



OCTOPUS

ENCOMPASS

關鍵性基礎建設保護

挑戰

如今關鍵性基礎設施必須同時管理複雜的設施、有限的資源、還需符合政府機構、處理越來越多的不同技術，同時為客戶提供高水準的服務、處理不安定事件，如恐怖主義、犯罪、網路攻擊、出乎意料的天氣事件和系統故障。在發生緊急情況下，關鍵性設施必須保持業務連續性和迅速解決事件以便儘快恢復正常操作。

- 運營成本高
- 難以驅散威脅
- 風險處置不當
- 無數據分析和交叉引用
- 與員工無交流
- 不同部門之間無同步性



導致事件管理效率低下且不符合規定



OCTOPUS
control and command

解決方案 | OCTOPUS ENCOMPASS

- **ENCOMPASS** 一個全新全面的關鍵性基礎設施保護解決方案，使安全、保密、互聯網管理和操作平臺等合為一體，為迎接新時代籌備你的組織。
- 一個接收來自複合源、相關資訊的所有事件和威脅的工具，其利用先進分析方法展現真實的情境圖。
- 簡單的配置程式、派遣力量、從使用者介面控制所有組織的系統。
- 通過專用手機應用程式與員工/訂閱者進行雙向溝通。



OCTOPUS ENCOMPASS | 綜述



- **OCTOPUS ENCOMPASS** 是為了安全與安全監測、應急調度和關鍵性基礎設施管理而研發的。
- **OCTOPUS ENCOMPASS** 是雲啟用並自帶接收資料、事件、視頻和外部威脅的中央指揮中心，與手機應用程式共同為實現與訂閱者的雙向交流而服務。
- **OCTOPUS ENCOMPASS** 為恐慌信號和事件報告提供了求救移動應用程式——“人體感測器”。
- **OCTOPUS ENCOMPASS** 帶有運行安全操作所需的所有模組——集成安全、電腦輔助調度(CAD)、應急程式部署、情報分析、路線和任務派遣、緊急呼叫、以及艦隊和武器監控。
- **OCTOPUS ENCOMPASS** 允許常規管理，如巡邏、建築管理和操作風險管理。
- **OCTOPUS ENCOMPASS** 手機移動應用在運輸和緊急服務資訊、地圖和的興趣點上提供簡要資訊。
- **OCTOPUS ENCOMPASS** 系統已經過測試，現在正被安全與政府機構、大型企業應用，如化工和醫藥植物、multi cited製造商、銀行、政府和部門、安全機構等。該系統可以處理的感測器和用戶數量達到1000。

