VIRTUAL SOC DEPLOYMENT FOR A BFSI ENTERPRISE

Google 4.0

Clutch 4.9

glassdoor 4.5

Countries we operate from

PROBLEM STATEMENT

A leading financial provider partnered with INT. to build a scalable SOC for real-time threat response amid rising digital banking attacks.

- MTTR (Mean Time To Respond) exceeded 12 hours, risking delayed breach containment
- Log data from mobile apps, cloud systems, ATMs, and customer portals was siloed
- In-house SOC resources were limited, with alert fatigue and lack of automation
- 24×7 online banking platforms lacked proactive security monitoring

INT.'S SOLUTION

INT. implemented a scalable virtual SOC to deliver continuous threat detection, response automation, and executive visibility.

- **Virtual SOC Framework:** Implemented Splunk Cloud and Microsoft Sentinel for centralized monitoring.
- **SIEM-SOAR Automation:** Enabled automated triage and alert escalation.
- **Threat Detection:** Utilized MITRE ATT&CK for detecting fraud and insider threats.
- **Threat Intelligence:** Provided weekly reports and IOC tracking.
- **Real-Time Dashboards:** Offered live insights into security posture for CISOs and IT leads.

A focused VAPT process with deep testing, prioritized fixes, and audit-ready reporting.

01

Assessment:
Reviewed existing monitoring tools, alert workflows, and incident response gaps

02

Design:
Defined architecture for a virtual SOC tailored to BFSI-specific threats

03

Deployment:
Implemented SIEM (Splunk Cloud) and SOAR (Microsoft Sentinel) across environments

04

Detection Engineering:
Built use cases using MITRE ATT&CK to detect financial fraud techniques

05

Automation Setup:
Integrated triage for phishing, credential abuse, and API anomalies

06

Reporting & Enablement:
Delivered executive dashboards, weekly threat reports, and SOC training

IMPACT

93%

alert triage automated, freeing SOC analysts from low-priority noise

MTTR reduced from 12 hours to 1.8 hours, significantly accelerating response

5

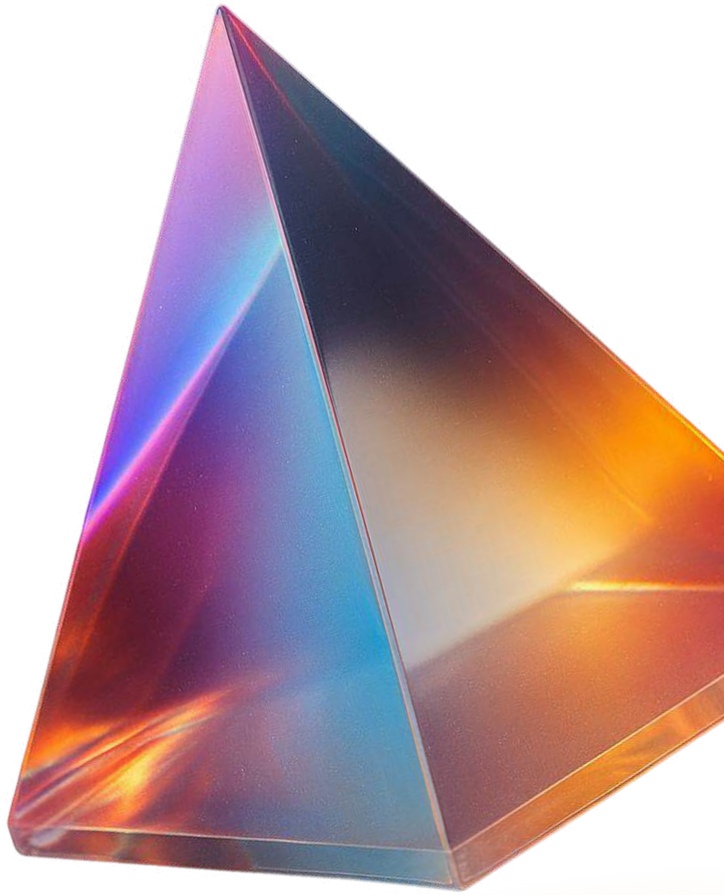
credential-stuffing campaigns neutralized during peak login hours

SOC maturity upgraded from Level 1 to Level 3 in under 6 months

24x7

visibility across core banking platforms, with no missed high-priority incidents

Executive teams gained real-time dashboards, boosting governance and audit readiness



INT.

Let's Help You

Delight Your Customers - The easiest way to achieve growth

info@intglobal.com

intglobal.com

27+ Years | **1000+** Professionals | **45+** Countries | **30+** Awards

INT. (Indus Net Technologies) is an award-winning full-stack software engineering solutions company with a pioneering legacy spanning 27 years, over 500 clients, and 11,000 plus client projects. INT. operates at the confluence of Data, technology, and marketing in the digital space.