Cyber Security

Managed Threat Detection and Response

A successful MD&R solution is structured around:

- **Endpoint detection and response** to Blocks ransomware and malware
- **Network detection and response** to detect early signs of an attack on your network
- **Cloud detection and response** for Microsoft 365, Google Workspace, Dropbox, AWS, Azure, etc. Salesforce, ZenDesk and Okta
- **Suspicious Email Analysis Service (SEAS)** empowering employees to send suspicious emails directly to Field Effect for immediate analysis
- **Vulnerability detection** detecting potential threats such as outdated patches, misconfigurations, externally exposed assets, shadow IT, and more
- **24/7 Security Operations Center (SOC)**
- **Active Response** with several options, from automated to manually verified
- **Threat Intelligence** Tapping into the global threat intelligence community.
- **DNS Firewall** to monitor and block connections to malicious websites to ensure safe web browsing and Internet access
- **Log retention** to store critical log data to boost Improve your ability to comply with compliance frameworks

Key Issues

- Security products are complex and require appropriately trained personnel
- Networks constantly updated / monitored
- Critical is ability to respond to zero-day
- Solution is supplied through partners that are trained and certified
- Subscription based

Mighty Oaks Wireless Solutions Inc., 29 Burnside Road, Victoria, BC V9A 6Z7
Mighty Raven Technology Inc., Tla'amin Nation, 5246 Beach Road, Powell River, BC V8A 0B1
www.mightyoaks.com, www.mightyraven.com; Contact us at: sales@mightyoaks.com or (250) 386-9398

Cyber Security

Need

Suppliers in the Aerospace and Defence supply chain face ever-evolving cyber security risks and compliance requirements to participate in the industry.

Challenge

The Aerospace and Defence companies, both SME and large enterprises face these sophisticated cyber threats constantly and must protect themselves against these state-sponsored bad actors. This is key to protecting this sensitive supply chain, those that operate in the supply chain and ultimately the security of the Nation.

The Cybersecurity Maturity Model Certification (CMMC) is an assessment framework and assessor certification program designed to increase the trust in measures of compliance. The National Institute of Standards and Technology (NIST) introduced Cyber Security Framework (CSF) in 2014 as a guide to mitigating cyber security risks. In its latest release (2024) assistance is extended to all organizations, regardless of their size and sector. CMMC has three levels based on NIST Special Publication (SP) 800-171.

The Canadian Government is working closely with NIST to ensure the Canadian standard is aligned with our US allies to provide cross border opportunities for Canadian companies.

Impact

Failure to demonstrate compliance with the CMMC security requirements of the NIST SP 800-172 standards could exclude contractors from securing Defence contracts.

Our Background

Since 2002 we have provided software solutions which required compliance with various standards (e.g., PCI-DSS, ISO 2700 and NIST). With customers in Canada, US and Australia we have extensive experience demonstrating compliance.

Our Solution

Our solution provides a systematic approach to protection with a combination of Monitoring, Detection, Response and mitigation. We combine the best-of-breed technologies from industry leading platforms into a comprehensive package. This includes active real-time monitoring, detection and response. This approach is intended to complement your internal IT team and software suppliers by providing a secure environment where they can focus on their key functions.

We frequently prepare Cyber Security Attestation Letters and score cards outlining your cyber security posture for you to present to collaborating organizations or prime contractors.

Our MDR

Our Managed threat Detection and Response (MDR) relies on endpoint detection and response to block ransomware and malware, network detection and response to detect early signs of an attack on your network, by protecting devices that cannot be protected by endpoint agents and cloud detection and response

The Suspicious Email Analysis Service (SEAS), empowers your employees to send suspicious emails directly for immediate analysis. Vulnerability detection is used to identify potential threats such as outdated patches, misconfigurations, externally exposed assets, shadow IT, and more.

Our Support

Active Response provides several options, from automated to manually verified. Threat Intelligence taps into the global threat intelligence community. DNS Firewall monitors and block connections to malicious websites and Log retention boost your ability to comply with compliance frameworks.

Mighty Oaks Wireless Solutions Inc., 29 Burnside Road, Victoria, BC V9A 6Z7
Mighty Raven Technology Inc., Tla'amin Nation, 5246 Beach Road, Powell River, BC V8A 0B1
www.mightyoaks.com, www.mightyraven.com; Contact us at: sales@mightyoaks.com or (250) 386-9398