ENCOMPASS | 關鍵性基礎設施保護和監控

ENCOMPASS 連接所有組織的安全系統和關鍵基礎設施：

- 安全檢測和監控
- 安全的感覺系統
- 房屋管理與基礎設施
- 資訊通信技術
- 能量和水分

ENCOMPASS 將會分析和關聯系統的所有資料並且高效協助應急情況和日常管理。

911 緊急情況

電力和公用事業

資訊通信技術

安全

民用基礎設施

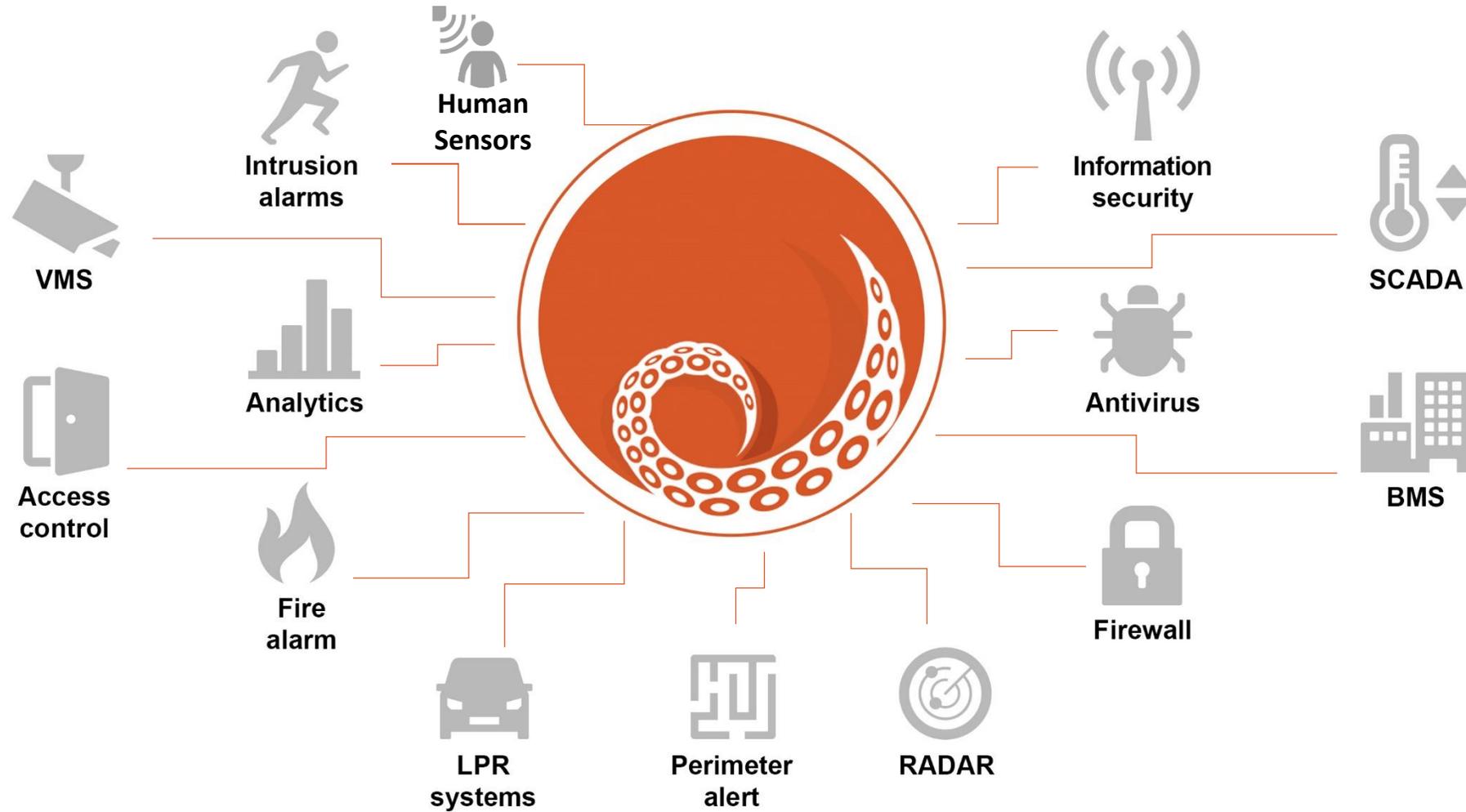
中水和污水

交通運輸安全



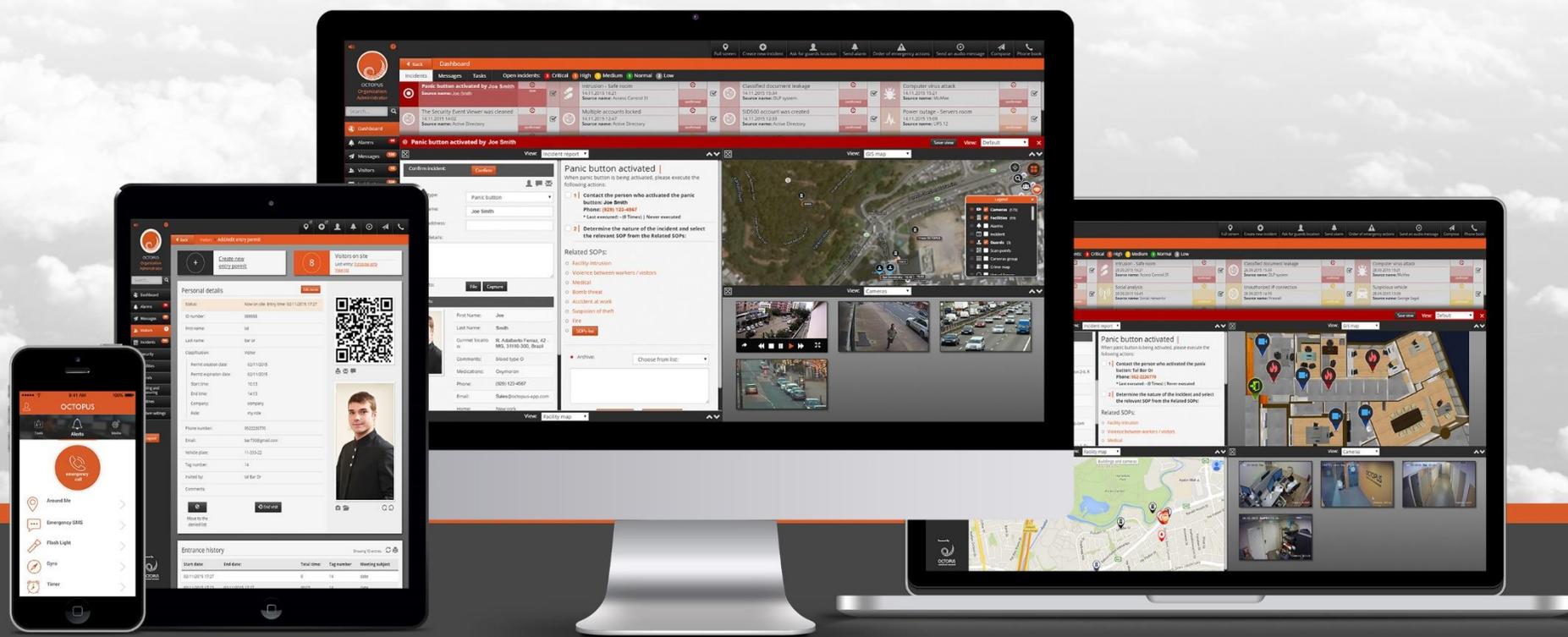
集成

聚集：所有組織的安全、互聯網技術和基礎設施資料系統的集成和介面，如：



突發事件管理

- **相關性**：系統分析和相關資料、事件和警報以確定實際情況和優先順序
- **驗證**：系統在清晰的常規操作畫面呈現了相關資訊
