

Security Operations Engineering

Prepare, Prevent, Protect

As organizations expand, they provide a target rich environment for malicious actors, and modern organizations must have a clear understanding of the challenges involved in the protection of the larger threat landscape. Organizations must shift from the less effective traditional, reactive model to the modern, proactive dynamic defense model.

Protiviti's security engineering experts deliver all facets of the modern security operations program in a collaborative, knowledge-aware approach. Our services give organizations the means to detect, analyze and neutralize threats before they can cause harm to the organization, maximize resource effectiveness, and provide the tools, measurements and knowledge to mitigate risk. Protiviti plans, builds and implements secure and high performing security operations infrastructures across all flavors of on-prem and cloud hosted tools.

Securing and
protecting the
Enterprise



Key Themes of Security Operations Engineering



Plan, Build, Run

Cyberattacks which target organizations are increasingly becoming the norm, and businesses must keep up with the growing threat landscape. Without functioning security operations, organizations may be at risk of inadequate response and detection of incidents. Planning the business security strategy, building a SOC that focuses on how to best protect the business, and implementing the tools to do so is paramount to minimize the risk of a business falling victim to an attack.



Design & Defense

Cybersecurity professionals must be able to understand threats and emerging attack patterns and develop solutions to best leverage an organization's defenses and controls. Despite the ever-changing nature of cybersecurity threats, Protiviti experts can guide organizations toward a forward-facing posture of solution design for prevention, detection, investigation and response. We help ensure security teams are able to prevent threats, mitigate or minimize risks and efficiently manage alerts.



Policy & Reporting Structure

Modern cybersecurity leaders can benefit from strong policies and reporting structure to provide leadership with end-to-end visibility into the security atmosphere of the organization. Organizations must not only align to and protect themselves through external security standards, but understand how organizational security processes can be leveraged to collect, quantify and identify how the organization could be more well protected.




Resource Development

One of the biggest challenges that modern security teams face is limited availability of workforce with cybersecurity expertise. Organizations must possess the ability to assign incidents to the right, skilled cybersecurity resources to maximize productivity, and minimize risk. Protiviti's security operations engineering offering closes the gap of skilled resources by augmenting the team and acting as a force multiplier and skilled practitioner for organizations, ensuring swift action when critical events occur.

Security Operations Engineering

Protiviti's security engineering experts deliver all facets of the modern security operations program in a collaborative, knowledge-aware approach. Our services give organizations the means to detect, analyze and neutralize threats to the organization and provide the knowledge to mitigate risk.



Plan, Build, Run

- Security Operation modeling for businesses
- Threat detection and containment planning
- Automation goal building
- Organizational planning



Resource Development

- Security Resource Maturity
- Resource Provisioning
- Staff Integration
- Staff Development



Definition & Architecture

- Architecture definition for enhanced visibility into threat and incident activity
- SIEM/Monitoring structure architecture design
- Process, metrics and reporting structure development



Program Development

- Security operations program development
- Strategic roadmap development
- Detailed containment automation and playbooks
- Processes & Documentation Development

The Protiviti Advantage



We start with the business problem – and apply the right solutions and technology to achieve business value



We support our clients through entire initiatives – from understanding business issues, to developing a strategy, delivering the implementation and providing ongoing support



Our methodologies are focused on holistically understanding risk – our approach goes beyond identifying gaps, issues or vulnerabilities. We determine root causes, validate issues, and develop short-term and/or long-term recommendation



Integrated approach – we integrate multiple disciplines and emerging technologies such as AI/ML when delivering our solutions



Established partnerships – our subject matter experts partner with major software companies and have access to their products, experts and roadmaps




Technology accelerators – we leverage the intellectual property within our partner ecosystem to help fast track technology deployments




Flexible delivery models – to address short-term skill gaps, deliver projects or transform your organization quickly and cost-effectively

Schedule a Technology Assessment today by contacting us at TechnologyConsulting@Protiviti.com.



 Protiviti.com/Technology Consulting

 TechnologyConsulting@Protiviti.com

 TCblog.Protiviti.com