Corporate Microsoft Security Operations Analyst Training

Drive Team Excellence With Expert-Led Enterprise Cybersecurity Skilling

edstellar®

The Evolution Of Enterprise Upskilling

Legacy Upskilling Challenges

Scattered vendors

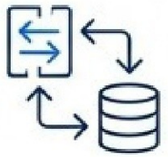
High administrative overhead

Content update delays

Logistical complications across multiple geographies

Unified Training Management

Edstellar's centralized platform



Seamless HRMS integration

Verified trainers

Tailored enterprise licensing

Scalable Enterprise Capability

Consistent global training quality

Hassle-free administration

15% to 30% reduction in total training costs

edstellar®

Executive Program Summary

40-45 Hours

Comprehensive Duration

Instructor-Led

Premium Group Format

Virtual / On-Site / Off-Site

Flexible Delivery Modalities

10,000+ Trainers

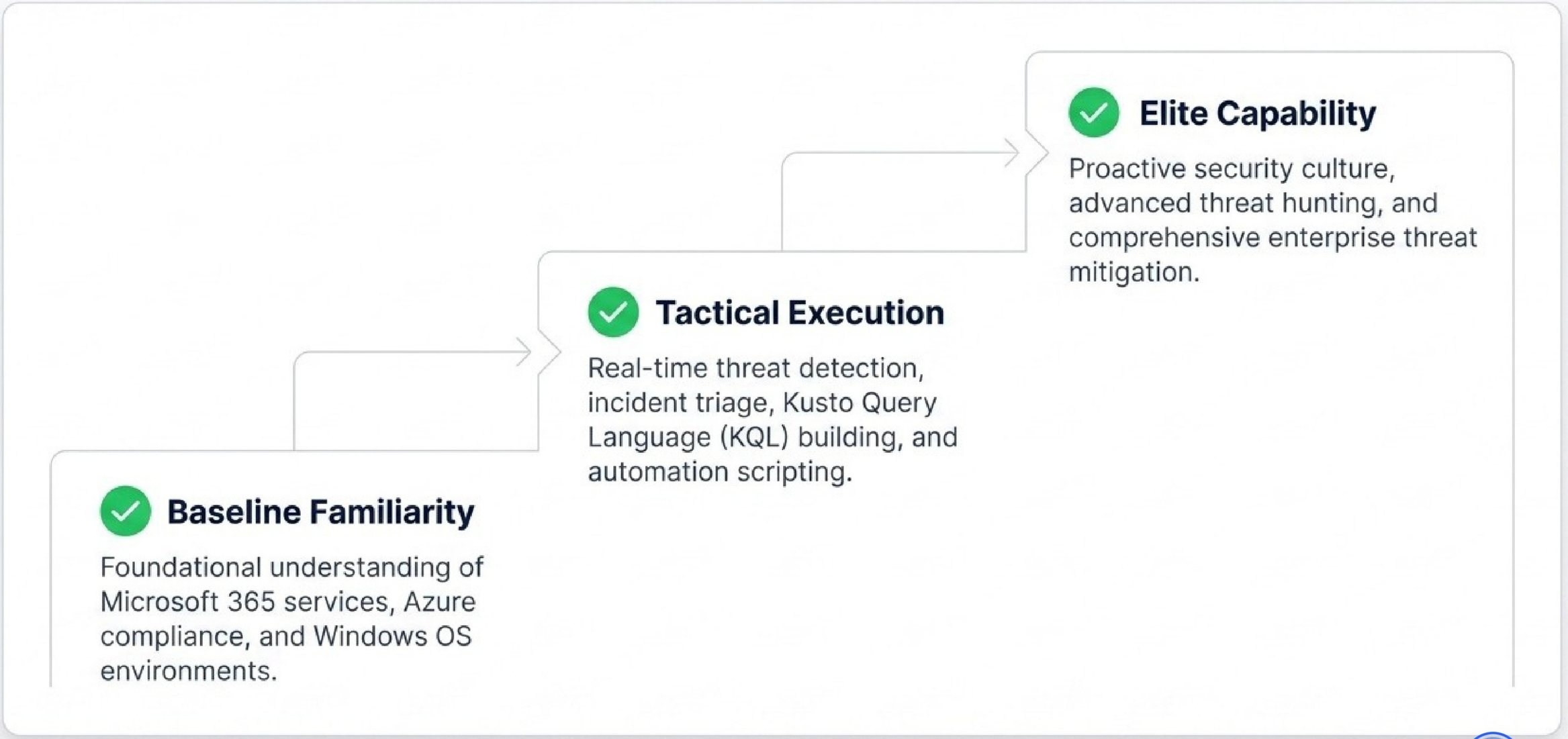
Verified Domain Experts

Official Certificate

Managed Certification

edstellar®

The Capability Activation Staircase



edstellar®

Strategic Curriculum Framework

Phase 1: Comprehensive Threat Mitigation

Modules: Microsoft Defender for Endpoint, M365 Defender, Azure Defender

Securing the perimeter, identities, and cloud workloads through advanced protection strategies and incident handling workflows.

Phase 2: Advanced Analytics And Investigation

Modules: Kusto Query Language (KQL), Azure Sentinel Configuration

Descriptor copy: Building automated multi-table statements and configuring log ingestion policies for intelligent threat detection.

Phase 3: Proactive Threat Hunting

Modules: Sentinel Detections, Playbook Orchestration

Descriptor: Utilizing Entity Behavior Analytics (UEBA) and custom Jupyter notebooks to proactively identify and neutralize cyber threats.

Phase One: Perimeter And Cloud Defense

Endpoint Protection Strategies

Deploying Microsoft Defender, remote response capabilities, and forensic evidence collection.

Azure AD Identity Protection

Conditional Access policies, insider risk management, and identity-based threat detection.

