Decisive™
A CALIAN COMPANY

Extended Expertise. Yes there is more.

Add-on Services

Supplementary Offerings Designed to Enhance Core Capabilities

Welcome to Our Library: Feel Free to Make Some Noise

Sitting adjacent to our core service offerings, Decisive has many capabilities which we offer to our clients. These services are complementary, however they can also stand on their own, as high value security controls for your environment.

Gotta cover your bases

It is imperative for businesses of all sizes to deploy security controls to protect their data. These controls begin with a foundational layer which is not a recommendation but a necessity, as the loss or compromise of data can lead to significant financial losses, damage to reputation, and legal repercussions. Navigating the many products on offer to make an informed decision can be daunting task. Determining how to invest a limited budget to provide adequate coverage can also be a challenge. Decisive Group has done the research and testing for you, partnering with industry leading vendors to offer competitive services which are designed to combat today's modern threats.

Advanced Endpoint Security

Endpoint detection and response (EDR) is a critical security control that extends beyond traditional signature-based detection methods. Endpoints, such as computers, laptops, and mobile devices, serve as the entry points to an organization's network and are often the targets of cyber adversaries. Signature-based detection relies on known patterns of malicious code, making it effective against known threats but inherently limited in addressing new and evolving forms of malware. Modern cybersecurity demands a more proactive and adaptive approach, which is where advanced endpoint security comes into play.

Service Features:

- Licensed per agent
- Endpoint security that goes beyond signature-based detection
- Detect known and zero-day exploits and malware variants through behavior analytics
- Block infections in real-time regardless of network connectivity/physical location
- Run domain wide search to find and remove malicious files
- Ability to quarantine hosts

- Threat Intelligence feeds used for threat assessment
- Reduce employee downtime due to infected equipment
- Integrates with SIEM and SOAR for comprehensive security protection
- Advanced customizable automation rules
- Minimal demand on memory/bandwidth/cpu
- No reboots required for agent updates/install
- 24/7/365 Monitoring of Security Events (Requires SIEM subscription)
- Monthly Reporting

CORTEX®

BY PALO ALTO NETWORKS

Vulnerability Management

Vulnerability management, within the broader framework of cybersecurity, stands out as a linchpin in the pursuit of data resiliency. It involves a systematic and proactive approach to identifying, assessing, prioritizing, and mitigating vulnerabilities within an organization's IT infrastructure. As technology evolves, so do the tactics of malicious actors seeking to exploit weaknesses in software, networks, and systems. Vulnerability management serves as a dynamic defense mechanism, continuously scanning and assessing the enterprise landscape to detect and address potential points of vulnerability before they can be exploited.

Service Features:

- Options for scheduled and continuous vulnerability scanning
- Scheduled scans are performed at a regular cadence
- Customized scan results and prioritization
- On demand scans against new critical vulnerabilities are performed
- Customized remediation plans
- Track vulnerablitites scan over scan to measure effectiveness
- Asset Modeling results are fed into the Decisive SIEM (if subscribed) increasing the fidelity of security investigations

tenable.io™

Security Awareness and Phishing

No data resiliency plan is complete without attention paid toward the human element of security, which is where awareness training plays a pivotal role. Employees, being the frontline defenders against cyber threats, need to be equipped with the knowledge and skills to recognize, prevent, and respond to security incidents. Security awareness training goes beyond mere theoretical knowledge, actively engaging employees to understand the importance of cybersecurity in their daily tasks and fostering a culture of vigilance.

Phishing, a prevalent and ever-evolving cyber threat, often exploits human vulnerabilities to gain unauthorized access to sensitive data. Hence, phishing simulation exercises are a fundamental requirement within security awareness training programs.

Service Features

- Licensed by number of employees in scope
- Ability to "port over" existing licensing or provide
- Regular assignment of security training to employees based on topical themes
- Tracking and reporting of training completion across teams
- Periodic testing of organization and/or specific teams via phishing campaigns
- Remedial training to those who fail testing
- Monitored mailbox for phishing reporting
- 24/7/365 Analyst team investigating reported messages

KnowBe4
Human error. Conquered.

Let us help you with Strategic Projects

Virtual Chief Information Security Officer (VCISO)

When budget and team throughput are a consideration, let Decisive help you decide how to best allocate resources. Responding to a high priority incident? We can help there too.

Penetration Testing

Our team can find the weak points in your armor before someone else does and provide direction on how to fix them.

Threat Risk Assessments

Awareness and visibility are essential precursors to strategic planning. Our established process will assist in preparation for critical decision making.

Network Transformation

Decisive's experts are no strangers when it comes to flat networks. Introducing network segmentation can increase return on investment and lock down internal traffic.

Defense in Depth for Data Resilience

Defense in depth is a security strategy that layers multiple security controls and measures across the various components of your infrastructure. This approach increases data resiliency by ensuring that if one layer of defense is breached, others still stand to protect. By implementing a diverse set of security controls, organizations can create a robust barrier against a wide range of threats. This redundancy in security measures ensures that attackers face multiple hurdles, making it more difficult to compromise data, and provides time for the organization to respond to threats before they escalate. Regular security training for employees, for example, can reduce the risk of data breaches caused by human error, while advanced endpoint security can actively block actions taken them in the event something is missed. By integrating these diverse layers of security, organizations can protect their data from a multitude of angles, ensuring that even in the face of a successful attack, the resilience of the system as a whole can prevent data loss or corruption.

How to contact us

☎ 1 (855) 336-3700

✉ inquiry@decisivegroup.com

118 Iber Road, Suite 105,
Ottawa, ON K2S 1E9

Prepare
Respond
Recover

You need the confidence that comes with knowing you are prepared when your data is threatened.

- Secure Backup
- Managed SIEM
- Disaster Recovery
- Managed Firewall

Decisive
A CALIAN COMPANY