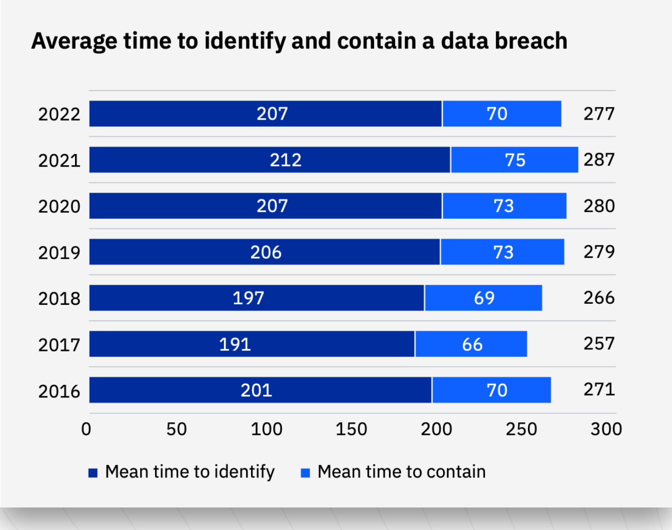
CELERIUM®

We power real-time automated, active cyber defense solutions.

It takes, on average, 207 days* (almost 7 months) to detect a data breach.

Are you concerned about gaps in your organization's systems? Celerium can help with early detection and real-time early defense of cyber threats.



*Source: IBM's "Cost of a data breach 2022" report

HERE'S HOW CELERIUM CAN HELP.

REAL-TIME, AUTOMATED CYBER COMPROMISE ACTIVITY DEFENSE.

Celerium's Compromise Defender™ solution reduces cyber threat overload so you can focus on your priorities. We'll detect and automatically block threats and compromise activity -- and alert you when something needs special attention.

- Easy to implement in less than 30 minutes.
- No new hardware or software required – no black boxes or agents.
- No dedicated staffing required.
- No integrations necessary.
- Patent-pending solution that can help your organization detect and contain cyber compromises.
- Proven through a pilot with the National Association of Counties (NACo) and several counties.

WHAT THEY'RE SAYING ABOUT CDN COMPROMISE DEFENDER™

"This is the simplest thing I've done in my career."
– A CIO on implementing the solution.

"This is immensely useful and fills the gaps."
– A former state CISO.

WHAT DOES IT DO?

Detect and disrupt compromise activity with CDN Compromise Defender™, part of Celerium's Cyber Defense Network (CDN).

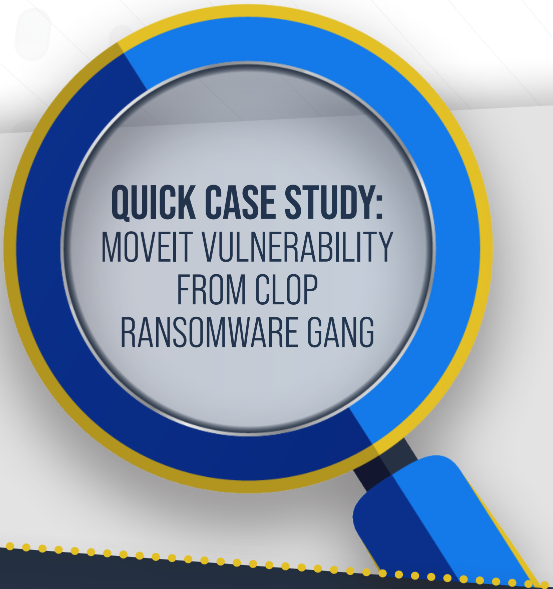
Assessment:
Continuous monitoring of network threats and cyber compromise activity, including early stage reconnaissance and pre-attack infrastructure activity.

Defense:
Turn on automated blocking to stop threats and contain compromise activity.

HOW DOES IT WORK?

- Quick, simple implementation on your organization's public-facing, on-prem firewall (supported firewalls include Palo Alto, Sophos, SonicWall, Cisco Meraki and ASA, FortiGate, PfSense, Ubiquiti, and Watchguard).
- The patented Decision Engine runs securely on the AWS cloud and analyzes syslog/netflow to identify threats.

Use the QR Code to see sample reports



QUICK CASE STUDY: MOVEIT VULNERABILITY FROM CLOP RANSOMWARE GANG

In June, a high-profile vulnerability with the MOVEit file-transfer software impacted federal agencies, universities, and state and local government entities. Celerium quickly added defensive measures against the vulnerability by integrating Government and Commercial IOCs into our CDN Compromise Defender™ solution for automatic blocking.

For customers already using the solution with blocking turned on, their organizations were protected without any further action on their part. Other organizations could stand up defenses in less than 30 minutes against the MOVEit vulnerability. This same process has been and will be used for other vulnerabilities.

ABOUT CELERIUM

Cyber attacks are one of the most significant risks to businesses today. These cyber attacks are magnified since many organizations are overloaded with work, overwhelmed with cyber complexity, and face a shortage of skilled people to deal with cyber-related problems.

That's where Celerium comes in.

Celerium helps overloaded and overwhelmed organizations fight cyber threats through real defensive solutions that can be implemented in 30 minutes and are 100% automated.

Celerium's Cyber Defense Network™ (CDN) powers active cyber defense solutions that are easy to implement and effective in the critical area of compromise activity defense – with an emphasis on community defense. As threat actors focus on finding open doors to gain access to multiple targets, we help improve the collective defense of communities – making cybersecurity efforts more impactful.

Get started protecting your organization from cyberattacks now. Request more information or schedule a demo.

Contact us:

Celerium.com
info@celerium.com

CELERIUM®
CYBER DEFENSE NETWORK
www.celerium.com