Cyber Security Services

At AUMA, we serve **COMMUNITIES** *not shareholders.*

Protecting your data has never been more critical.

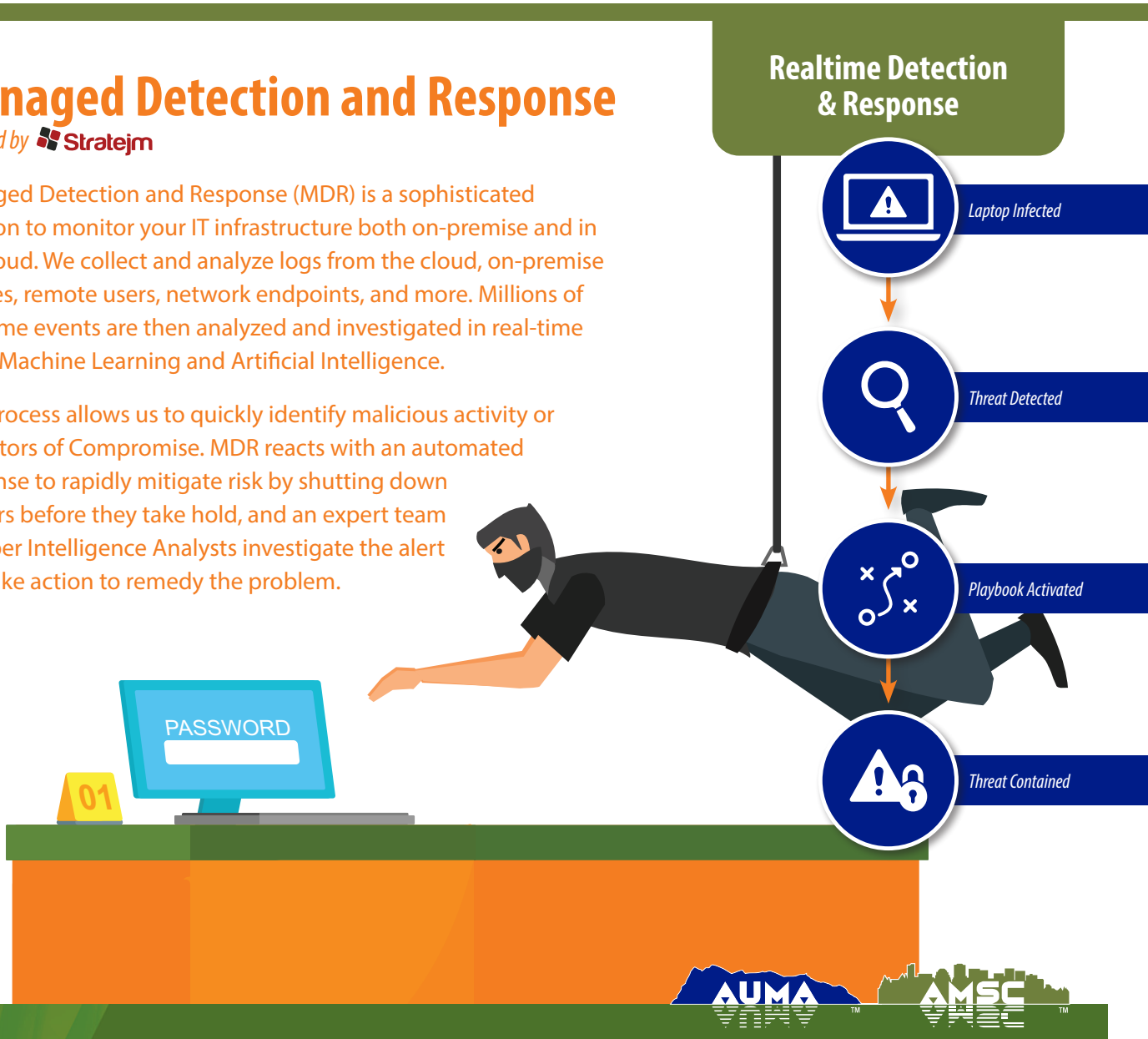
At AUMA, we are always looking for ways to support building strong and resilient Alberta communities. We've developed a suite of Cyber Security Services to strengthen your understanding of your risks, provide protection, and support your recovery & response.

Managed Detection and Response

powered by Stratejm

Managed Detection and Response (MDR) is a sophisticated solution to monitor your IT infrastructure both on-premise and in the cloud. We collect and analyze logs from the cloud, on-premise devices, remote users, network endpoints, and more. Millions of real-time events are then analyzed and investigated in real-time using Machine Learning and Artificial Intelligence.

This process allows us to quickly identify malicious activity or Indicators of Compromise. MDR reacts with an automated response to rapidly mitigate risk by shutting down hackers before they take hold, and an expert team of Cyber Intelligence Analysts investigate the alert and take action to remedy the problem.



Talk to us about your risks and your security options.

310-AUMA | tech@auma.ca | auma.ca/tech

How Managed Detection & Response works:

Your Organization

You will have access to a portal or dashboard, and security analysts will directly interact with your staff to manage issues.

24/7 Cyber Intelligence Centre

A state-of-the-art Cyber Intelligence Center incorporates the traditional functions of a Network Operations Center and Security Operations Center to achieve a holistic, 360-degree view across all IT assets.

MDR includes agile processes that add 24/7 dedicated threat hunting capabilities and access to a team of experts that respond to the constantly evolving threat environment.

Security Information & Event Management as a Service

Using Machine Learning, Artificial Intelligence, and automation you receive immediate protection. Hackers are detected and shut down before they take hold. This feature offers capabilities like visibility, correlation, automated response and remediation in a single, scalable solution.

Incident Management and Response Platform

Our incident management and response enables security teams to identify and investigate incidents, manage events, and automate incident response for fast results. The platform helps detect prevalent and zero-day threats with automated and manual remediation actions in varying attack scenarios.

Log Sources

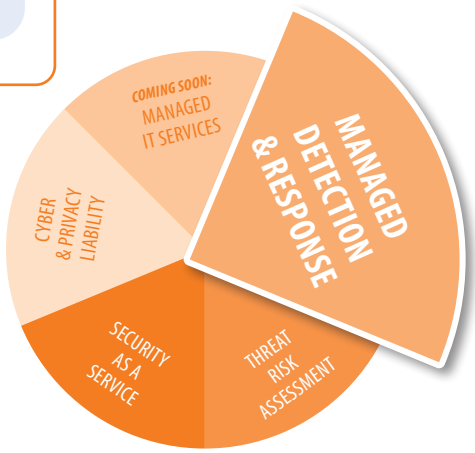
Malicious activities are detected, collected, and analyzed using logs from endpoint devices, EDR, IDS/IPS, anti-malware solutions, DLP, VPN connection web filters, firewalls, honeypots, network devices, and other infrastructure.

In addition to vast amounts of log data being fed into the SIEM for analysis and threat detection, the Incident Management and Response Platform receives the data which enables the security team to take action.

Threat Intelligence Platform

Commercial-grade Threat Intelligence allows you to understand the targets, motives, tactics and attack behaviors. Cyber Intelligence Analysts take full responsibility for curating threat data to produce contextual and actionable outputs that help facilitate informed security decisions.

Ask us about our suite of Cyber Security & Managed IT Services



Talk to us about your risks and your security options.

310-AUMA | tech@auma.ca | auma.ca/tech