- **流動性**：可以在非固定崗位管理事件



危機管理協議和承諾

- 系統基於組織的政策和其他監管指南為處理緊急和常規事件提供標準操作程式(SOPs)。
- 系統自備關鍵性基礎設施的最佳實例
- 業務連續性和工作流過程可以基於要求自動操作或部署



威脅和情報

- 集成開源情報（OSINT），如：
 - 犯罪體系
 - 情報源
 - 社交媒體
 - 天氣系統
 - 車輛記錄和登記
 - 背景和篩選系統
- 事件管理期間的相關資訊
- 允許情報、威脅和風險的分析和管理的
- 通過Octopus手機應用程式、短信和電子郵件（集中通知）向安全部隊、員工/訂閱者傳播相關資訊。



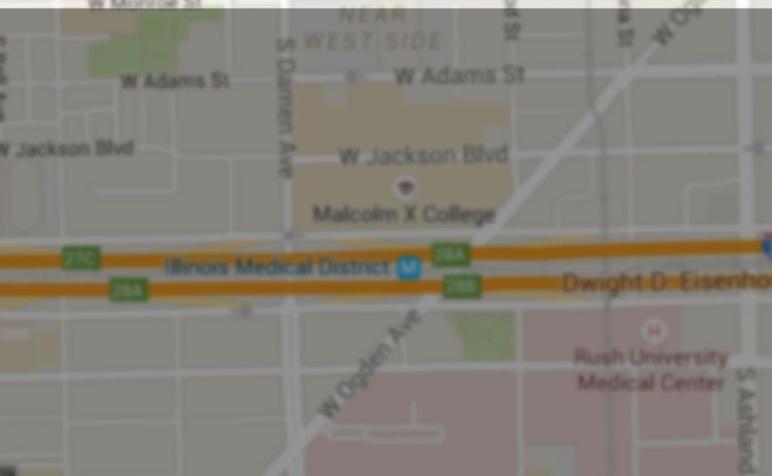
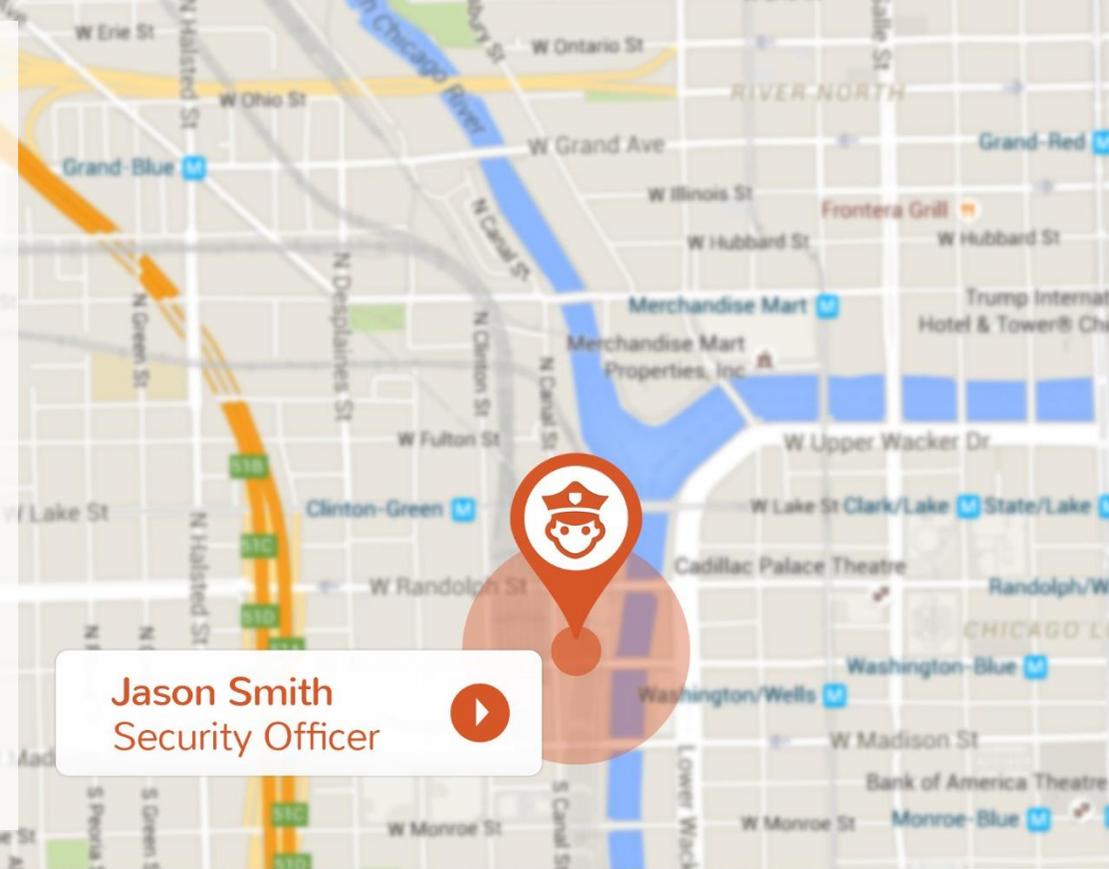
網路保護

