CELERIUM-NACo

CYBERSECURITY PILOT PROGRAM

APRIL – JULY 2023

PILOT PURPOSE:

Help overwhelmed county IT staff with early detection and defense of cyberattacks.

EXECUTIVE SUMMARY

In the spring of 2023, Celerium embarked on a four-month cybersecurity pilot program with the National Association of Counties. The pilot's purpose was to help overwhelmed county IT staff with early detection and defense of cyberattacks.

Celerium's Compromise Defender™ solution powered the pilot program. The focus of the solution is on the science of compromise activity detection and defense.

The success of the pilot came down to being able to detect and deter compromise activity within participating counties' networks. In the end, the Compromise Defender solution was able to identify:

- More than 2 million network threats
- Nearly 2,000 cyber compromise activities

ABOUT COMPROMISE DEFENDER™

Compromise Defender detects, disrupts, and deters cyber compromise activity which often succeeds the network intrusion phase of a cyber incident and can be a precursor to later-stage ransomware and data breach attacks.

The innovative solution combines rapid implementation and automation to provide early detection and defense of compromise activity.

Solution highlights include:

- 30-minute non-intrusive implementation, without any hardware or software to install.
- Secure connectivity between an organization's perimeter firewalls to Celerium's Decision Engine hosted on the AWS cloud.
- 100% automated so it does not require integration with a SIEM or other tools.
- Autonomous operation, requiring no IT staff for day-to-day management.
- Real-time automated defense mechanisms to block network threats and compromise activity. The real-time mechanism re-optimizes defensive measures every 15 minutes.
- Integrated automated analysis and reporting platforms show compromise activity (of reconnaissance, C2 server activity, malicious port activity, and more) in the Compromise Defender portal.
- Configurable support for a community of individual organizations.

PILOT PROGRAM OVERVIEW

The pilot program took place over a four-month period in 2023, beginning in April and ending in July, through three phases:

PHASE 1: NETWORK DEFENSE

This phase focused on analysis of incoming threats with reports showing daily, weekly, and monthly information. Additional information provided includes countries and sources of threats.

PHASE 2: COMPROMISE DEFENSE

This phase included reports on more specific insights related to compromise activity -- including potential C2 server communications, and activity from bots, scanners, honeypots, and bruteforce attempts. Reports showing related malware and compromise activity distribution were also available.

Additionally, Celerium added support for server-based reporting using a CTT (compromise translation) table.

AUTOMATED BLOCKING / DEFENSIVE MODE: Many participants chose to turn on automated blocking of high confidence threats at this time. See the section on risk scoring for more information.

PHASE 3: BREACH DEFENSE

This phase added reports on port analysis and potential data breach activity.

The requirements to participate in pilot included:

- Use of one of the supported firewalls*
- No intermediaries (e.g., MSPs)
- No integrations with other security tools (e.g., SIEMs)

See supported firewalls at **https://www.celerium.com/supported-firewalls*

WHY DID COUNTIES JOIN THE PILOT PROGRAM?

The pilot participants included counties that are members of the National Association of Counties (NACo) and its Tech Xchange program.

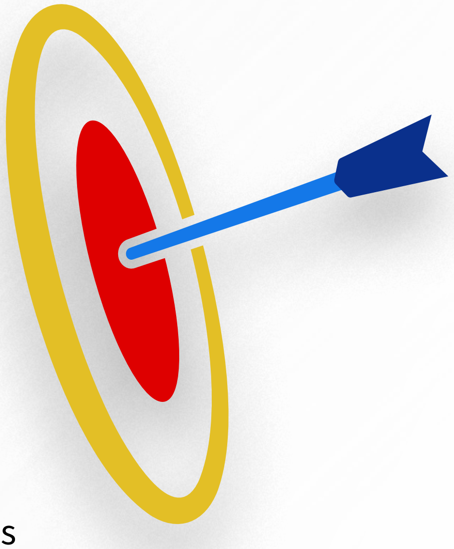
Points of contact within the participating counties included CISOs, CIOs, and IT Directors. When asked why they joined the pilot, many people expressed interest in identifying gaps and see if they are missing anything. Specific reasons stated include:

- We want to identify gaps in our systems.
- Always looking to make our IT jobs easier.
- Always looking for ways to improve our cybersecurity.
- Want to know if our existing controls are detecting everything or if Celerium can help find things we're missing.
- Looking for gaps in defense.
- We assume we have bad guys in our system and just don't know about it.

Counties can't take on a heavy lift due to existing workload, staffing, and resources.

COMPROMISE DEFENDER™ SOLUTION OBJECTIVES

There are four key objectives for Celerium's Compromise Defender solution:



1. Detect and disrupt current known threats which could result in ransomware, data breaches, or other problems.
2. Address recent evolving threats (Cl0p/MOVEit)
3. Address future emerging threats such as automatically generated malware campaigns and phishing attacks created by ChatGPT and other AI-powered technologies or threat actors.
4. For communities (such as a community of NACo counties), provide community common operating pictures, situational awareness, and a community defense mechanism.

SOLUTION OPERATION

Analysis: Includes an integrated analysis and reporting platform with dashboard and results for both individual counties and the community of county participants.

Defense: Leverages a patented technology, which has been used by the U.S. Department of Defense / Defense Industrial Base for four years, that re-optimizes block lists for firewalls every 15 minutes.

Automated: No integration with SIEMs or other security tools* is required.

