LevelBlue

CASE STUDY

Major financial institution chooses LevelBlue for Microsoft-first security approach

LevelBlue recently partnered with a major bank to implement a Microsoft-first security strategy, with Microsoft Sentinel as the core solution. As a Managed Security Services Provider (MSSP), LevelBlue leveraged its specialized Microsoft expertise to offer a comprehensive suite of security services tailored to the client's needs.

The challenge

During initial discussions with the bank, it became clear the client had concerns with its existing MSSP. The financial institution's current provider had limitations around log management and alert development, and they were not satisfied with the intellectual property (IP) being hosted on the MSSP's platform.

Additionally, the bank wanted to retain control over its monitoring and alerting capabilities, as well as any new use cases developed within the service. Additionally, they sought access to a broader array of security tools to address potential blind spots.

With a looming deadline for the expiration of its current service contract, the bank needed a solution in place quickly – within just three weeks.

The solution

LevelBlue rose to the challenge and successfully met the tight deadline by completing Phase 1 onboarding and migration on schedule. All Microsoft log sources were integrated into Sentinel, active use cases were deployed, and LevelBlue's Security Operations Center (SOC) began monitoring for Indicators of Compromise (IOCs) and malicious activity.

The LevelBlue solution adopted by the client included:

- Co-Managed SOC with Sentinel
- MDR for thousands of endpoints
- Advanced Continual Threat Hunting
- DFIR – Emergency Incident Response
- Onboarding
- Additional consultancy for custom use cases

Beyond these core technical services, LevelBlue also provided "soft" benefits derived from decades of cybersecurity experience and a long-standing partnership with Microsoft. Our deep knowledge of Microsoft technologies, combined with our established credentials and ability to deploy quickly, made LevelBlue the bank's provider of choice.

When the bank's security team, which was new to Sentinel, needed assistance during its transition, we stepped in with our expertise and our technology-agnostic approach allowed us to provide a flexible solution.

LevelBlue's Co-Managed service offering enables clients to retain ownership of its intellectual property (IP), which, as noted, is important to the client.

The client's final word

The client was impressed with the cloud-native LevelBlue Fusion and our ability to integrate with Sentinel. In the initial conversations with the bank, its team expressed a strong preference for Fusion, appreciating its central dashboard.

LevelBlue's solution allowed the bank to drive greater efficiencies, allowing the client to consolidate its technology infrastructure and adopt a Microsoft-first approach. Additionally, LevelBlue's onboarding process allowed the client continuity with operations during the contract transition and expedited the migration process seamlessly.

Finally, the client attained its goal of appointing an MSSP to help deliver a managed security service and bring in the expertise to help them migrate seamlessly from its previous system to Microsoft Sentinel and provide 24×7 monitoring and management of security devices and systems.