關鍵性基礎設施基於更容易造成網路攻擊可以導致重大中斷操作的基礎設施實現更多的IP。

- **Octopus SIEM SOC** ——安全資訊事件管理和安全操作中心
- **Octopus基礎設施保護器** ——掃描和保護SCADA和IP設備使之免受駭客攻擊
- **Octopus手機衛士** ——保護員工的手機免受駭客和使代理白名單、黑名單和反欺騙
- **集成了網路保護、防病毒、IT和網路系統**
 - 域保護系統
 - 防病毒系統和代理
 - 防火牆和網路安全
 - 反惡意軟體和木馬
 - IT系統
- 網路事件管理的相關資訊
- 網路威脅和風險的分析和管理的

電腦輔助調度

- 系統對事件進行手動或自動派遣最近的應急單位
- 響應人員立即接收事件簡介：
 - 事件詳情
 - 照片和位置
 - 導航指示
- 指揮中心在GIS地圖上跟蹤緊急救援人員的位置
- 根據現場救援人員視覺的位置自動彈出相機視圖



常規巡邏路線

○ 車輛

- 系統可以根據對位置回應的最大時間和威脅預測等標準自動生成車輛巡邏路線。
- 定期更改路線以避免可預測性
- 車輛會被追蹤，並且如果他們偏離航線或停止太長時間時控制中心將會接到通知

○ 步行

- 為守衛掃描使用中的手機應用程式生成地理參照檢查點條碼
- 守衛可以接收檢查點任務和報告結果
- 如果檢查點無法按順序或準時掃描的話控制中心就會收到通知

Legend

- Cameras (9)
- Facilities (16)
- Alarms (181)
- Incident
- Guards (0)
- Scan points
- Cameras group
- Crime map
- Virtual fences (24)

