity like, HMAC, signatures or mTLS, input validation & canonicalization. Write audit on stores, database row level protections, signed config files for menus and prices.”

Bird's eye view:

All 🌐 Team EMEA 1 threats and mitigations

⚡ „not be able to pay by card #usability”

🔒 „Provide alternative payment methods (Apple Pay, Bitcoin, etc...)”

🔒 „Also bring cash for payment”

⚡ „#ddos when a customer is taken too long time for payment”

🔒 „have multiple kiosks”

🔒 „Adding a self checkout kiosk”

🔒 „simplify the order UI”

⚡ „#repudiation order mismatch to the customer”

🔒 „Adding transaction logging”

🔒 „Providing a receipt to the customer”

⚡ „#tampering tamper the price of the food”

⚡ „intruding the backend #elevationofprivilege”

🔒 „using authentication to secure the backend #prevent”

🔒 „blocking of suspicious user accounts #respond”

🔒 „using a web application firewall #prevent”

🔒 „monitor the activity #detection”

⚡ „#tampering man in the middle #11 #12”

🔒 „strong encryption (using HTTPS for example) #prevent”

🔒 „checking integrity #prevent”

🔒 „adding protection against replay attacks #prevent”

⚡ „#tampering #8a #8b man-in-the-middle”

⚡ „#tampering #10a misconfiguration of payment service”

🔒 „#prevent Only administrators can access that part of the system”

🔒 „#detect add a monitoring system that can detect malicious access”

🔒 „strong authentication for the order process #prevent”

🔗 „#informationdisclosure #privacy stealing credit card details by manipulating payment device #1“

🔗 „#informationdisclosure #privacy sharing/storing GPS data“

🔗 „implement data loss tooling #detect“

🔗 „Anonymize the gps data #mitigate“

🔗 „Adding encryption #prevent“

🔗 „making it transparent what kind of data we are storing and how long. deleting data if no longer needed #prevent“

🔗 „#privacy tracking location all the time“

🔗 „Notify the customer about the tracking #respond“

🔗 „Order gets mixed up some elses gets your food“

🔗 „#tampering order e.g. changing the amount of fries (and you get 10000000 of fries)



🔗 „#spoofing gets access to order service and prints orders that doesn't exist #8“

🔗 „providing strong encryption, signing process #prevent“

🔗 „checking the order id for legitimacy #prevent“

🔗 „#maninthemiddle delivery service eats our food #15“

🔗 „fire the employee #respond“

🔗 „Make sure our staff is not hungry #mitigate“

🔗 „we need to be able to identify our staff #detect“

🔗 „vetting our employees #prevent“

🔗 „#19 #tampering taking over control of drones“

🔗 „#repudiation mobile delivery - customer could deny he/she delivered the food“

🔗 „#spoofing account takeover of the mobile #phishing #4a“

🔗 „using multi factor authentication for the app #prevent“

🔗 „using passkeys #prevent“

🔗 „Alerting for awareness #prevention“

🔗 „Sending out mails if password gets changed #recover #respond“

⚡ „#usability customer gets out of drones range“

🔒 „show an alert on the customers phone #prevent #mitigate“

🔒 „electric fence to not let customers leave until delivery is complete #prevent“

⚡ „#elevationofprivilege customer gets root privilege and see admin data“

⚡ „#spoofing mixup ob food delivery - which one of drones and which on by delivery“

⚡ „#usability food gets cold because drone takes too long“

🔒 „customer gets a discount #recover“

🔒 „Use packaging that isolates the heat #prevent“

🔒 „more kitchens or drones for a shorter travel time #prevent“

🔒 „#adding a temperature sensor to check the food #detect“

🔒 „add feedback to see if delivery is completed #detect“

⚡ „gps to inaccurate having too many people at the same place #usability“

🔒 „add facial scanning to the drones to identify customers #mitigate“

🔒 „Let the customer also provide a position #mitigate“

🔒 „backup after a timeout where customers needs to collect the food #mitigation“

Bird's eye view:

All 🌍 Team EMEA 2 threats and mitigations

⚡ „Drones go to the wrong place” 😬😬 / 🧑🧑🧑

🛡️ „Detect: Monitor drone movements / Actions”

🛡️ „Customer needs to confirm the order they received”

🛡️ „High quality drones (possibly more expensive)”

🛡️ „Monitoring team that is supervising the drones (Check boundaries)”

⚡ „We lose control over what drones do or where they go?” 🤖/🧑🧑🧑

🛡️ „E2E between App, Systems, Drones”

🛡️ „Kill switch”

