



SERRAFORM

Microsoft Sentinel

Intelligent security analytics and threat intelligence across the enterprise



The Challenge

Processing overwhelming data volumes, navigating complex threat landscapes, managing resource-intensive security operations, and responding efficiently to security incidents.



Cloud-Native and Scalable

Easily scale your security measures as you grow, eliminating the need for more infrastructure, making it cost-effective.



Threat Intelligence

Leverage AI and advanced analytics to detect and respond to threats. Get protection against the most sophisticated attacks.



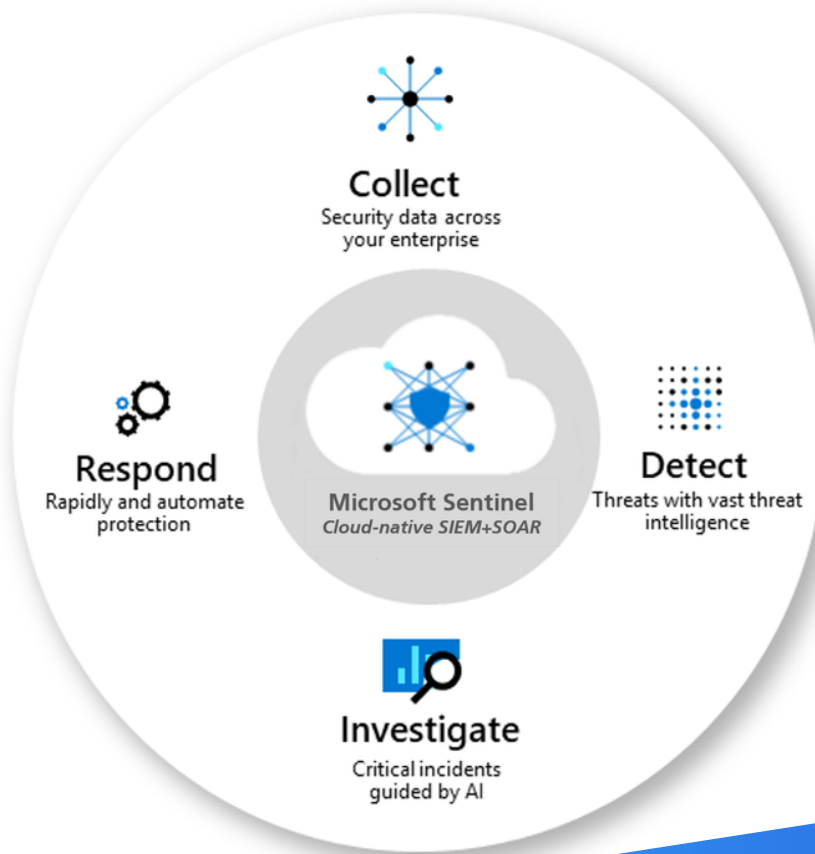
Seamless Integration

Integrate with existing systems and applications, offering a unified and comprehensive view of an organization's security landscape.



contact@serraform.com

www.serraform.com



Objectives

Get unlimited cloud speed and scale that empowers your SOC. See and stop threats across your entire enterprise with intelligent security analytics and advanced ML.

Considerations

We want to understand your SOC operations as they exist today, and help you elevate your SIEM and SOAR capabilities so that you can do more with less.

Our Implementation Approach (4-6 weeks)

- Define your project scope
- Collaborative planning & design sessions
- Gather business requirements
- Provision Microsoft Sentinel + Log Analytics
- Enable data connectors
- Deploy workbooks for interactive visibility
- Define roles and responsibilities
- Deploy advanced analytics
- Create custom playbook automations
- Provide guidance and recommendations
- Knowledge transfer and know-how
- Advanced SIEM + SOAR roadmap strategy



contact@serraform.com

www.serraform.com