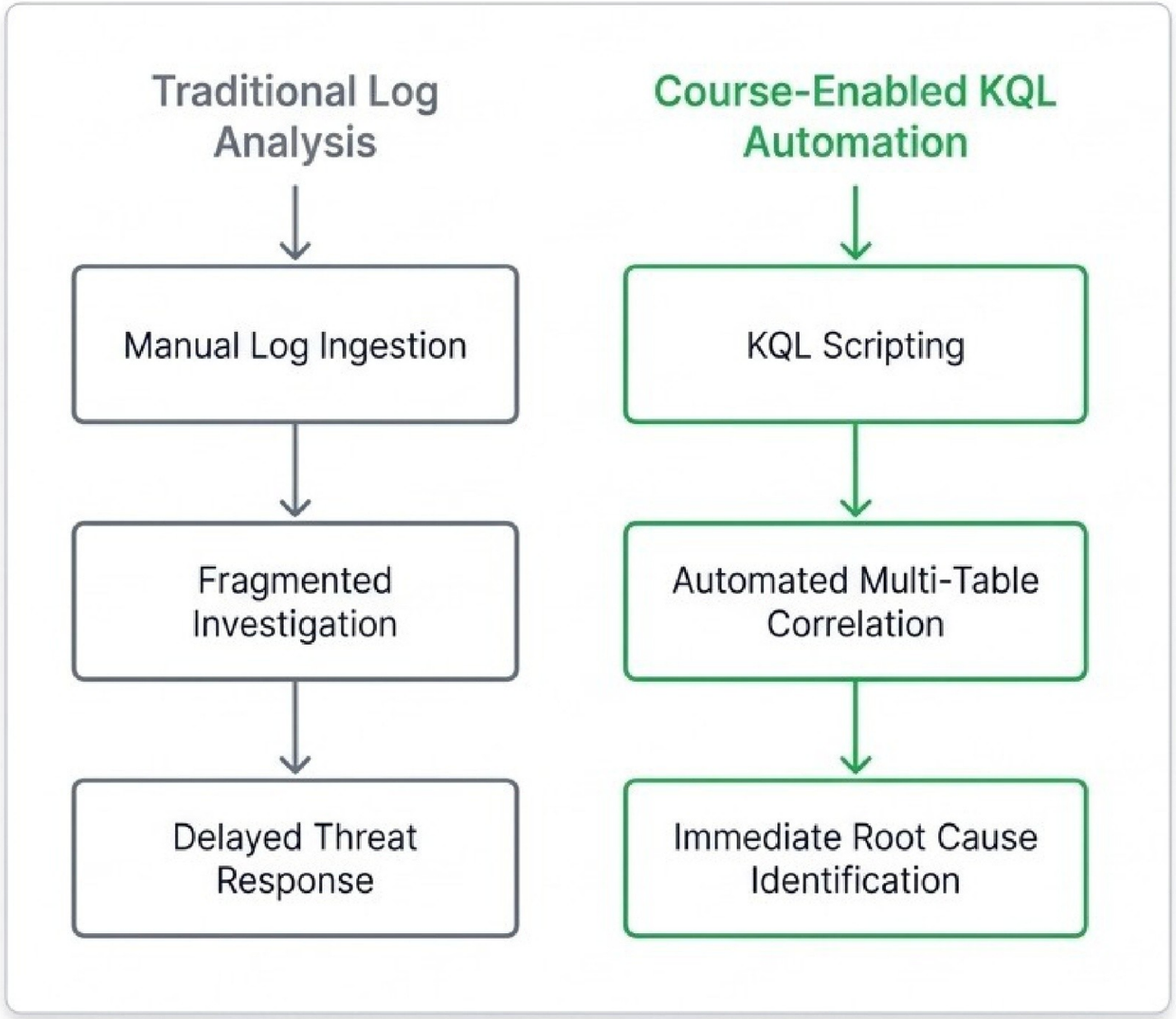
Incident Handling Workflows

Alert triage, risk prioritization, and automated response orchestration.

Cloud Workload Planning

Securing hybrid environments and integrating Azure Security Center best practices.

Phase Two: The Automation Advantage



Security Automation

Enhancing efficiency and mitigating threats swiftly.

Log Analysis Automation

Streamlining data insights and reducing errors.