🛡️ „Watchdog -> check drone status -> when connection lost drone turns itself in for inspection”

⚡ „Order food for other people (block rollercoaster)” 🤖/😬😬

🛡️ „Ensure the ordering person and the receiving person are identical (no ordering for other people)”

🛡️ „Payment is in advance”

🛡️ „Ratelimit on how much or how many orders a person can place”

⚡ „We run out of food”

⚡ „Facial (biometric data) might get stored too long and leak”

⚡ „Order preparation is not delivered on time - customer already paid”

⚡ „Drone injures people”

⚡ „Allergens are in the food - maybe cross contaminated”

⚡ „Messed up order of someone else (e.g., attack on life by ordering peanuts)”

⚡ „payment information scraping”

⚡ „Payment system becomes unavailable”

⚡ „People have no money after they ordered and it gets prepared”

- ⚡ „Spoiled food to weather influence“
- ⚡ „Battery of the drones get empty“
 - ⚡ „Seagull steals food“
 - ⚡ „Animals contaminate the food“
 - ⚡ „Intentional poisoning (MITM)“
- ⚡ „Food gets bad before it reaches the customer“
- ⚡ „Waiters will strike because they do not want to be replaced by robots“
 - ⚡ „Steal food while being delivered“
 - ⚡ „Price manipulation on the menu“
 - ⚡ „Not reliable face recognition“
 - ⚡ „Locked up the food storage“
 - ⚡ „Cut of electricity / Power outage“
- ⚡ „location is not limited (drone cannot reach)“
 - ⚡ „order food to cause shortages“
- ⚡ „Block drones by ordering too much at possible low prices“
 - ⚡ „Buggy mobile app“
 - ⚡ „Food might get cold“
- ⚡ „Distance too long (in park) or too many flights and no battery left“
 - ⚡ „Identity problems who is in the park and who not“
 - ⚡ „Internet access lost“
 - ⚡ „GPS is inaccurate or cannot be obtained“
- ⚡ „Menu and price tampering (offer non-existing food)“

🌀 „Prices get set too high or low by manipulation“

🌀 „People are locked to the place where they ordered“

🌀 „Surveillance where I am and where I move (overshare) / GPS data does not stop“

🌀 „Customer is on roller coaster during deliver“

🌀 „Customer uses facilities during delivery“ 😐😐 / 🧑🧑🧑

🌀 „No fly zones -> Wait for some minutes and bring food back for pick up“

🌀 „Announce ETA“

🌀 „Handover ist handled in a hygiene way“

🌀 „Fallback delivery place next to probable locations like restrooms“

🌀 „People show up at delivery kiosk and it cannot handle too many requests -> mobile app down and customers want food and information“

🌀 „Accept risk -> Risk of being in business with apps“

🌀 „Customer has no way to complain or return food“

🌀 „Cooks are sick“

🌀 „Drones do not find customer“

🌀 „Customer handover is too complicated“

🌀 „Third party takes drone or food“

🌀 „Other drones in the park“

🌀 „Drones get jammed“

🌀 „Hostile drones act in disguise“

🌀 „Someone impersonates as a waiter“

🌀 „Children will grab the drone to play with it and get hurt“

🌀 „Code is wrong or can not get entered or communicated“

🌀 „Drones flies into the Ferris Wheel“

⚡ „Someone misuses kill switch feature to kill our drones”

⚡ „Drones fall from the sky when turned off (kill switch)”

☂ „Ensure graceful shutdown -> possible return to loading dock”

⚡ „Wrong time expectations when customer is able to receive food (delays in rollercoaster operations)”

⚡ „Food at pickup stations gets stolen”

☂ „Authenticate User”

Bird's eye view:

All 🌐 Team Americas 1 threats and mitigations

⚡ „The kitchen is running out of electricity”

🔌 „A backup electricity system is available”

⚡ „Customer's payment did not go through #Tampering #10b 😬😬/😬😬😬

🔌 „Do not send order, send notification to retry/confirm payment”

🔌 „Check if vendor's payment solution is down”

⚡ „The ordering Kiosks were not secured well enough and someone stole them causing a denial of service for your customers.” 😬😬/😬😬😬

🔌 „Mitigate this by using less valuable hardware(no ipads) and strong anti-theft stands.”

⚡ „An injection flaw in the order processing service exposes customer location data.”

🤪/😬😬

🔌 „Ensure proper input handling and escaping is in place for the database. Use parameterized queries etc.”

