Who Is Odeabank?
Founded in 2012 and headquartered in Istanbul, Turkey, Odeabank is one of the country’s leading banks. Offering services across corporate, commercial, retail, investment and private banking, the organization has consolidated assets equivalent to over US$35 billion.

Growing Rapidly through Service Excellence
Following fast-paced growth, Odeabank has climbed from the 49th largest bank by asset size to a top-ten player in its domestic market. The bank serves customers through a wide variety of channels, including 48 physical branches as well as online and mobile banking platforms. Digital solutions play a key role in all aspects of Odeabank’s offering, and the company is mandated by Turkey’s Banking Regulation and Supervision Agency (BRSA) to maintain rigorous information security and data governance controls.

Emrecan Batar, Information Security Senior Specialist at Odeabank, explains: “As a future-facing bank, we manage a large IT estate: from endpoints such as laptops and desktops in our branches and back-office locations, to application servers and core banking platforms in our data center. Keeping these systems protected 24/7 is crucial—and to help achieve that goal, we rely on our Security Operations Center [SOC].”

In the SOC, Odeabank’s information security specialists are responsible for sifting through potential security events, determining which are most likely to represent actual incidents, and prioritizing the investigation and remediation of cyber threats. Odeabank uses security information and event management (SIEM) data to help surface potential threats, and security orchestration, automation, and response (SOAR) capabilities to help manage investigation and remediation activities.

“Rather than writing multiple playbooks for each type of potential security threat, we use a single set of branching logic in ArcSight SOAR to help us close 33% of cases without any human involvement.”

Emrecan Batar
Information Security Senior Specialist
Odeabank

At a Glance

Industry
Banking

Location
Turkey

Challenge
Minimize volumes of duplicate and false-positive security alerts, enabling security specialists to investigate the most significant threats

Products and Services
ArcSight Enterprise Security Manager (ESM)
ArcSight Security Orchestration Automation and Response (SOAR)

Success Highlights
• Up to 15,000 security events surfaced per second
• 90% reduction in security incidents forwarded for investigation
• 33% of cases resolved and closed via SOAR, without any human involvement
• Helps Odeabank monitor service-level agreements and ensure regulatory compliance
Addressing Large Volumes of Threat Data

Increasingly, many Odeabank customers prefer to engage with the bank via digital channels. Batar continues: “As demand for our digital systems grows, so is the volume of security event data. We need to track thousands of alerts per day, which was beginning to put increased strain on the SOC. To empower our lean SOC team to protect the bank and meet our regulatory requirements, we looked for a better way to sort the signal from the noise.”

To realize its information security objectives, Odeabank uses ArcSight Enterprise Security Manager (ESM) to enable real-time threat detection, and ArcSight SOAR to intelligently automate repetitive security activities.

“Thanks to the CyberRes solutions, we’ve strengthened the capabilities of our SOC, which helps us to meet our regulatory requirements,” adds Batar. “For example, we now use an integration between ArcSight SOAR and our service management solution to automatically push information on incidents to our IT infrastructure teams—helping us to demonstrate our compliance and enable timely remediation.”

By enabling automated orchestration workflows using ArcSight SOAR, Odeabank is dramatically shrinking manual work for its SOC team—empowering them to spend less time sifting through data and more time on value-added investigation and remediation activities.

“By consolidating duplicate events and eliminating false positives with ArcSight SOAR, we have cut down the number of daily alerts to our SOC team by 90%,” concludes Batar. “Rather than writing multiple playbooks for each type of potential security threat, we use a single set of branching logic in ArcSight SOAR to help us close 33% of cases without any human involvement: for example, by allowing or blocking an IP address. Our CyberRes solutions are vital to maintain a strong security posture, and we plan to continue to enhance our capabilities going forward.”