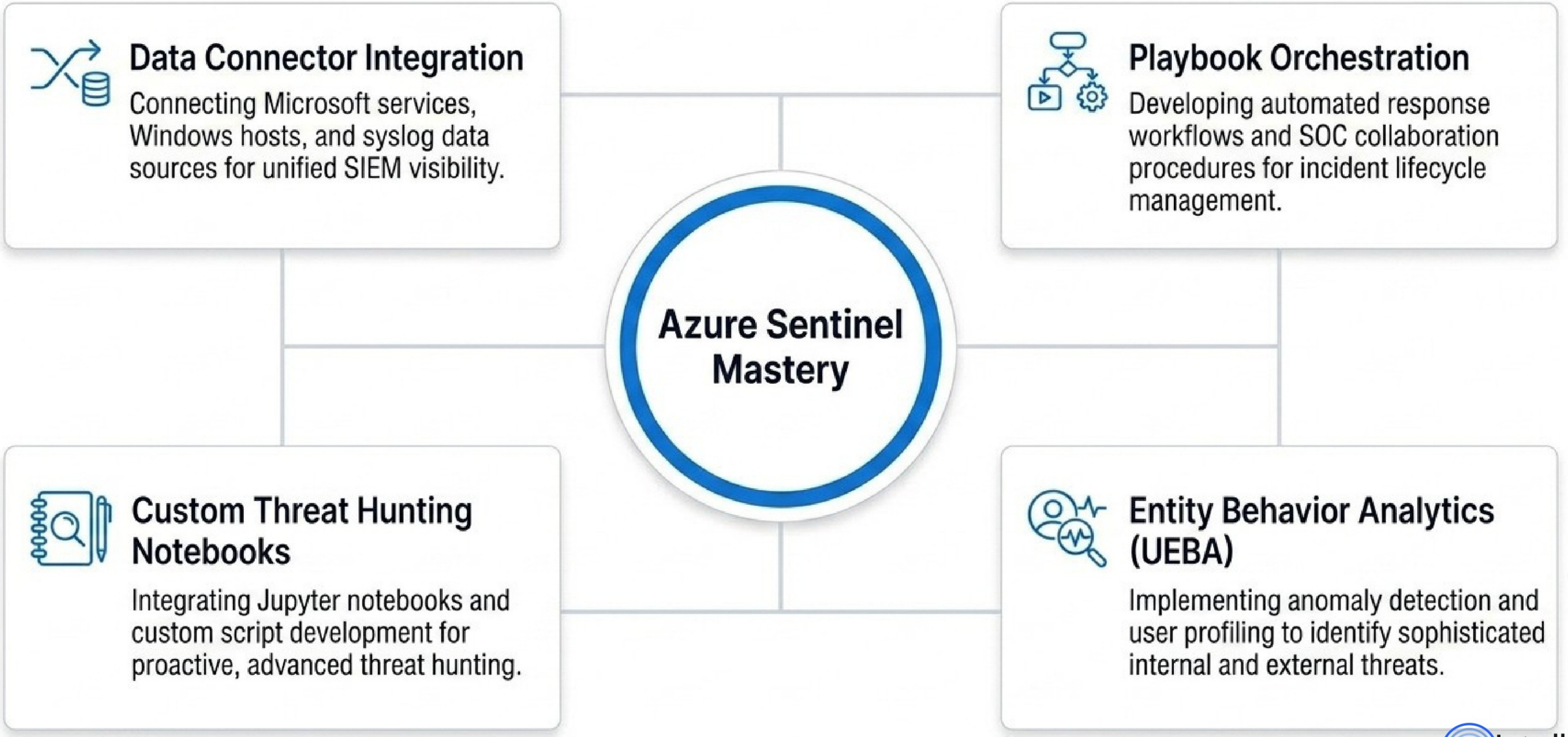
Root Cause Identification

Determining fundamental causes to prevent recurrence.

Incident Response Automation

Minimizing human error and ensuring consistent threat handling.

Phase Three: Proactive Enterprise Security



Data Connector Integration

Connecting Microsoft services, Windows hosts, and syslog data sources for unified SIEM visibility.

Playbook Orchestration

Developing automated response workflows and SOC collaboration procedures for incident lifecycle management.

Custom Threat Hunting Notebooks

Integrating Jupyter notebooks and custom script development for proactive, advanced threat hunting.

