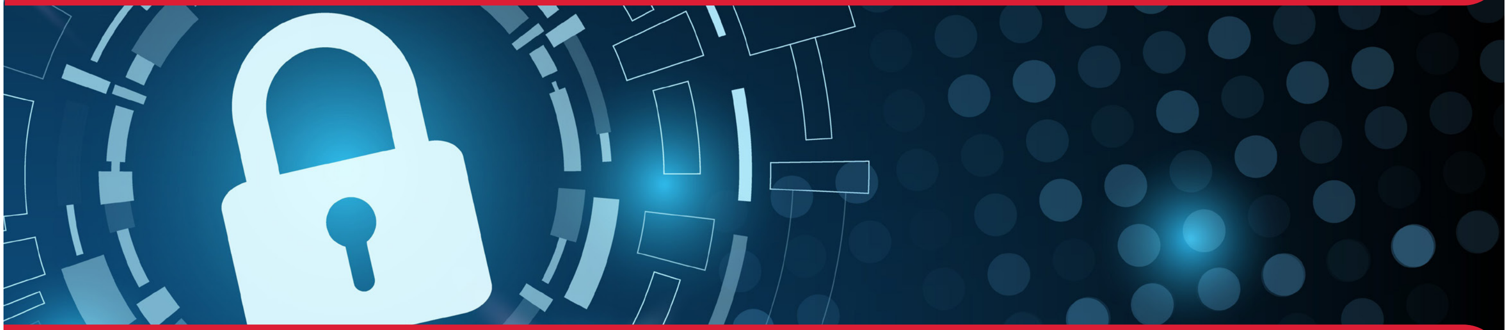
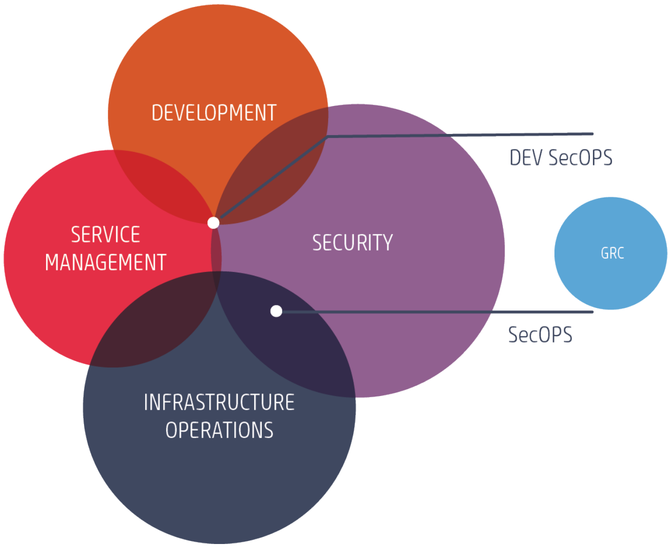


Integrated Security Operations - iSecOps

Many IT leaders today find themselves facing a growing tension between ensuring that their organization, it's systems and data are secure, while at the same time supporting application performance and accessibility requirements from an ever-increasing user base and growing budgetary pressure. This tension is real and can create competing priorities if not addressed.

To close this gap, IT leaders often implement cross-functional teams, like SecOps or DevSecOps, to enhance the connection, collaboration and communication between their security and operations teams. At the core of SecOps is an understanding that the more security aware the operations teams are, the easier it is to balance the priorities and ensure applications remain secure and accessible.



Can you answer YES to these questions:

VISIBILITY

- Do you have continuous visibility into known, unknown, and shadow assets?
- Do you continuously monitor the security "state" of your assets?

CONTEXT

- Do you understand which threats and weaknesses to prioritize?
- Do you know how to measure security posture and assurance?

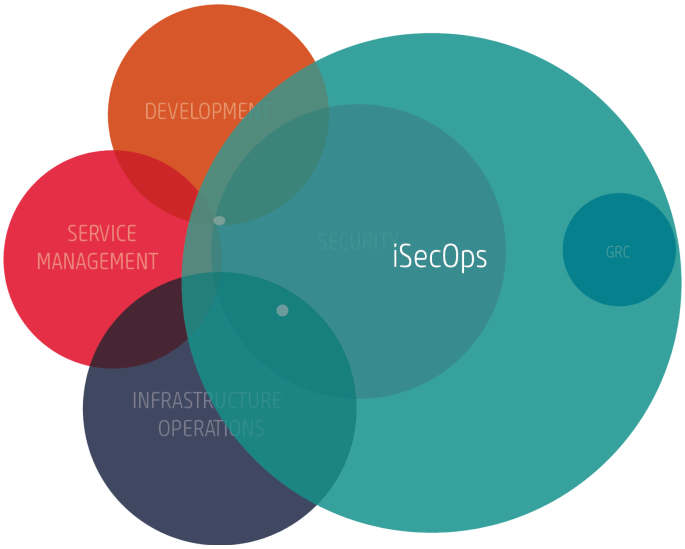
ACTION

- Are you vigorously protecting your assets with the latest updates and proactive techniques?
- Are you able to take decisive actions to respond to attacks?

Making SecOps Integrated: iSecOps

iSecOps takes a holistic view of the priorities across all IT functions, typically starting with Governance, Risk and Compliance (GRC). It looks at how existing toolsets are currently being used and identifies how they can be better leveraged – e.g., security tools helping out with operations and vice-versa. This integrated approach prioritizes security, drives more value from existing technology investments, and ultimately reduces organizational risk.

SERVICE OVERVIEW



iSecOps addresses questions like:

- What are the specific security requirements of your Human Resources and Legal departments? Are they understood? How are they being supported?
- What governance and compliance issues do your functional departments have to address? Do they conflict with each other? How might they impact application performance?
- Are you getting full value from the tools and licenses you own? Can you improve operational effectiveness and increase the visibility into your environment without any additional expense?

HOW TO GET STARTED

The need to have an integrated view on security and operations has never been more pressing. Our iSecOps approach allows our clients to start immediately with either:

TARGETED RESPONSE: Address a specific functional challenge or audit finding.

We work with you to identify the appropriate cross-functional areas, and:

- assess your tools
- leverage what you have today to remediate the issue of concern
- measurably reduce organizational risk and create business value

Some common examples: Ransomware Protection and Response, Multi-Cloud Provider Integration, Asset Management, Patch Management, Identity and Access Management, M365 Full Use Implementation, etc.,

ALL-INCLUSIVE REVIEW: Assess the overall environment and develop and iSecOps Roadmap.

We look at all IT operations across your organization and with an iSecOps view we:

- identify and prioritize the security or operational gaps
- provide targeted tool or process remediation action plans
- work with you to develop an executable Roadmap aligned to organizational strategy

online
business systems

Contact:
Online Business Systems
1.800.668.7722
info@obsglobal.com

About Online Business Systems

Founded in 1986, Online Business Systems is a Digital Transformation and Cybersecurity consultancy. We help enterprise Clients by designing improved business processes enabled with secure information systems. Our unsurpassed delivery, our people, and the Online culture of loyalty, trust and commitment to mutual success set us apart.