應急通信集成

跨部門應急通信和
品質通知：

- 本地手機程式
- PTT廣播
- 網路語音電話業務
- 陸上通信線
- 行動電話
- 衛星
- 短信
- 電子郵件
- 電子留言板
- 公告



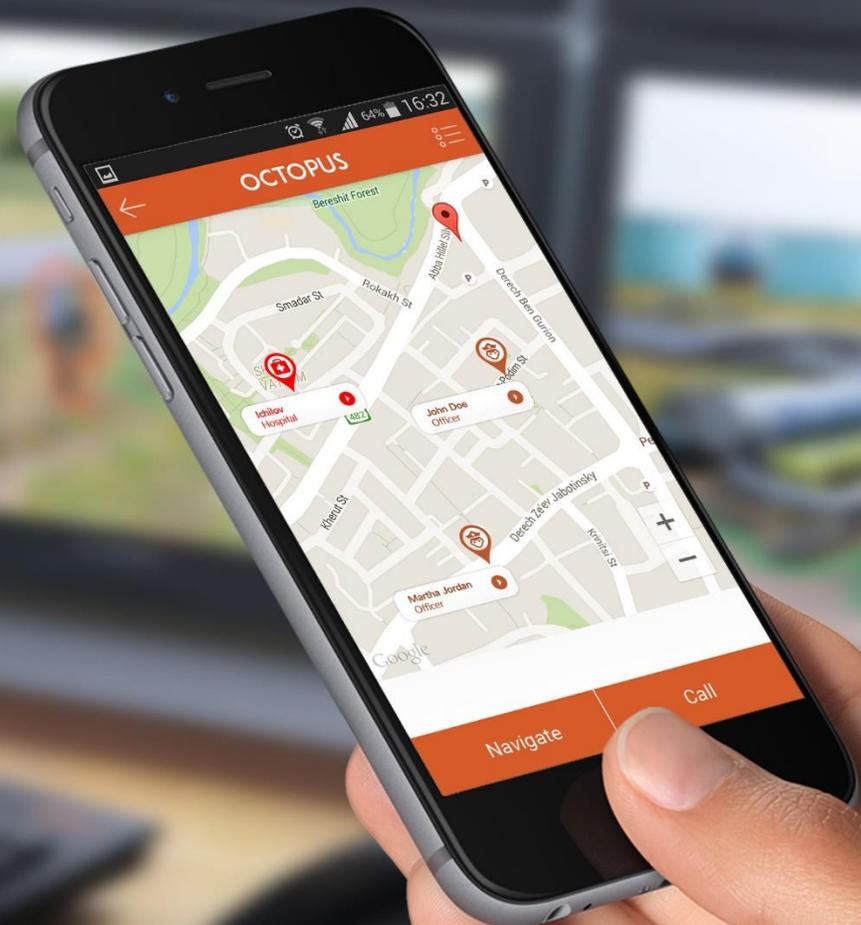
手機應用程式——綜述

- OCTOPUS手機應用程式連接組織中的所有人，在緊急事件中能節省寶貴時間
- 功能特點：
 - GIS位置基礎應急開關
 - 可以發送和接收文本、圖片、音訊和視頻的位置基礎資訊系統——品質通知
 - PA / IP手機
 - 即時視頻傳輸
 - 我周圍——GIS位置基礎模組顯示使用者預先確定的設施和他所在位置周圍的重要點
 - 安全部隊追蹤
 - 緊急短訊服務模組



