DYOGUARD

# SENTRY AI SECURITY OPERATIONS

Guide Sheet

## AI SECURITY OPERATIONS CONTROL PLANE FOR MICROSOFT SENTINEL AND DEFENDER

### AI-ENABLED SECURITY OPERATIONS CONTROL PLANE

Security operations are still constrained by manual investigation work, inconsistent response, and automation that security teams cannot trust. DYOPATH turns Microsoft-native security operations into a governed operating model by providing the management, orchestration, and trust plane required to run AI workflows in production.

AI is not the product. Control is the product. DYOPATH makes AI usable by enforcing policies, approvals, audit trails, and repeatable workflows that match how analysts actually work.

### WHY SECURITY TEAMS CHOOSE SENTRY AI

1. **Faster response with safe automation**: Automate triage, investigation, and response inside governed workflows so analysts can resolve incidents dramatically faster and with consistent outcomes.
2. **Control plane over your Microsoft Security stack**: Manage and orchestrate response across Sentinel, Defender, and Entra ID through one control plane, gaining federated visibility while maintaining sovereignty and compliance requirements.
3. **Standardized investigations and response actions**: Use governed workflows to reduce variance across analysts and shifts. Every incident produces consistent summaries and decision trails for review and reporting
4. **Measurable efficiency gains**: Move from human-bound workflows to outcome-based automation that increases efficiency per incident while keeping security teams in control.

## WHAT'S INSIDE THE PLATFORM

- **Federated control plane:** Unified visibility and orchestration
- **Gamebooks:** AI-generated responses mapped to MITRE ATT&CK & D3FEND
- **Human-in-the-loop workflows:** Analysts can approve or automate actions.
- **Continuous detection updates**: Always-on rule generation and tuning
- **Audit Activity:** Bi-directional case management updates in your EDR and SIEM
- **Data Sovereignty:** Compliant, scoped access to your security infrastructure

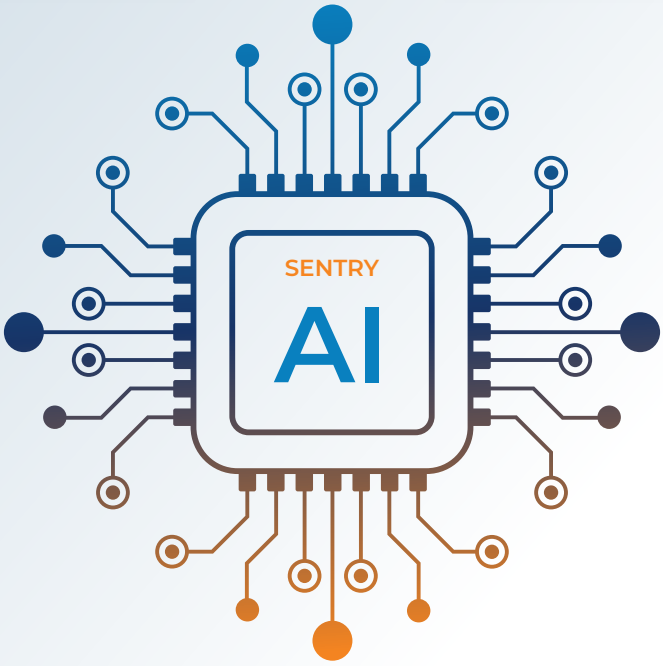
## MEASURABLE IMPACT

### DEPLOY FAST

Connect, configure, and orchestrate in about 1 hour

### RESOLVE FASTER

Up to 60x faster incident resolution speed




### AUTOMATE THE HEAVY LIFT

95% of triage, investigation, and response tasks automated

### IMPROVE UNIT ECONOMICS

Transition from labor to compute-based economics with simple cost per user pricing.