DREXEL UNIVERSITY

CeruleanSOC

AI Triage Copilot for SecOps Shared Inboxes

TEAM 6
Senior Design Project
Drexel University

AWS-Hosted · SOP-Grounded · Outlook-Integrated · Human-Review Controlled

THE PROBLEM

Security and IT teams rely on shared inboxes for a wide variety of user-reported issues. These messages arrive in unstructured language, mix high-risk events with routine requests, and require manual triage, research, response, and documentation.

- High email volume
- Inconsistent triage
- Slow response time
- Manual SOP lookup
- Limited auditability
- Delayed escalation

OUR SOLUTION

CeruleanSOC automates and augments the triage process using AI and your organization's SOPs. It classifies incoming messages, retrieves the right guidance, assigns severity, and generates professional responses—while keeping humans in control.

BEFORE	AFTER
Inbox	AI Reads & Understands
Manual Review	Retrieves Relevant SOPs
Analyst Judgment	Classifies & Prioritizes
SOP Lookup	Drafts Response
Draft Response	Logs & Documents
Update Records	Human Review (if needed) or Send

WHAT WE BUILT

- AWS-hosted n8n instance live over HTTPS
- Outlook trigger connected via Graph API
- SOP PDF upload & processing workflow
- Qdrant vector knowledge base populated
- Postgres triage logging & decision tracking
- AI classification & severity assignment
- Professional response generation
- Conditional draft or send workflow
- Full audit trail & traceability
- Network access restricted to Drexel/VPN ranges

HOW IT WORKS

1. **Outlook Inbox Trigger** — New emails in the shared inbox are automatically detected.
2. **n8n Workflow Automation** — The workflow orchestrates each step of the triage process.
3. **Normalize Email** — The email content is cleaned, structured, and prepared for analysis.
4. **Postgres Event Logging** — Incoming message metadata is securely stored for tracking and auditability.
5. **AI Agent** — The agent analyzes the message using retrieved SOP knowledge.

- **AWS Bedrock (LLM)** — Generates reasoning & response
- **Qdrant (Vector DB)** — Retrieves relevant SOP content
- **Titan Embeddings (Amazon)** — Converts SOPs into vectors

6. **Normalize Agent Output** — The response is structured with classification and recommended action.
7. **Approval Check** — The system evaluates the decision and determines the best next step.
8. **Postgres Decision Update** — Triage decision, severity, and response are stored for full traceability.
9. **Outlook Response** — A draft is created for review or the response is sent automatically.

CONTROLLED AUTOMATION

CeruleanSOC is designed for safe, human-centered automation.

AI Generates Decision & Response — The agent produces a recommended action with reasoning.

→ **Human in the Loop When Needed** — Analysts review drafts for sensitive or unclear cases.

→ **Send or Escalate Automatically** — Confident, routine responses are sent, saving time and effort.

The right balance of speed, consistency, and security.

KNOWLEDGE-GROUNDED TRIAGE

SOPs are uploaded, embedded, and stored in a vector database. The agent retrieves the most relevant guidance during triage so responses are accurate, consistent, and grounded in your organization's procedures.

SOP PDFs & Documents → Titan Embeddings (Amazon) → Qdrant (Vector Database)

Sample SOP Categories

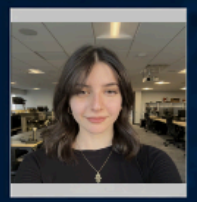
- Phishing Reports
- Suspicious Logins
- MFA / Auth Issues
- Password Resets
- Malware & Links
- Vendor Notices
- Access Requests
- General Questions
- Misrouted / Other
- Unknown / Needs Review

TECHNICAL ARCHITECTURE

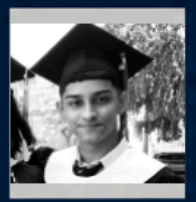
Application Layer	n8n Workflow Automation · Microsoft Outlook (Trigger & Response)
Data Layer	Postgres (Triage Events & Decisions) · Qdrant (Vector Database)
AI Layer	AWS Bedrock (LLM) · Titan Embeddings (Amazon) · Model Fallbacks (Premium / Nova Pro)
Infrastructure Layer	AWS EC2 (Compute) · Docker Compose (Containers) · Caddy (HTTPS Reverse Proxy)

Deployed on AWS · Secured · Drexel / VPN Access Only

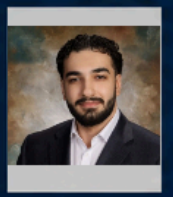
MEET TEAM 6



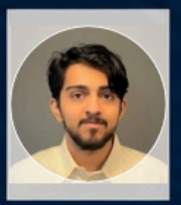
Dina Gordon
QA Engineer
Builds documentation, manages GitLab, and ensures quality and traceability.



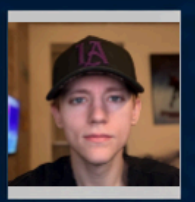
Ariyan Karim
Identity Engineer
Manages Microsoft Entra ID and Graph API integration for secure Outlook connectivity.



Zach Nashi
Product Owner
Leads product direction and project strategy with expertise in security operations and AI.



Dylan Patel
Automation Engineer
Builds and maintains the n8n workflows and AWS Docker-based infrastructure.



Michael Trent
Data Engineer
Develops SOP content and RAG pipelines with Qdrant and embedding technologies.