Wragby Business Solutions & Technologies

Wragby Security Operations Center (wSOC)

Challenges with Existing Security Solutions

- With so many employees working remotely, IT groups are routing more traffic directly to cloud apps, rather than through the network. In this model, traditional network security controls aren't enough. Endpoint signals and identity-based security matter more than ever.

- Also using several security tools that aren't well integrated, correlating signals across your entire environment is tough. To find the real threats, you may spend hours combing through false positives. Alert fatigue is inevitable, making it easy to miss true issues.

Challenges with Existing Security Solutions

- Without visibility across all platforms where business information is stored and transacted, you don't have a full view of your corporate security program and risk profile. Organizations require a holistic view to correlate threats and assess how one threat may impact another resource.

- As more employees use cloud apps and mobile devices for work, the traditional network security perimeter has lost relevance. This puts greater emphasis on endpoint monitoring and protection. But it goes beyond employee devices to visibility across devices, identity, cloud apps, data, and infrastructure.

Challenges with Existing Security Solutions

- The ability to identify compromise rapidly and respond to incidents in the middle of an attack where minutes matter is a major challenge. Also, it's critical that you respond quickly and intelligently. But these are also the moments when adrenaline runs high, and people panic. You may not make the best decisions in a state of high alert. To provide structure during an incident, it helps to have a plan.

Overview of Wragby's Security Operations Center

The Wragby Security Operations Center(wSOC) is a suite of modern and intelligent security solutions built on Microsoft platform to better secure remote workers.

wSOC monitors and analyzes activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise. The wSOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.

wSOC also monitors for vulnerabilities in order to protect sensitive data and comply with industry or government regulations.

Benefits of Wragby's Security Operations Center

- The key benefit of deploying the Wragby Security Operations Center is the improvement of security incident detection through continuous monitoring and analysis of data activity.
- The 24/7 monitoring provided by a SOC gives organizations an advantage to defend against incidents and intrusions, regardless of source, time of day, or attack type.
- Having a security operations center helps organizations close that gap and stay on top of the threats facing their environments.

Components of the Wragby Security Operations Center

Based on our choice to focus on Security Management, our SOC Practice will be built on the following Microsoft products and services.

- **Gain Visibility into Security Health**
  - Azure Sentinel
  - Azure Security Center
  - Azure Network Watcher
  - Azure Monitor
  - Microsoft 365 Secure Score
  - Office 365 Advanced Threat Protection
  - Office 365 Threat Intelligence
  - Microsoft Cloud App Security
- **Detect and Respond to Threats**
  - Azure Sentinel
  - Azure Security Center
  - Azure Advisor
  - Microsoft Defender Advanced Threat Protection

Thank You