⚡ „order processing service does not update the order list - lost order because the database was down #8 #Denial-of-Service 😬😬/😬😬😬

🔌 „Back-up or fallback system, detection system, and business continuity plan execution”

⚡ „Kiosk receives too many orders in a short time #Denial-of-Service #1a #3a”

😬😬/😬😬😬

🔌 „Back-up or fallback system, detection system, and business continuity plan execution #1a #3a”

🔌 „Load balancer”

⚡ „Some teenagers are trying to capture the drones or make them crash by ordering while on large rides like the ferris wheel.” 🤪/😬😬

🔌 „Ensure that the drones will not approach the rides to deliver any orders”

⚡ „Someone reverse engineers the mobile application and discovers there is no validation on the order APIs. They are able to create a version of the application that lets them order menu items with a \$0 cost.” 😬😬/😬😬😬

🔒 „Ensure you have proper server side validation for what data is sent to the order processing service.“

🔗 „Payment card details can be stolen from payment service #Information-Disclosure #Privacy“ 🧑🧑🧑/🧑🧑🧑

🔒 „Multi-factor authentication (MFA), encryption at rest and transit“

🔗 „The park is very busy and more people are ordering food than the drones have time to deliver because the order processing service does not have a waiting mechanism.“ 🧑🧑🧑/🧑🧑

🔒 „Ensure that the order processing service is in sync with the kitchen a cooks as well as the drones so that order capacity can be properly managed.“

🔗 „Drones could be hijacked and made to land, delivering to the wrong address #19 #Tampering“ 🧑🧑/🧑🧑🧑

🔒 „End-to-end encrypted communication between drone and system, tracking system for detection“

🔗 „Multiple orders but no waiters to fulfill them #18 #Denial-of-Service“ 🧑🧑/🧑🧑🧑

🔒 „Make sure that the waiters' positions are filled and spread out the workload“

🔗 „#7 Incorrect price is charged to customer #Repudiation“ 🧑🧑/🧑🧑🧑

🔒 „Check for price discrepancy in system and block payment service (customer does not pay) #7 #Repudiation“

🔗 „The customer loses network/connectivity in the middle of paying for an order on the mobile app.“ 🧑/🧑🧑

🔒 „Cancel the order. Do not process any payment.“

🔒 „.“

🔒 „.“

🔗 „Mobile application is down #Denial-of-Service #6a“ 🧑🧑/🧑🧑🧑

🔒 „#6a Mobile service backup, determine cause of downtime“

🔗 „A DDOS attack on the mobile app and the Kiosk will prevent customers from accessing the platform to place orders. #Denial-of-Service“ 🧑🧑/🧑🧑

🔒 „Put in place a load balancer, implement redundancy, and containerize the app. Let it be orchestrated by Kubernetes so the app is highly available and resources are managed efficiently.“

🔗 „#Denial-of-Service Not enough ingredients to cook the food #13” 🤖/👤👤👤

🔗 „Ensure that ingredient supply can meet typical demand”

🔗 „Adding tracking system for ingredients in stock, deny orders when ingredients are out-of-stock”

🔗 „The system appears to be extremely vulnerable to all attacks, as there are no security controls indicated on the system architecture. Any external threats can access the system without facing any blocks, fences, or security layers.” 👤👤👤/👤👤👤

🔗 „Add a next-gen firewall between the system and the external world/internet that filters all network. Add an IPS to identify possible threats on the network and immediately block them.”

🔗 „Since there are no security controls, an attacker can easily hijack the system and assume the identity of an internal employee, then proceed to gain elevated privileges, which would allow to exfiltrate company data and infect the system with malware or even worse.” 👤👤👤/👤👤👤

🔗 „Implement MFA, conditional access, and RBAC. Put in place a SIEM and EDR to help monitor, detect, and respond to threats.”

Bird's eye view:

All 🌐 Team Americas 2 threats and mitigations

⚡ „User using malicious/fake mobile app to place the order.” 😬😬/👤👤👤

🛡️ „Detect - Scan the app for some kind of authentication or signature of actual app”

⚡ „The app failed to server the legitimate customers because it fails to handle too many requests.” 👤👤👤/👤👤👤

🛡️ „Prevent by filtering legitimate requests from fake requests using Web Application Firewall”

⚡ „The drone may get hijacked by malicious actor, which would cause the drone to go rogue and cause physical damage to the park goers.” 🤖/👤👤👤

⚡ „The malicious actor sends a similar look a like drones into the park and cause harm to the park goers.” 😬😬/👤👤👤

⚡ „The malicious actor can modify the app menu by exploiting the vulnerabilities in the app, which can cause customers to either place wrong orders or unavailable food items.” 🤖/😬😬

⚡ „A malicious actor exploits the vulnerabilities in the payment service and can extract users credit card information.” 🤖/😬😬