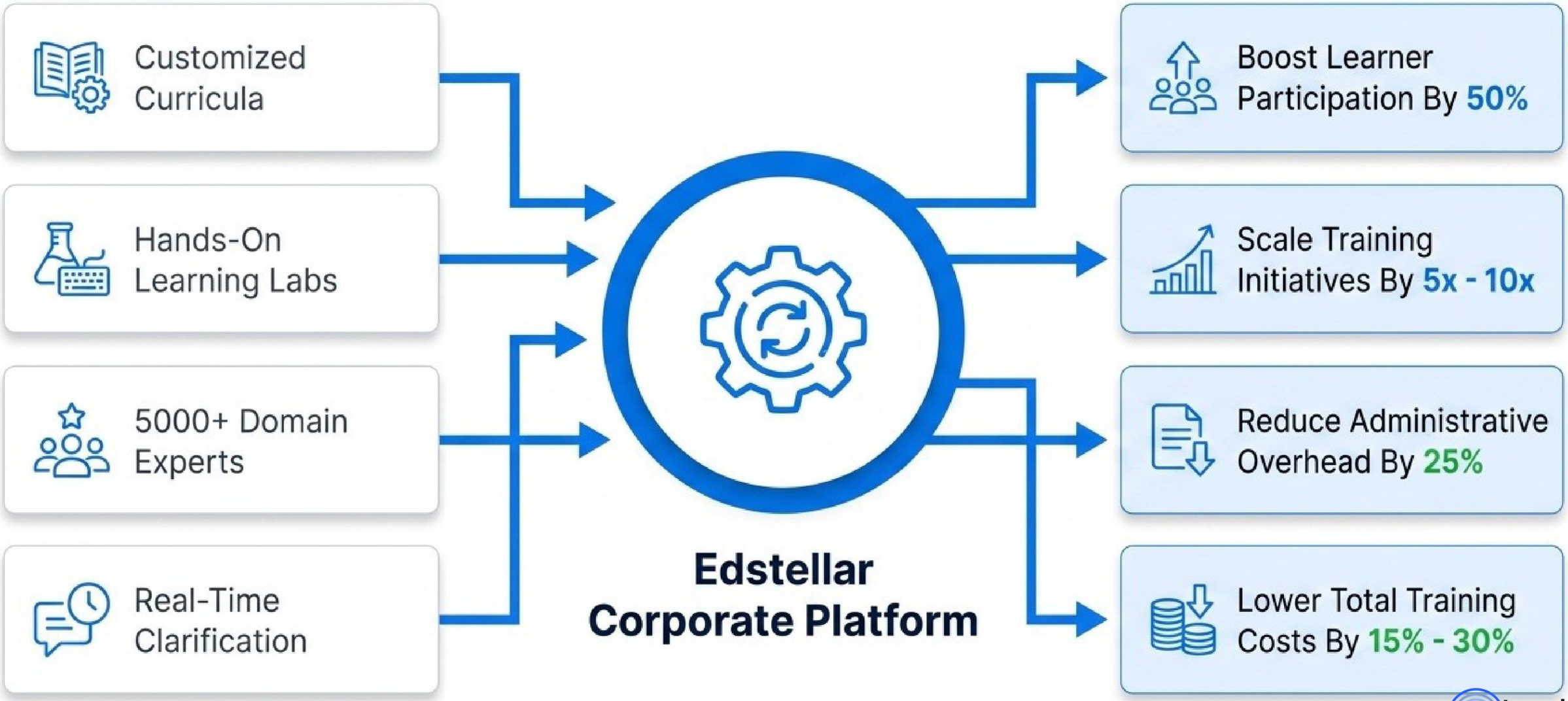
Entity Behavior Analytics (UEBA)

Implementing anomaly detection and user profiling to identify sophisticated internal and external threats.

