



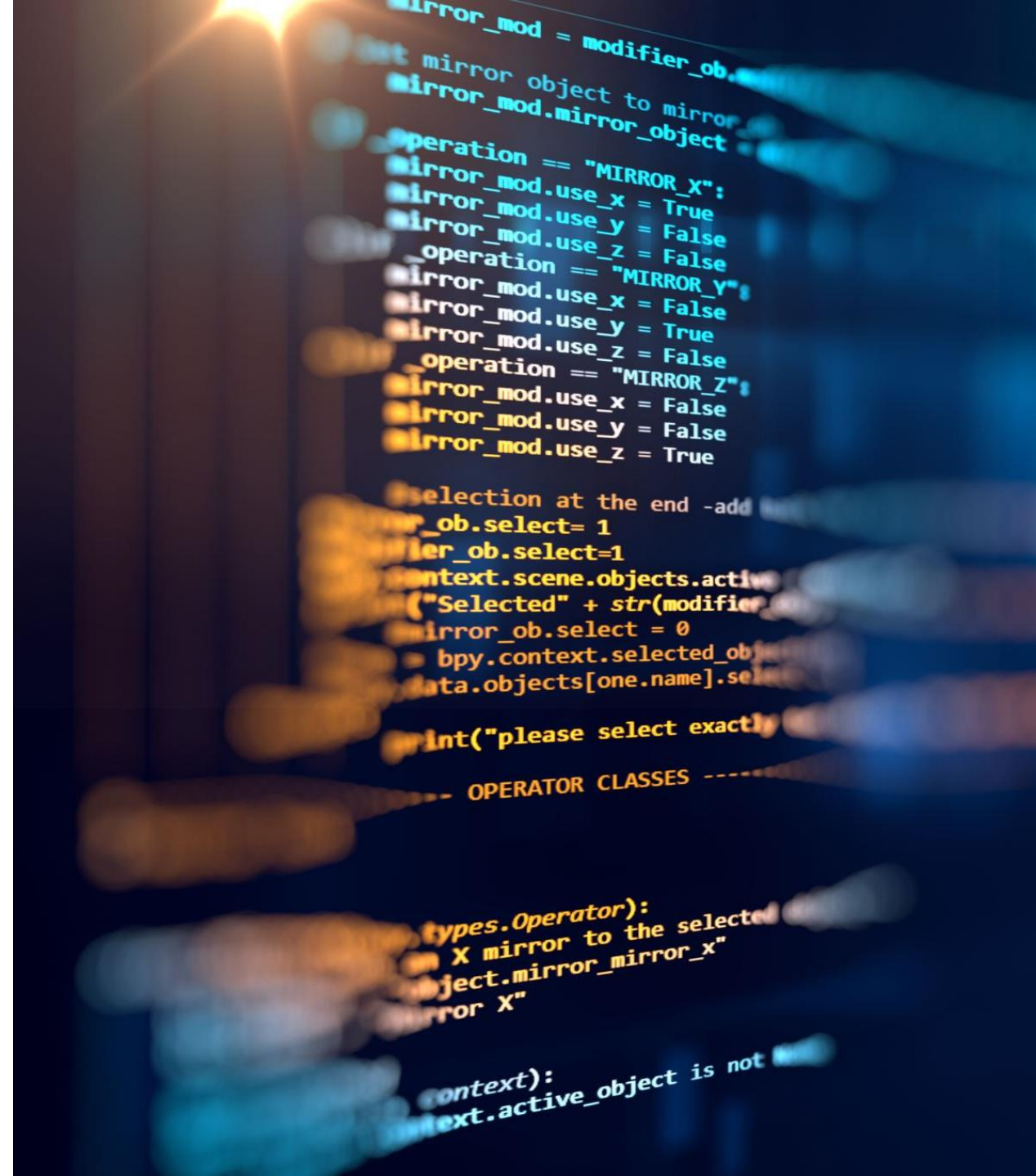
Microsoft Sentinel Overview

Kieran Bhardwaj
Security Global Blackbelt



Security and Information Event Management (SIEM)

- Collect, store, investigate, analyze and report event data in real time
- **Early detection** of targeted attacks and data breaches for incident response, forensics and regulatory compliance
- **Aggregates event data** produced by security devices, network infrastructure, systems and applications
- Event data can be **combined with contextual information** about users, assets, threats and vulnerabilities
- Data can be **normalized from disparate sources** for specific visibility
- **Real-time analysis of events** for security monitoring, query and long-range analytics for historical analysis.