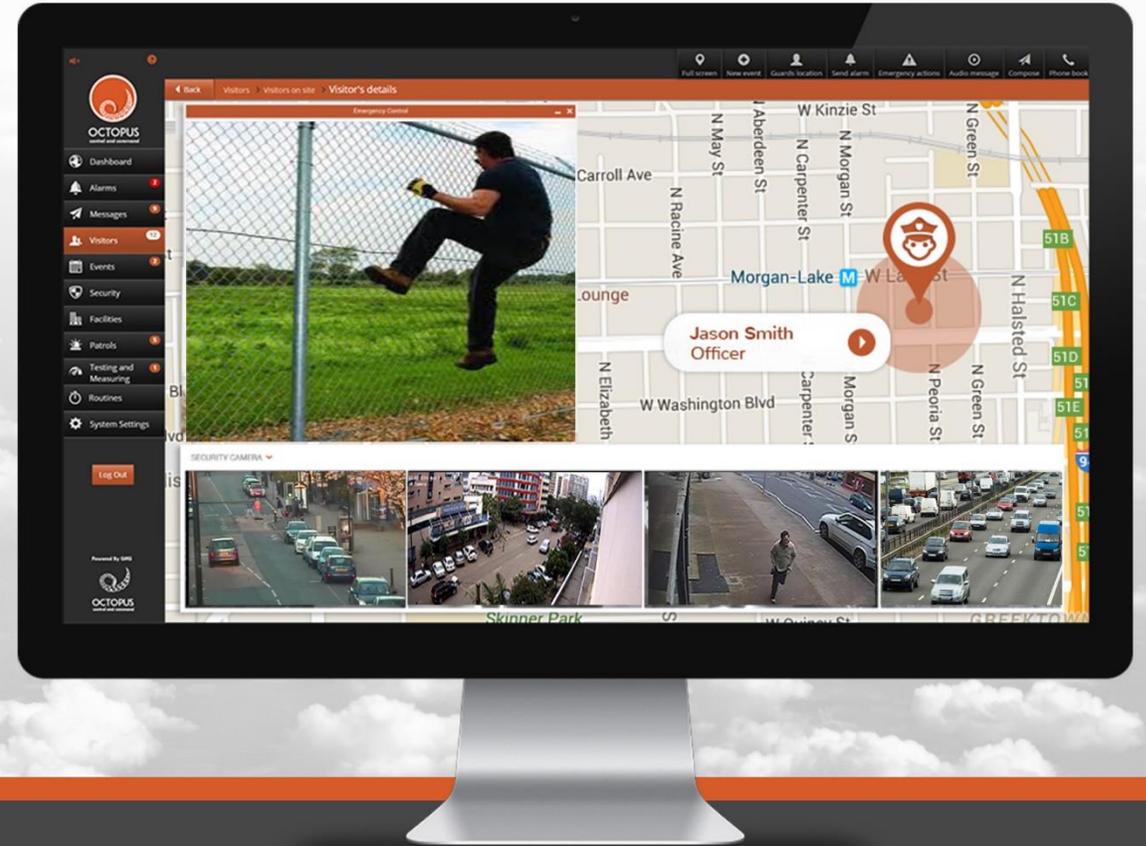
為安全人員設計的手機應用程式

- 監視手機中的所有安全技術
- 在緊急情況下立即調動應急小組
- 管理安全人員——事件、任務和狀態報告的雙向交流
- 通過手機發送緊急通知
- 安全人員是“人體感測器”——報告所有可疑活動
- 填寫現場報告和檢查的移動終端
- 優化和發送守衛旅遊和巡邏路線至應用程式



場景示例

- 1) 柵欄感測器為指揮和控制中心提供入侵跡象
- 2) 相機感測器在指揮控制中心自動出現允許驗證真實警報
- 3) 部署組織的周界入侵程式
- 4) 開源情報與更好的洞察所有相關的潛在威脅有關聯
- 5) CAD派遣最近的安全人員
- 6) 品質通知系統通過手機應用程式、短信和電子郵件通知該地區的所有使用者



建設和安全管理

- 集成關鍵性建築系統、接收資料並自動警報：
 - 關口和大門
 - 火光和瓦斯檢測器
 - 用水和浪費
 - 電源——米、UPS、發電機
 - SCADA、遙測和PLCs
 - 相機和安全系統
- 包括互動式建築佈局圖系統和警報的特徵定位
- 管理疏散和應急計畫及程式、部署自動化的工作流程。
- 所有來自同地的管理維護、訪問者和供應商、建築安全
- 對個人和設備的職能管理
- 資產管理——管理供應商、資格證書、測試和SLA。
- 為操作人員自動生成或手動創建任務
- 報告模組——現場報告和檢查
- 安全日常管理和性能監控

風險和性能監控

- 搜集和分析來自不同安全、網路、基礎設施和運營資源、自動或手動從業人員等的資訊。
- 基於預先定義的演算法計算績效指標、性能和風險
- 挖掘深入調查的隱含資訊
- 根據閾值生成行動和自動化操作



案例研究——以色列化工有限公司



金屬、化肥和其他化學產品的礦山和製造商的所有者



挑戰——ICL安全管理平臺

主營產品

- 溴
- 碳酸鉀
- 鎂
- 碳酸鹽

2014年財務

- 收入61.4億美元
- 運營收入7.58億美元
- 利潤4.66億美元

公司

- 14個國家
- 48個網站
- 12000名員工

安全要求和目標

- 提高車間安全性能
- 創建統一的、前瞻性和預防性的安全管理程式
- 減少事件和事故
- 加強管理人員之間的安全管理
- 建立共同的統一的語言
- 控制工具條款

功能需求

- 線上和離線安全日常報告
- 雲計算
- 手機應用程式
- 性能儀錶盤
- 可擴展平臺和報告
- 自動報表工具

RDI目標

- 減少安全成本
- 減少合規處罰
- 提高服務標準
- 改善ICL環境的聲譽

案例研究——以色列化工有限公司



解決方案——Octopus安全程式平臺

The smartphone screen shows the Octopus app interface with the following content:

OCTOPUS
selected and controlled

Detailed Manager Routine - Second Step

Risk Survey

What are the risks in the specific task?

Invalid Valid Neutral

How have you minimize the risks?

