DEFCOM by CyberHorses AG

Defender Companion

Delivering smarter security - fast

Enhanced Business Risk Integrated in Your Security Decisions

DEFCOM transforms your Defender for Endpoint into a context-aware security platform. By automatically tagging and continuously profiling your devices with data from Active Directory, Entra ID, asset inventories, and more, DEFCOM empowers your organization to prioritize risks, streamline escalations, and align incident response actions with business impact.

Why DEFCOM?

- **Smarter Access Control**: automatically group devices using dynamic, tag-based RBAC that mirrors your organizational structure—streamlining governance and reducing access risk.
- **Business-Driven Risk Prioritization:** focus remediation where it matters most by targeting vulnerabilities on high-impact assets, not just those with high technical severity.
- **Proactive Threat Hunting:** detect identity misuse and access anomalies faster by connecting real-time security signals to device ownership and business context.
- **Real-Time Asset Intelligence:** keep a continuously updated view of device roles and criticality—ensuring every security action reflects its impact on your core operations.

The Three-step Continous Cycle

1 - Gather

Continuous gathering of contextual data by integrating in existing tools.

- Azure Graph API
- Active Directory / Entra ID
- Asset inventory
- IP Address Management
- Vulnerability Management

+ custom integrations

2 - Process

Correlating gathered context data with real-time Defender for Endpoint telemetries.

- Extensive historical context enables accurate incident analysis.
- Context is continuously kept up to date.
- DEFCOM processing can be configured to address your unique needs.

3 - Consolidate

Defender for Endpoint tags are added/removed based on configured logic.

- Standardized naming convention for tags.
- Seamless Defender integration.
- Fully utilizing native Defender for Endpoint features, leveraging tags for: custom RBAC definitions, device discovery policies, device scores, etc.

Security isn’t a feature, it’s the foundation

info@cyberhorses.io