Introducing Microsoft Sentinel

Cloud-native SaaS SIEM for intelligent security analytics for your entire enterprise

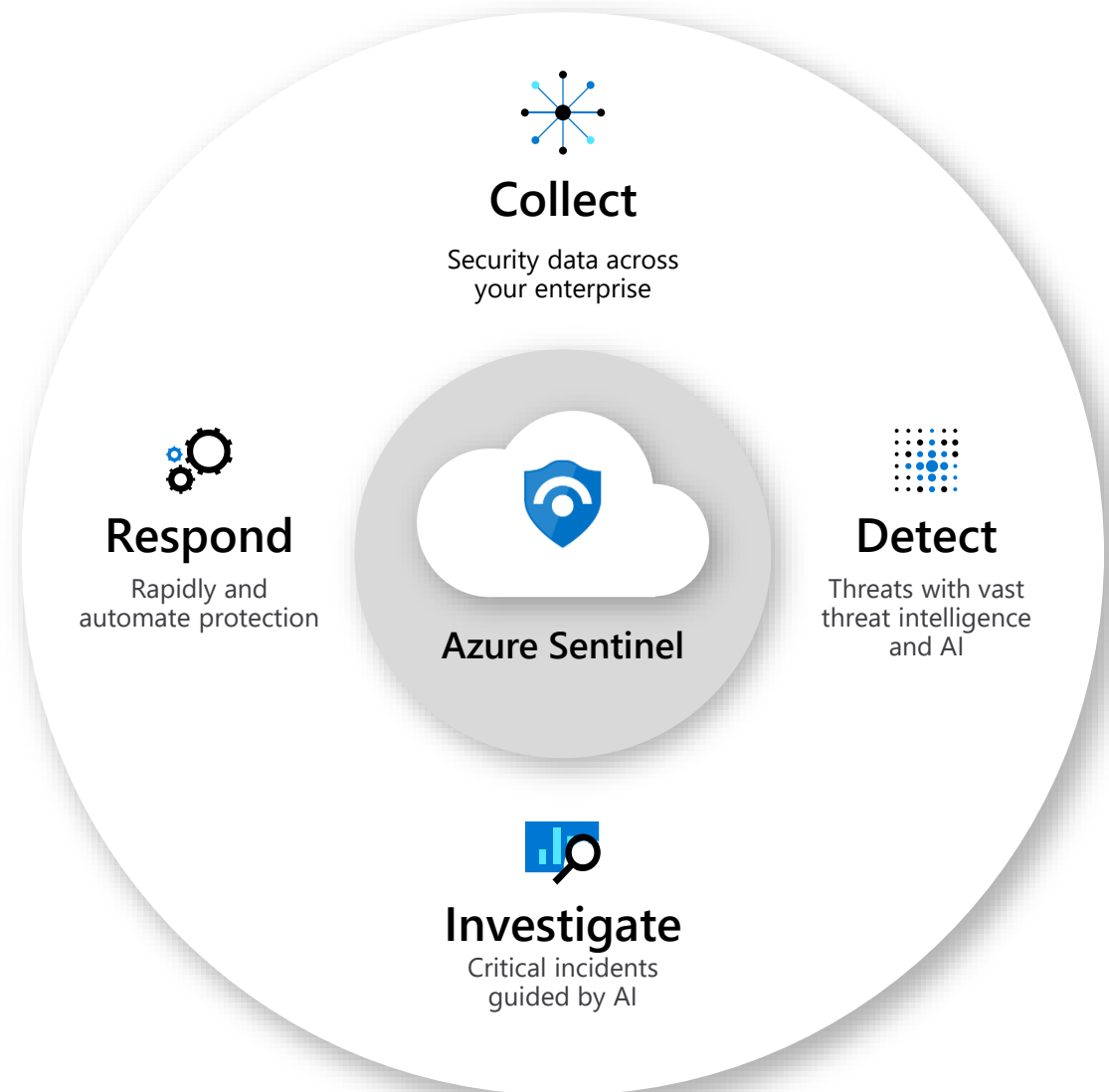
Limitless cloud speed and scale

Bring your **Office 365 data for Free**

Easy integration with your **existing tools**

Faster threat protection with **by your side**

Integrated SOAR, UEBA, ML, & AI capabilities



Collect security data at cloud scale from all sources across your enterprise

Pre-wired integration with Microsoft solutions

Connectors for many partner solutions

Standard log format support for all sources

Proven log platform with more than
10 petabytes of daily ingestion



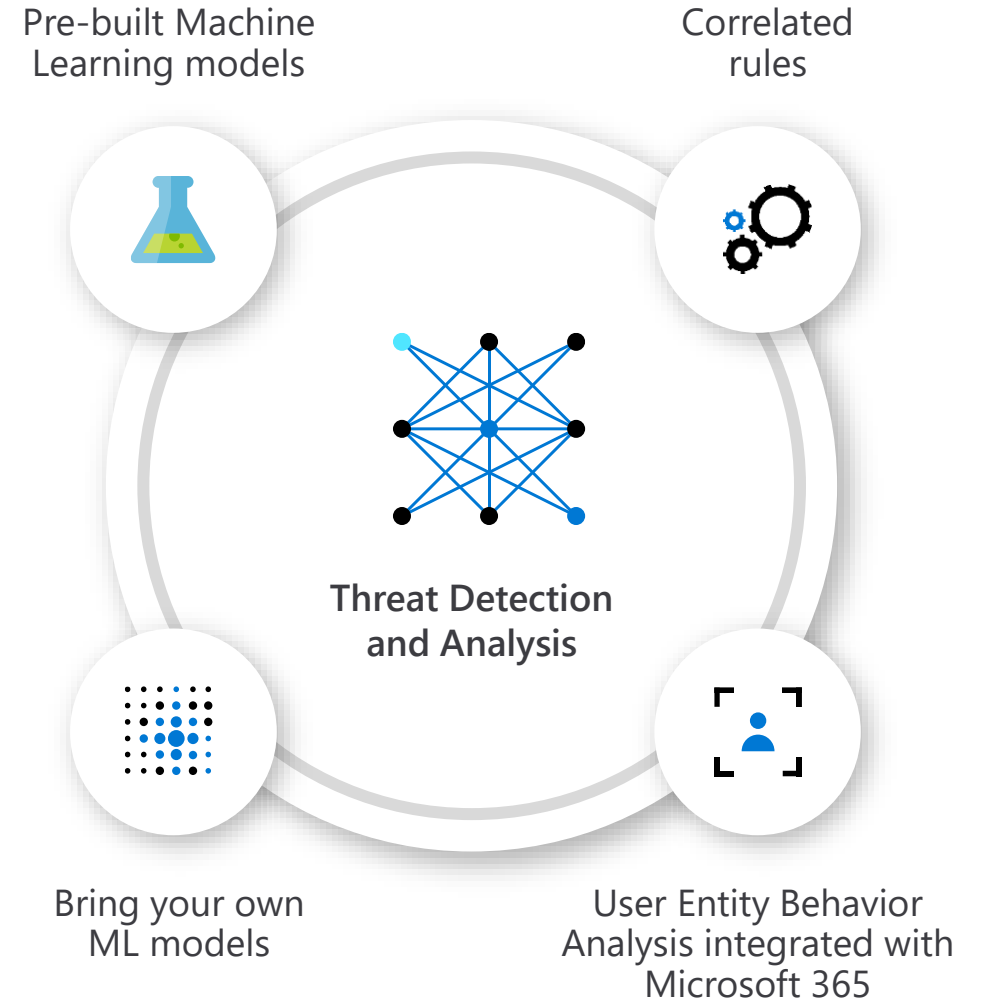
Detect threats and analyze security data quickly with AI

ML models based on **decades of Microsoft security experience and learnings**

Millions of signals filtered to few **correlated and prioritized incidents**

Insights based on vast **Microsoft threat intelligence** and your own TI

79% decrease in false positives
over three years¹



How it works / Features

Kusto Query Language

Collect

Microsoft
Services



Apps, users,
infrastructure



Public Clouds



Security solutions

Visibility



Dashboard

Analyze & Detect



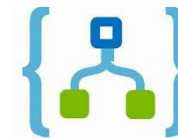
Machine
learning, UEBA

Investigate & Hunt



Pre-defined Queries,
Azure Notebook

Automate & Orchestrate Response



Playbooks

Enrichment



Data Ingestion



Data Repository

Azure Monitor



Data Search

Integrate

now
ServiceNow



Other tools



Community

Microsoft Resources

[Become an Azure Sentinel Ninja: The complete level 400 training](#)

[Azure Sentinel Deployment Guide](#)

[Azure Sentinel: The End-to-End SOC Scenario](#)

[Architecting SecOps for success: Azure Sentinel Best Practices](#)

[Move Your Azure Sentinel Logs to Long-Term Storage with Ease - Microsoft Tech Community](#)

[Azure Sentinel Pricing | Microsoft Azure](#)