overere

overere.io

How ThreatEcho Built Production Microsoft 365 Security in 2.5 Weeks Using Overe

Avoided 4-5 months of Microsoft integration engineering

ThreatEcho is a digital risk intelligence platform developed by Safetech Innovations Global Services, operating across the UK, US, EU, and Middle East.

The platform helps organisations and MSSPs identify, prioritise, and respond to digital risk across Microsoft 365 environments, identities, domains, and vendors.

Rather than building and maintaining complex native integrations across Microsoft Graph, Defender, Entra ID, and Purview, ThreatEcho integrated directly with the Overe Partner API.

Name	Jay Kay (Director of Technology)
Company	ThreatEcho / Safetech Innovations Global Services
Website	https://www.safetechinnovations.com/
Industry	Cybersecurity / MSSP Platform
Location	UK, US, EU & Middle East
Focus	Digital Risk Intelligence & Microsoft 365 Security

CHALLENGE

ThreatEcho initially evaluated building directly against Microsoft's native security and Graph APIs. The engineering and operational complexity quickly became clear, particularly for a multi-tenant MSSP platform.

Key challenges:

- Multi-tenant OAuth and admin consent handling for every customer
- Token storage, refresh, and rotation per tenant
- Separate API coverage across Graph, Defender, Purview, and Entra ID
- Normalising inconsistent Microsoft security schemas and alerts
- Ongoing maintenance caused by Graph deprecations and schema drift
- Scaling onboarding and operational workflows across MSSP-managed tenants

SOLUTION

ThreatEcho integrated directly with the Overe Partner API, giving the team a single, consistent integration surface across Microsoft 365 security operations.

Instead of building separate integrations across Microsoft Graph, Defender, Purview, and Entra ID, ThreatEcho could rapidly provision tenants, onboard MSSP environments, and ingest normalised alerts through a unified API layer.

The initial integration was completed in approximately 2.5 weeks of focused development time, from authentication and provisioning through to production alert ingestion and workflow automation.

> *"Most native integrations fall apart at multi-tenant scale. Overe was clearly built for it from day one, which matched our MSSP-first go-to-market."*
> **— Jay Kay, Director of Technology, Safetech Innovations Global Services**

overere

overere.io

How ThreatEcho Built Production Microsoft 365 Security in 2.5 Weeks Using Overe

THE INTEGRATION

ThreatEcho completed the initial integration in approximately 2.5 weeks of focused development time, from reading the Overe Partner API specification through to production tenant onboarding and alert synchronisation.

The integration included:
~3 days on authentication and partner credential handling and **~4 days** on provisioning and site lifecycle workflows
Live workflows now running in production include **auto-disable on compromised identities**, forced **MFA re-enrolment on risky sign-in patterns**, **bulk conditional access and sharing policy hardening across MSSP-managed tenants**, and **continuous compliance posture** sync against ISO 27001 and NIST frameworks.

The turning point came during bulk MSSP onboarding, where ThreatEcho realised customer tenants could be provisioned and managed through a single partner workflow instead of maintaining separate app registrations per tenant.

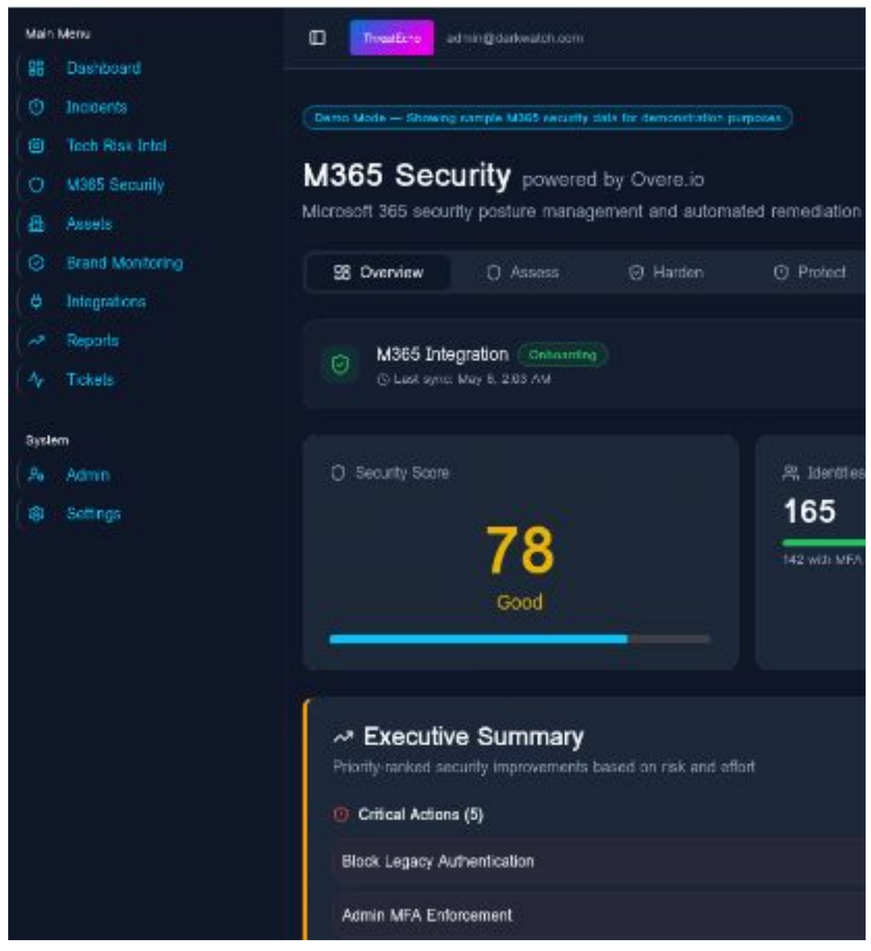
> *"For a team our size, that's the difference between shipping features and babysitting integrations."*
> **— Jay Kay, Director of Technology, Safetech Innovations Global Services**

RESULTS

✅ Production Microsoft 365 integration completed in **approximately 2.5 weeks**
✅ **Avoided an estimated 4-5 months** of backend Microsoft integration engineering
✅ Single integration surface across **Graph, Defender, Entra ID, and Purview**
✅ **Rapid MSSP tenant onboarding** through unified partner workflows

✅ **20-30% ongoing reduction** in Microsoft API maintenance and schema drift overhead
✅ **Enabled engineering focus** on detection logic and customer workflows instead of integration management

By building on Overe's Partner API layer, ThreatEcho accelerated time-to-market while avoiding the operational complexity typically associated with large-scale Microsoft 365 security integrations.



WHY IT MATTERS?

For MSSPs and security vendors, the challenge is not accessing Microsoft telemetry. The challenge is operationalising it at scale.

ThreatEcho used Overe as the Microsoft 365 security infrastructure layer underneath its platform, allowing the team to focus engineering effort on customer workflows and detection logic instead of maintaining fragile Microsoft integrations.

READY TO SEE FOR YOURSELF?

Get started now with Overe.
Experience the full power of Overe Protect in your environment with a 14-day free trial — no limitations, no commitment.

app.overe.io

Learn more at overe.io

TRY IT FOR FREE

hello@overe.io