ServiceNow Security Operations (SecOps)

Automated and integrated security solutions that reduce risk

servicenow Partner

Elite

The modern Security Operations challenge

SecOps teams work hard at keeping organizations safe from ever-evolving threats while supporting new digital transformation initiatives. But often, IT security programs are hampered by siloed teams, manual processes and disconnected tools and datasets.

Cyber threats are becoming more advanced, as demonstrated by the 2020 SolarWinds breach. SecOps programs must transition to proactive, automated and integrated solutions. This requires the expertise that Edgile brings in three interrelated areas:

Risk management

Identity and access management (IAM)

Security in cloud and hybrid environments

Automate security tools to run seamlessly with IT

Leveraging the built-in SecOps capabilities in ServiceNow, Edgile's Quick Start implementation packages bring incident data from your security tools into a structured response engine that uses intelligent workflows, automation, and a deep connection with IT to prioritize and resolve threats based on the impact they pose to your organization.

We help you demonstrate to management along with risk, compliance and audit stakeholders that your SecOps capabilities are effectively meeting objectives and actively reducing risk from day one. This means you spend less time responding to assurance teams and more time mitigating security risks.

Scale security solutions to specific threat responses

ServiceNow SecOps applications delivered by Edgile allow you to scale security solutions to meet business needs in four critical areas:

Security Incident Response
Speed up critical incident remediation with powerful workflow and automation tools

Vulnerability Response
Identify and respond to vulnerabilities quickly and efficiently through a single shared platform

Configuration Compliance
Prioritize and remediate misconfigured assets using data from third party scans

Threat Intelligence
Find and report Indicators of Compromise (IoC) and hunt for low-lying attacks and threats

Edgile's ServiceNow SecOps service areas model

Edgile's ServiceNow SecOps applications give your business unparalleled control over security remediation efforts. You get:

• **Precision**—Comprehensive incident reports built on a single system of records that captures everything related to the incident, including tasks, attachments, post incident reviews, work notes, and more.
• **Visibility**—Fully understand broad business impacts and immediately know who owns an asset before taking action to avoid business disruption when patching or taking systems offline
• **Speed**—Faster remediation with orchestration.

Service Areas / Security Operations

Service Areas	Security Operations		
Security Program Office	Organizational Model	Roles & Responsibilities	Program Status
	Policies	Standards	Process & Procedures
	Training & Awareness	Executive Level Reporting	KPI & KRI Monitoring
Vulnerability Response	Automated Scanning	End User Vuln Reporting	Vulnerability Impact Analysis
	Vulnerability Prioritization	Vulnerability Exception Mgmt	Vulnerability Remediation
	Vulnerability Orchestration	Rescanning for Closure	
Security Incident Response	Scenario Analysis	Playbooks / Runbooks	Response Plans
	Prioritized Alert Ingestion	End User Incident Reporting	Incident Impact Analysis
	Incident Prioritization	Incident Remediation	Incident Orchestration
	Incident Exception Management	Post Incident Review	Phishing Mitigation
Threat Intelligence	Threat Data Sourcing	Record Enhancement	Threat Hunting
Configuration Compliance	Regulatory Aligned Baselines	Automated Config Scanning	Config Prioritization
	Continuous Monitoring	Config Remediation	Config Orchestration
	Rescanning for Closure	Config Exception Management	
Integrated Support Services	Asset Inventory Management	Patch Management	Application Portfolio Management
	Config Management (CMDB)	Change Management	IT Services Management
	Software Asset Management	Penetration Testing	Security Awareness
	Network Operations	Security Operations	Red Team / Blue Team
	Forensics	Secure Code Review	Secure SDLC

Services implemented across seven layers:
- Governance
- Roles and Responsibilities
- Process and Procedure
- Reporting, SLA and Metrics
- Technology
- Training and Awareness
- Assurance

Connect with us to get started

To learn more on how to leverage built-in SecOps capabilities in ServiceNow, please contact:

Brian Rizman
(908) 489-3293
brian.rizman@edgile.com

David Deckter
(312) 371-6363
david.deckter@edgile.com

Edgile: We Secure the Modern Enterprise[SM]
Edgile is the trusted cyber risk and regulatory compliance partner to the world's leading organizations. We have over two decades of deep expertise in three interrelated disciplines—Security and Risk, Information and Cloud Security, and modern Identity Access and Governance. As a ServiceNow global Elite Partner, Microsoft Security System Integrator of the Year and SailPoint Admiral Delivery Partner three years running, Edgile is uniquely positioned to deliver strategic, business-aligned risk management services that drive secure and compliant growth for our clients.

Identity
Information
Risk and Compliance