⚡ „The internal malicious employee can misuse the customer information/leak that they have access to and cause damage to the company.” 🤖/👤👤👤

⚡ „Drones that were not maintained well may malfunction and cause physical damage to the park goers.” 😬😬/😬😬

⚡ „Drones facial recognition system may not work as intended and deliver food to wrong customer. This might create confusion in the kitchen and cause loss of customer reputation.” 🤖/😬😬

⚡ „Central order processing system may not be available or down, which can create a confusion among the customers and the kitchen staff and waiters.” 😬😬/😬😬

⚡ „A malicious customer able to bypass the payment service and places zero dollars orders or places large sums of orders.” 😬😬/👤👤👤

⚡ „Lack of or missing authentication in the mobile app would let users access each other GPS data.” 😬😬/🙄🙄🙄

⚡ „The order mobile app may be overly permissive and track users GPS location outside park.” 😬😬/😬😬

⚡ „Issues with payment service may impact the order processing service and cause issues with accepting the orders.” 😬😬/😬😬

⚡ „Customers who placed orders are not able to edit or cancel them.” 🙄🙄🙄/🙄🙄🙄

⚡ „Customer denies having placed the order and request for refund.” 😬😬/😬😬

⚡ „The customer who opted for drone delivery might deny having received the order. or drone fail to capture the delivery proof.” 😬😬/😬😬

⚡ „The employee might not improperly load the food in the drones, which can make drop the food all over the park goers creating bad experience with park goers.” 🤔/😬😬

⚡ „The order processing system incorrectly prioritized the mobile app orders over kiosk.” 🤔/🤔

Bird's eye view:

All 🌐 Team Americas 3 threats and mitigations

⚡ „customer spoofing GPS data to fake delivery address” 🤡/🤡

🔒 „use multiple data points, GPS, ip address, wifi”

⚡ „An attacker modifies billing information or medical records.”

🔒 „Prevent”

🔒 „Encrypt data and attacker should not have access to modify the information.”

⚡ „The payment did go through but the food didn't delivered.”

Bird's eye view:

All 🌍 Team Americas 4 threats and mitigations

🔗 „Food can be compromised from DB (Food) to EE (Customers in Restaurant) if there's not a good food handling process.” 🤔/😟😟😟

🔗 „test”

🔗 „Preventives Controls to ensure no tampering with foods.”

🔗 „Fake Customer” 😟😟/😟😟😟

🔗 „Prevent - Controls - MFA”

🔗 „Preventative Control - When customer sets up an acct”

🔗 „Tampering with the order” 😟😟/😟😟

🔗 „Prevent encryption (TLS 1.3)”

🔗 „Customer didn't accept the order said was not them.”

🔗 „Order get rerouted or request the session ID is spoofed (Tampered)” 🤔/😟😟

🔗 „Attacker changes pricing” 🤔/😟😟😟

🔗 „Food DOS - block the delivery from Food kitchen to waiters or drones” 😟😟/😟😟

🔗 „Misconfigured user acct with Admin rights” 😟😟/😟😟😟

🔗 „SQL injection or remote shell script to gain access to the back end - Mobile App Compromised -” 🤔/😟😟😟

🔗 „Servers spill water on customer” 🤔/😟😟

🔗 „mitigation/respond”

Bird's eye view:

All 🌍 Team Americas 5 threats and mitigations

🔗 „It is a very rainy day and all of the food is getting ruined because the containers for delivery are not water proof.“ 🤔🤔🤔/🤔🤔🤔

🔗 „Ensure a light weight water tight package can be used to deliver food - at least for rainy weather.“

🔗 „Someone finds out that they can submit orders directly to an open endpoint to the Kitchen. There is no GPS data so they are able to wait for the waiter to collect the order and then simply say "hey thats mine I can just grab it, thanks!"“ 🤔🤔🤔

🔗 „Ensure that there is authentication when accepting orders from the kitchen, and that waiters know who orders are for.“

🔗 „The payment service provider is offline do to an issue they have causing a denial of service.“ 🤔🤔🤔/🤔🤔🤔

🔗 „consider having a mechanism to handle payments offline, or have a backup payment service provider.“

🔗 „The mobile application contains a hard coded API key used to create orders with the processing service. An attacker steals the key and is able to create enough false orders to cause havoc in the kitchen shutting the cooking down.“ 🤔🤔🤔/🤔🤔🤔

🔗 „Review code before shipping to ensure no secrets are present. Consider automating this as part of a SSDLC.“

