Tesco

Harry McLaren, Head of Cyber Defense

As Head of Cyber Defence, I lead the organisation's unified Threat Intelligence, Detection Engineering, Investigation, and Response (TIDIR) function, responsible for protecting critical business services, colleagues, and customers through an intelligence-driven, threat-informed defence model. I oversee both strategic direction and operational execution across a converged cyber defence ecosystem, ensuring we stay ahead of an increasingly hostile threat landscape and a rapidly modernising digital estate.

One of the world's largest retailers of consumer goods from food to fashion. Serving our customers, communities and planet a little better every day in our stores and online is at the heart of everything we do.

Founded in 1919 by Jack Cohen using the £30 he received on leaving the Royal Flying Corp, we've come a long way from his small market stall in East London. Today over 400,000 colleagues work across our stores, office, distribution and customer engagement centres in the UK, Europe and Asia.

WHAT ARE YOUR KEY DEPARTMENTAL OBJECTIVES OVER THE NEXT 6 TO 12 MONTHS?
- Increase security posture across focused areas.

- Increase the maturity of our supplier management.

- Focus on value extraction of existing technology investments

WHAT IS YOUR CURRENT TECHNOLOGY STACK?
Microsoft, Splunk, Palo Alto Network, Proofpoint

HOW MANY PEOPLE REPORT TO YOU (BOTH DIRECTLY AND INDIRECTLY)?
27

WHO DO YOU REPORT TO?
Security Director

WHAT IS YOUR TOTAL BUDGET OVER THE NEXT 12 MONTHS PERIOD?
€20 million

PROJECT OR INITIATIVE DESCRIPTION
Leverage AI to enhance Threat Detection & Incident Response Platforms

Public Cloud Security (Azure)

Container Workload Security (Public Cloud & Self Hosted)

Active Directory Platform Security

WHAT 3RD PARTIES ARE YOU HOPING TO MEET WITH?
Wiz or similar, SIEM-like vendors or similar, Anvilogic or similar

WHAT IS YOUR TIMELINE FOR IMPLEMENTATION?
12-18 months

WHAT IS YOUR BUDGET FOR THIS PROJECT?
Each initiative has a budget of up to €5 million

What technology/services are of strategic importance to you in the next 12 months?

Please indicate level of need/importance below.

We realize everyone has priorities, so we asked the delegates theirs. This is so that we can create a more personalized experience for all our attendees.

Leveraging AI to enhance threat detection	A
Convergence of Data Privacy and Data Security	E
Protecting the enterprise against the emerging use of GenAI and LLMs	C
Universal Privilege Management - Why you Need to Address More Than Passwords	D
Save the SOC: How to Increase Investigation Speed, Efficiency and Accuracy	A
Next Gen Browser Securiity	C
Creating an Intelligence Forward Cyber Security Program	A
Integrated and agile identity platform providing authentication and secure interactions for users, systems, and devices	E
Optimizing security portfolio investment by focusing on best-of-platform vs. best-of-breed	C
AI tools that can quickly repair or recover files to enhance remediation	C
Continuous Visibility of Security and Compliance Across On-Premises Assets, Endpoints and Multi-Cloud Environments	B
Creating a Zero Trust Environment	E
Five Best Practices When Deploying Zero Trust in the Modern Data Center	A
Bot mitigation and prevention strategies	D
Delivers advanced managed services and solutions for cybersecurity, cloud, artificial intelligence (AI), machine learning (ML), and IT modernization.	E