FINANCIAL SERVICES | THREAT HUNTING

Threat hunt program development for a large global financial institution

A large global financial institution wanted to move from reactive detection to proactive threat hunting, but lacked a repeatable, in-house capability. **Optiv Consulting** built the framework, playbooks, and skills to make hunting a standing discipline.

SECTOR	DISCIPLINE	METHOD	OUTPUT
Global financial institution	**Threat hunting**	**Phased maturity roadmap**	**Hunt playbooks**

THE CHALLENGE

The team needed consistent hunt execution across different analysts and technical domains, and visibility into the telemetry gaps that let advanced techniques go unseen.

OUR APPROACH

- Evaluated current detection capabilities, data sources, and analyst skills against industry benchmarks.
- Developed a multi-phase roadmap focused on incremental maturity gains.
- Authored custom hunting playbooks and templates for hypothesis generation, evidence collection, and reporting.
- Guided initial hunt executions with over-the-shoulder review of logic and output.

Lower MTTD

Mean time to detect reduced through structured playbooks

BENEFITS

- Transitioned the security team to a formal, repeatable hunt program.
- Improved the return on existing tools by tuning logging and alerts to hunt findings.
- Equipped the internal SOC with the skills and documentation to run the program independently.