Security Operations and Response

COGNITIVE TECHNOLOGY TO PREVENT, DETECT AND RESPOND TO ATTACKS

Prevent. Detect. Respond.

It is a simple concept, yet the cleverness of today's cyber attacks makes protecting your organization more complicated every day. It requires strategic security operations that only an experienced, security savvy partner can provide.

> **Today's data-driven, highly distributed environment, has serious threats that must be addressed aggressively. It requires an integrated system of analytics, real-time defenses and proven experts, so you can make strategic decisions about how to safeguard your business.**

Protecting your perimeter and all access points involves a layered security protocol, which provides an end-to-end barrier against cyber attacks. The process starts with creating insights. Innovative security operations and response architectures use advanced cognitive technology to deliver insights that lead to response across endpoint, network, cloud and users.

Mainline's comprehensive solution to prevent, detect and respond to attacks includes:

Network Protection – Protect your entire network in real time with actionable insights. Known and unknown threats can be identified with behavioral analysis and intelligence. Increased control over applications and user behavior can reduce exposure. Automated threat intelligence feeds and virtual patch technology save time and resources.

Endpoint Security – When your organization is breached you must be able to assess vulnerabilities, accelerate risk prioritization and quickly respond to the threat across all endpoints – on and off the corporate network. Mainline's Endpoint Security solution enables you to monitor and secure every endpoint before, during and after an attack. Also, sharing real-time incident response across endpoints will minimize damage.

Security Intelligence and Analytics – Security intelligence enables you to detect and prioritize the threats that pose the greatest risk and require immediate attention. Behavioral anomaly detection helps identify high-risk threats. An integrated architecture allows you to analyze user and asset data vulnerability. Overall, you gain full visibility into network, application and user activity.

Incident Response – An integrated incident response solution makes security alerts instantly actionable, provides valuable intelligence and incident context, and enables adaptive response to complex cyber threats. Automated incident response provides the agility, intelligence, and sophistication needed to contend with complex attacks.

Fraud Protection – Prevent the full range of threats responsible for most online, mobile and cross-channel fraud. By analyzing risk factors and flagging high-risk transactions, you can prevent the root cause of fraud. At the same time, the solution allows you to continue providing high quality experiences with transparent protection to customers who are making legitimate transactions.

Mainline's Security Operations and Response solutions are based on avoiding risk in the first place.

To learn more, call us toll-free at 866.490.MAIN(6246) or speak with your Mainline Account Executive.

Security Operations and Response

COGNITIVE TECHNOLOGY TO PREVENT, DETECT AND RESPOND TO ATTACKS

Security Services From Mainline

Penetration Testing – We conduct internal and external pen testing to identify vulnerabilities to your network, applications, computer systems, and employee access points, to name a few.

Security Controls Review – During this high level review we gather baseline information about the vision and current state of your security program. A comprehensive report is provided.

Managed Services or Staff Augmentation – Mainline offers short- and long-term staffing to fill any resource gaps you may have.

Governance and Risk Management Review – This custom, in-depth assessment includes a review of your current risk management program. A gap analysis report is provided.

Risk Management Through Business Continuity Planning

A very important part of risk management is having a business continuity plan (BCP). BCP is a core business discipline that establishes a company's ability to respond and recover in a crisis. An enterprise business continuity plan provides the framework, planning and tested recoverability required to respond to, and manage, business recovery when an outage occurs.

You can manage your risks by ensuring you have a secure environment and by having a business continuity plan in place in the event of an incident, whether man-made or natural. Mainline can integrate BCP with your information protection solution.

Comprehensive Security Solutions From Mainline

3 Pillars of Protection

Security Operations and Response	Information Risk and Protection	Security Transformation

Your biggest risk is not being prepared.

28% likelihood of a recurring breach over the next two years

$3.86 million is the average total cost of data breach

6.4% increase in total cost of data breach since 2017

$148 is the average cost per lost or stolen record

Source: 2018 Cost of Data Breach Study: Global Overview , Ponemon Institute, July 2018