Organizational Challenge Alignment

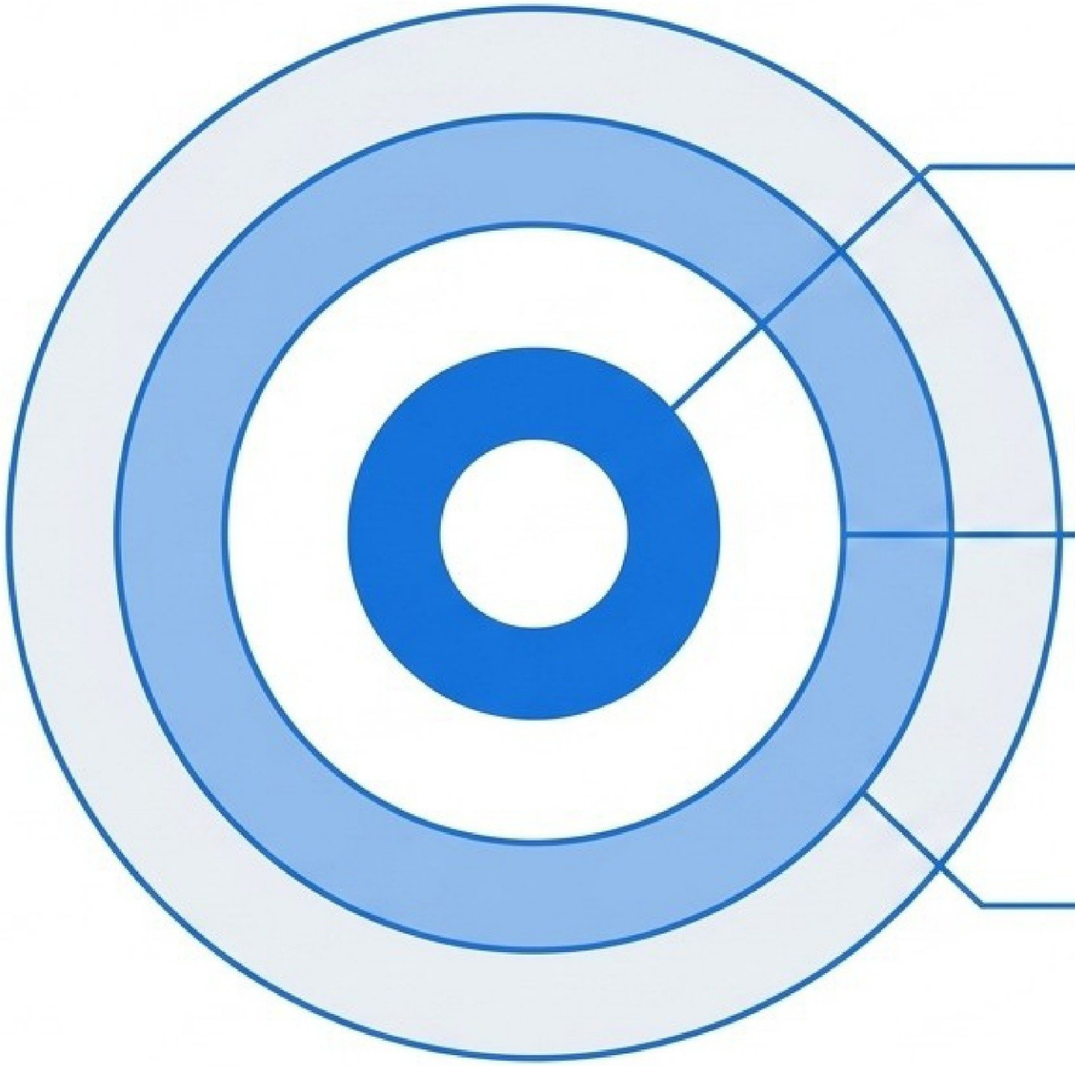
Enterprise Challenge	The Edstellar Solution	Business Outcome
Scale Complexity And Diverse Needs	Unified Training Management Dashboard	**Scale** Training Operations **5x to 10x**
Administrative Overhead And Logistics	Fully Managed Training Services	**25% Reduction** In Administration Time
Budget Constraints And Vendor Sprawl	Tailored Enterprise Licensing Models	**15% to 30%** Improvement In Cost Efficiency

The Skill-To-Value Transformation Engine



edstellar®

Target Audience Alignment



Tactical Execution

Roles: SOC Analysts, Security Engineers, IT Security Analysts.

Focus: Real-time monitoring, triage, and direct threat mitigation.

Heading: Operational Management

Roles: Incident Response Teams, Network Security Teams, Vulnerability Management.

Focus: System architecture, protocol enforcement, and coordinated response.

Heading: Strategic Oversight

Roles: Security Operations Managers, Threat Intelligence Analysts.

Focus: Proactive security culture, risk management, and enterprise-wide defense planning.

Flexible Enterprise Deployment

Virtual Live Training

- Global reach from any location
- Consistent training quality across teams
- Zero travel requirements

On-Site Face To Face

- Tailored to specific workplace environments
- High engagement through direct interaction
- Hands-on process demonstration

Off-Site Face To Face

- Distraction-free dedicated scheduling
- Dynamic environment away from office disruptions
- Improved team bonding and morale

The Microsoft Security Operations Analyst training exceeded my expectations in every way. As a Lead Cybersecurity Analyst, I gained comprehensive knowledge of practical applications that transformed my approach... My productivity and technical capabilities have increased dramatically since applying these concepts. The instructor's expertise in practical simulations made complex concepts crystal clear and actionable."

Thurman Palmer, 13pt
Lead Cybersecurity Analyst, 12pt
Security Operations Center, 12pt

edstellar®

Borderless Skilling Infrastructure

100+ Countries

Global Delivery Capability

Seamless training execution across North America, EMEA, and APAC regions.

10+ Languages

Localized Instruction

Expert-led sessions available in English, Español, Deutsch, Français, 日本語, and more.

edstellar®

Plan Your Skill Transformation

Email: contact@edstellar.com

Phone (US): +1 682 297 4830

Phone (UK): +44 151 453 4009

edstellar®