opentext™ | Cybersecurity

Case Study

Turkcell

ArcSight modules partner with MITRE ATT&CK framework to deliver sophisticated real-time data correlation and incident response.

Who is Turkcell?

Turkcell is a converged telecommunication and technology services provider, founded and headquartered in Turkey. It serves its customers with voice, data, TV, Digital Security Services and value-added consumer and enterprise services on mobile and fixed networks.

Distilling Billions of Security Events into Meaningful Alerts

With over 50 million worldwide subscribers, data security and privacy is absolutely vital for Turkcell. Advanced cyber security threats and data privacy regulations such as KVKK and the Turkish Data Protection Act were reasons to introduce a sophisticated Cyber Defence Center (CDC). Security analysts and a digital forensic team work hand-in-hand with an incident response team and a planning team. ArcSight Enterprise Security Manager (ESM) by OpenText was selected to create a next-generation Security Information and Events Management (SIEM) by OpenText with powerful, efficient threat detection and response through security analytics. Cihan Yuceer, Cyber Defence Center Manager with Turkcell, explains: "We act as a Managed Services Security Provider (MSSP) for over 20 of our corporate customers. With over 550 data sources, our CDC processes six billion data logs every day. These are filtered down to three billion, and then aggregated into 1.8 billion logs. After sophisticated data correlation 400 million logs remain which result into over 300 daily alerts that need to be actioned, on behalf of our MSSP customers. ArcSight ESM's powerful real-time correlation gave us the fastest path to detect threats and mitigate them."

> "[OpenText™] Vertica Analytics Platform is embedded within ArcSight Intelligence. This enables us to take security log data from the ArcSight smart connector sources and perform sophistication correlation and data analytics at high speed."
>
> **Cihan Yuceer**
> Cyber Defence Center Manager
> Turkcell

Turkcell CDC engineers developed the BOZOK threat intelligence platform, which includes data leakage, brand protection, and vulnerability modules, within an Integrated Operations Center (IOC) platform. They will use the IOC platform for threat intelligence use cases with ArcSight ESM.

TURKCELL

At a Glance

Industry

Telecommunications

Location

Turkey

Challenge

Effectively and quickly detect and mitigate cyber threats through a maze of 6 billion daily data logs from over 550 sources

Products and Services

ArcSight ESM
ArcSight Intelligence
ArcSight SOAR

Success Highlights

- Distilling 6 billion daily data logs down to 300 actionable alerts and 20 escalations
- Powerful ArcSight correlation combines with Turkcell's BOZOK threat intelligence platform to detect and mitigate threats
- SLA and auditing compliance with ArcSight SOAR capabilities
- MITRE ATT&CK compliance strengthens cyber security

> **“The great integration capabilities demonstrated in the ArcSight toolset have allowed us to create an end-to-end SIEM with MITRE ATT&CK compliance and new data sources in ArcSight ESM, additional use cases and reporting with ArcSight SOAR, and enhanced overall security with ArcSight Intelligence.”**
>
> **Cihan Yuceer**
> Cyber Defence Center Manager
> Turkcell

Connect with Us
www.opentext.com

ArcSight ESM has been enhanced by the introduction of ArcSight Intelligence. This supports security operations with threat detection software that finds unknown threats quickly. It allows Turkcell to distill its billions of events into a list of prioritized threat leads, reducing alert fatigue and enabling them to focus on the threats that matter.Through the combination of ArcSight ESM 24/7 security monitoring and ArcSight Intelligence by OpenText prioritization process the incident response team deals with approximately 20 escalated cases each day.

ArcSight Leveraged for KPI and SLA Tracking

ArcSight ESM provides real-time detection and machine learning-based coverage for the MITRE ATT&CK framework. This framework is a free, globally accessible service that provides comprehensive and up-to-date cyber threat information to organizations looking to strengthen their cyber security strategies. Turkcell also appreciates the high speed data processing capabilities, as Yuceer comments: “[OpenText™] Vertica Analytics Platform is embedded within ArcSight Intelligence. This enables us to take security log data from the ArcSight smart connector sources and perform sophistication correlation and data analytics at high speed.”

With growing numbers of daily alerts collected in the Turkcell CDC, the number one priority is to give security staff enough time to take the proper action against threats before damage is done. ArcSight SOAR by OpenText provides detailed reporting on every single incident to help managers understand historic events and better plan future directions. Everything is then logged and forwarded to ArcSight ESM to create weekly executive reports, track Key Performance Indicators (KPIs) and compliance with Service Level Agreements (SLAs) for auditing purposes. With the seamless automation engine of ArcSight SOAR, Turkcell can define any number of complex cyber attack scenarios for the engine to execute. All of the mundane and repetitive tasks are offloaded to tactical automation so that the security team can scale its activities in the face of growing cyber threats.

ArcSight Integration Delivers End-to-End SIEM

“The great integration capabilities demonstrated in the ArcSight toolset have allowed us to create an end-to-end SIEM with MITRE ATT&CK compliance and new data sources in ArcSight ESM, additional use cases and reporting with ArcSight SOAR, and enhanced overall security with ArcSight Intelligence,” says Yuceer.
He concludes: “We enjoy our partnership with Micro Focus (now part of OpenText). We have worked directly with Product Management and Research and Development on new features and functionality, which does not only benefit Turkcell, but other ArcSight customers too. We receive great support and when working jointly on security projects, Micro Focus (now part of OpenText) Professional Services consultants always ensure effective knowledge transfer to our own CDC team members.”

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.