Invalid Valid Neutral

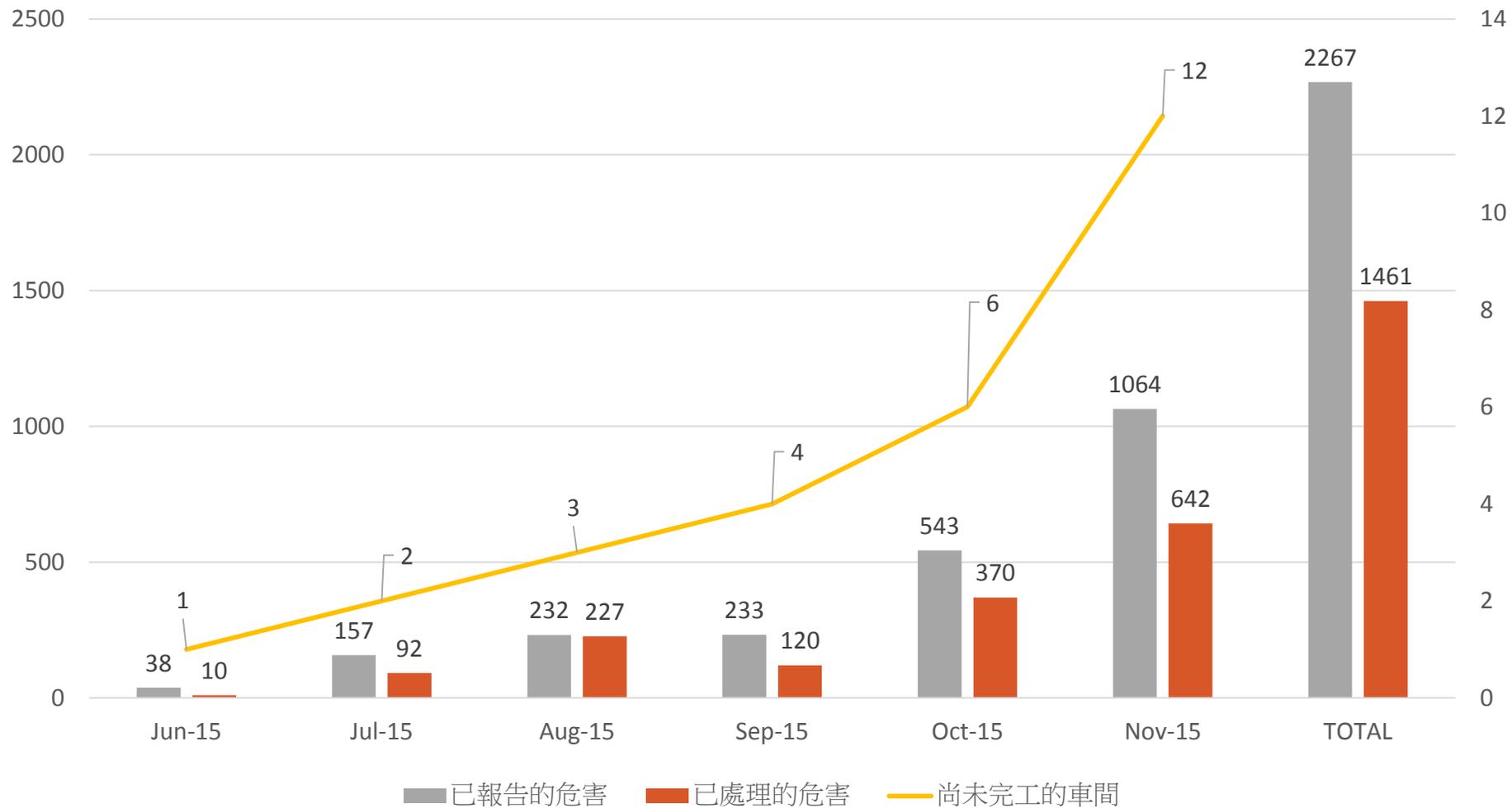
Was it accompanied by an escort operator?