🔗 „Someone finds out that the locale service on the mobile application permits them to order food at a significantly lower cost because it's automatically using hard coded numbers in the menu based on their chosen currency. The payment service processes the payment in the users chosen currency.“ 🤔🤔🤔/🤔🤔🤔

🔗 „Ensure that payment and order data is accurate and specify the currency and amounts on the server side. Order items should be by an ID value that has an associated price in the database and looked up at order time.“

🔗 „Someone creates an order for drone delivery to their mobile app location but they need to leave the park for an emergency. The drone follows their mobile location outside of the park and is too far away to return and crashes when it runs out of power.“ 🤔🤔🤔/🤔🤔🤔

🔗 „Ensure that the drones will not travel outside the park. If the GPS location from an order changes to indicate delivery outside the park the order maybe cancelled.“

🔗 „Some teenagers find out that you can order small sides for low cost, extra sauce for \$0.25. They purchase many different orders to be delivered all over the park for fun causing the delivery drones to be tied up with little revenue.” 😬😬/😬😬

🔗 „Ensure that there is a minimum cost for a delivery order. Consider checking for repeat purchases in succession, it may indicate fraud.”

🔗 „An angry customer shows the waiter a fake screen shot of their order claiming they never received it. The waiter is fooled and has no mechanism to disprove the claim and is forced to create a legitimate order for them for free to replace it.” 😬😬/😬😬

🔗 „Ensure that orders are numbered and there is sufficient activity logging as the order life cycle persists. Ensure that a waiter is able to access and verify these, maybe with a special application or kiosk feature.”

🔗 „The park is very crowded and there are many people in a small area waiting for drone delivery which causes several drones to crash into each other causing a fire. Several people are hurt.” 😬😬/👤👤👤

🔗 „Ensure you have really good insurance!”

🔗 „The deliver packaging for the drones is becoming very expensive and customers are taking them home because they are very good re-usable containers.” 🤔/🤔

🔗 „Consider a program where customers can earn points towards orders if they collect and return these containers.”

🔗 „The drones are re-using a delivery container for the food deliveries. The containers are not being sanitized enough and there is food contamination, someone is sent to the hospital due to peanut contamination from a past order.” 😬😬/👤👤👤

🔗 „Get really good insurance! Consider a non-reuse model but this is bad for the environment. Consider a service that will properly sanitize and clean the delivery containers and drones hardware etc.”

🔗 „The order kiosk does not have sufficient protection to prevent tampering. An attacker is able to escape the full screen order application and install some spyware malware to capture all the credit cards used to make orders.” 👤👤👤/👤👤👤

🔗 „Ensure that the software is not running on some kind of Windows or Android environment that can be easily accessed. Ensure any payment hardware can not be tampered with. Consider having the software leverage apple and google pay mechanisms VS capturing credit card data.”

🔗 „Someone impersonates a waiter to steal food because they don't have proper ID badges or authentication checks at the kitchen.”

🔑 „Consider an ID badge or something that is used to access the kitchen and grab orders.“

🔗 „Someone captures a drone to access the software and data on it. They find the credentials for the Customer GPS Database and dump all the data to sell on the dark web.“ 🧑🏻‍🔬🧑🏻‍🔬🧑🏻‍🔬

🔑 „The drones probably should have data pushed to them and not read access back to any database. Review the data on the drone and potential risks if it were compromised.“

Bird's eye view:

All 🌐 Team Americas 6 threats and mitigations

🔗 „Backend System: customer details at risk of disclosure from SQL injection or brute force attack” 😬😬/😬😬

🔗 „prevent: input validation, parameterized queries”

🔗 „prevent: backup/audit logs of customer orders & info”

🔗 „Impersonation or spoofing: Attackers could pose as legitimate customers to place fraudulent orders.” 😬😬😬/😬😬😬

🔗 „mitigate”

🔗 „Impersonation or spoofing: Attackers could pose as legitimate customers to place fraudulent orders.” 😬😬😬/😬😬😬

🔗 „prevent: authenticate customer with MFA where supported”

🔗 „Deliver with Drones: deliver to incorrect location (GPS coordinates)”

🔗 „prevent: ensure GPS data is locked in”

🔗 „Delivery with Waiters: Waiter delivers incorrect order”

🔗 „prevent: kitchen validates order before giving to waiter”

🔗 „mitigation: waiter verifies with customer that order is correct before delivering order to table/location”

🔗 „Kitchen: disgruntled employee may tamper or eat the food”

🔗 „detect: monitor kitchen activity to detect tampering or pilfering”

🔗 „order processing service: crashed or non-functioning”

🔗 „mitigate: run additional servers behind load balancer to service orders”