Invalid Valid Neutral

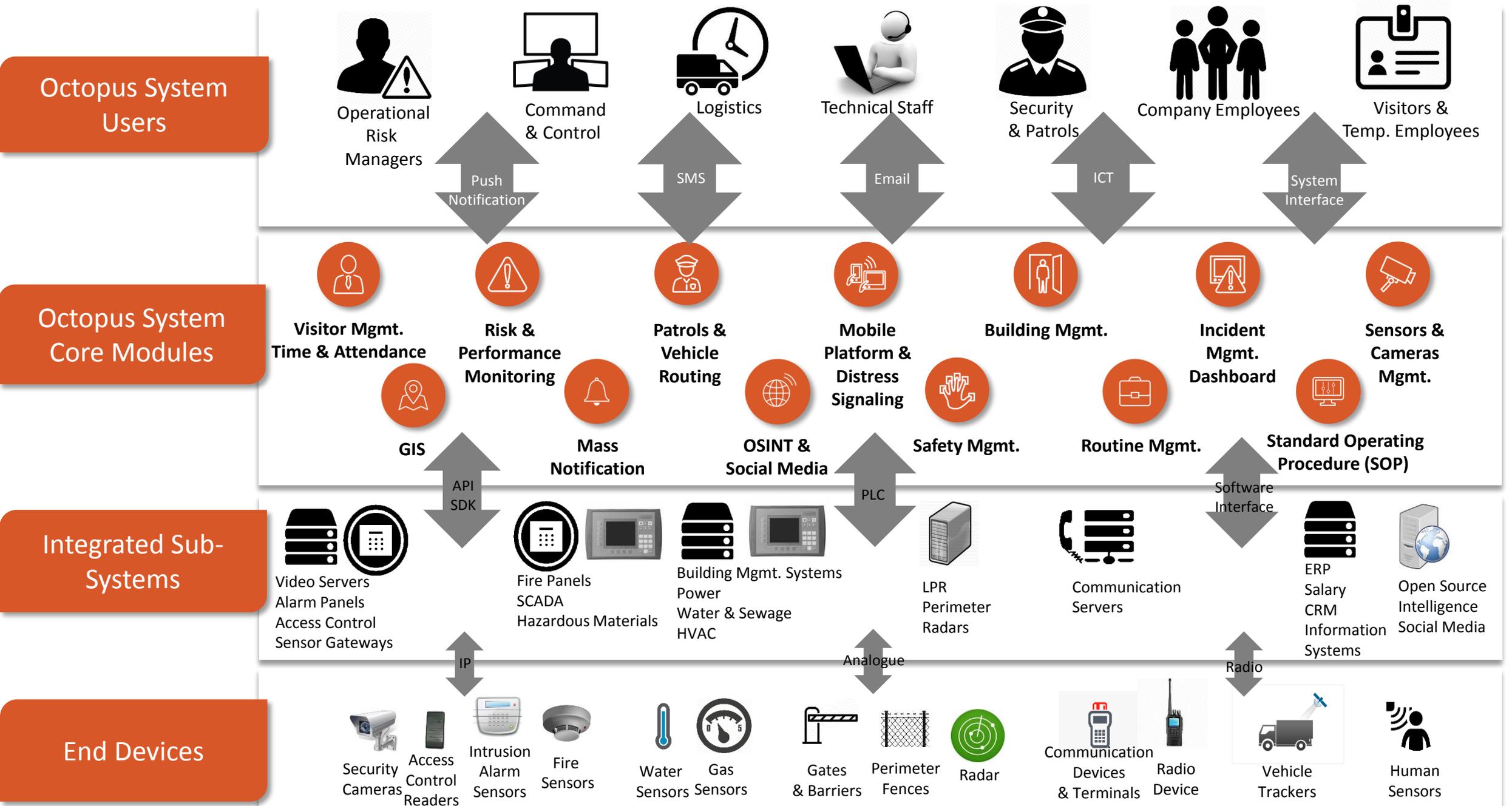
Did the escort operator have mentioned the risks factors (Hazardous Materials, Steam, Hot solutions ect.)



ICL | 實施階段——ROTEM & DSW



Octopus PSIM core entity flow diagram



OCTOPUS ENCOMPASS 綜述和效益

1. 唯一的雲使能完整PSIM解決方案——簡單、安全和組織中央指揮和控制平臺的多個網站有效管理的成本。也有可能將經營場址佈置在當地。
2. 滿足關鍵性基礎設施保護需求的一站式商店——35種不同模組，可以滿足組織的特定安全與後勤需要。
3. 資訊安全SIEM解決方案——為組織授權安全資訊事件管理(SIEM)系統，用於融合安全並提供作為系統一部分的資訊安全模組。
4. 通過智慧手機和平板電腦使用——緊急情況或需要移動指揮所時遠端系統管理事件。
5. 立即響應緊急事件——與所有安全部隊、應急人員、應急機構、運作功能和來自指揮中心或手機設備的組織員工進行快速簡便的交流。
6. 經濟——雲使能解決方案在降低IT成本的同時提高了互通性。
7. 安全情報——集成即時風險與威脅分析和外部刑事相關性、政府或組織資料來源、開源情報、社交媒體等。
8. 最佳實踐協定——系統為企業危機管理和安全與網路安全相關事件提供了最佳實踐方法和標準操作規程。
9. 開放式體系結構系統——集成了主要安全和基礎設施供應商和製造商，允許組織保留現有的硬體投資，但使指揮和控制集中。同時處理1000個感測器。
10. 統一常規操作畫面——在有直觀且先進使用者界面的地點通過全部安全格局的即時畫面增強態勢感知。