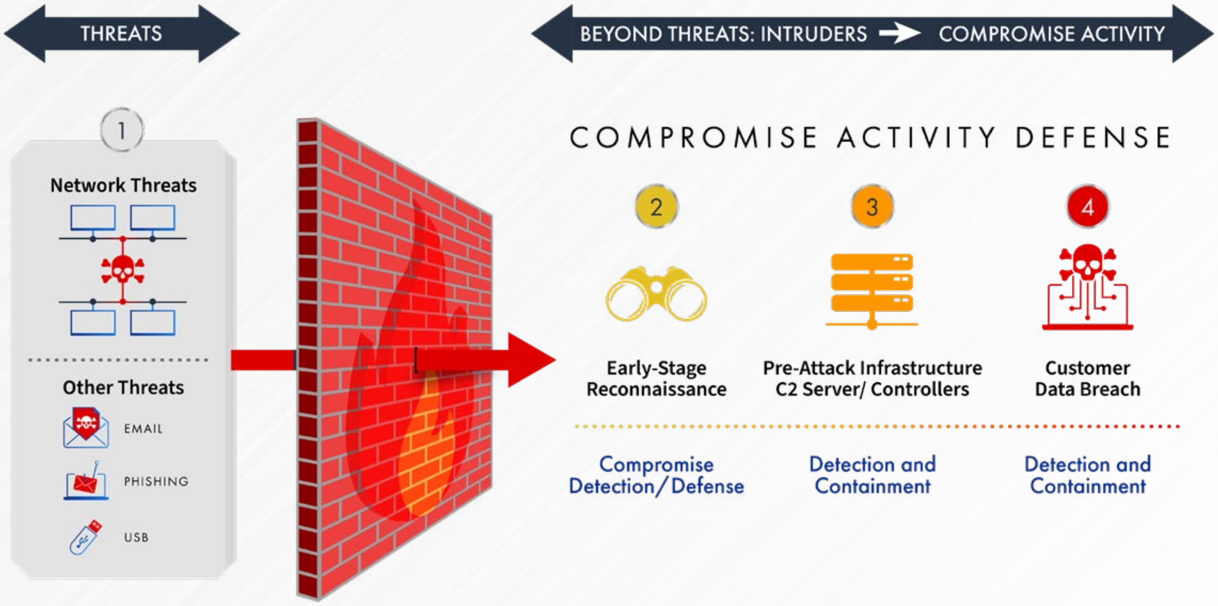
Autonomous: No day-to-day management is required.

Real Time: Block lists are re-optimized every 15 minutes.

Bottom line: Detection and automated real-time disruption, containment, and deterrence of network threats and compromise activity such as reconnaissance, and C2 server activity.

The solution does require the use of a support firewall.

SOLUTION DIAGRAM


THREATS
BEYOND THREATS: INTRUDERS → COMPROMISE ACTIVITY
1
Network Threats
Other Threats
EMAIL
PHISHING
USB
COMPROMISE ACTIVITY DEFENSE
2
Early-Stage Reconnaissance
3
Pre-Attack Infrastructure C2 Server/ Controllers
4
Customer Data Breach
Compromise Detection/ Defense
Detection and Containment
Detection and Containment

Compromise Defender analyzes ingress data coming into the firewall to determine if traffic consists of network threats and threats such as malicious emails, phishing, and USBs. It also analyzes egress (outgoing) data to identify early-stage reconnaissance activity, pre-attack infrastructure, and potential customer data breach activity.

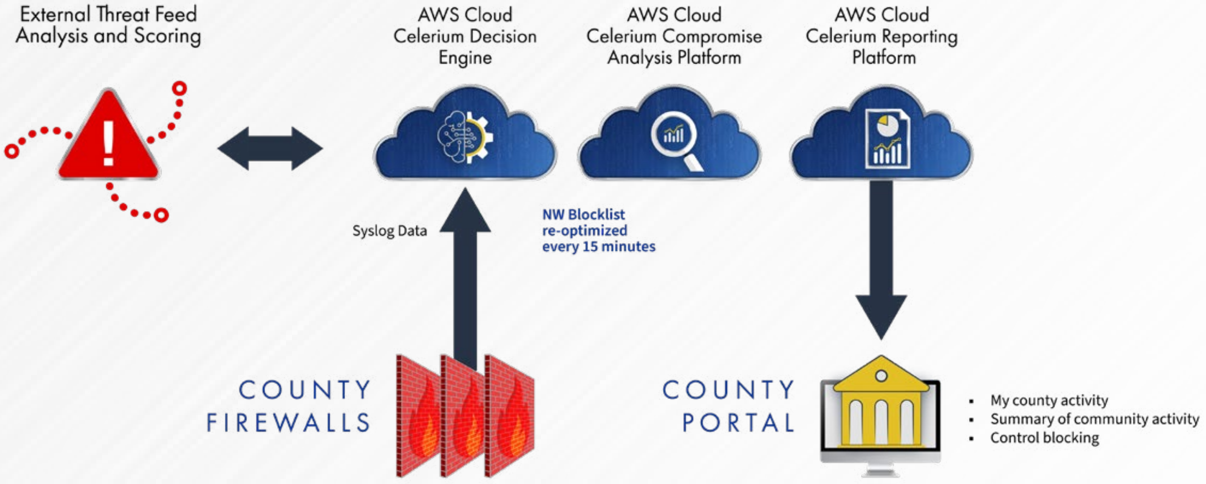
SOLUTION IMPLEMENTATION

An important piece of the pilot and its objective to help overwhelmed county IT staff is the ease of use, specifically the ease of implementation.

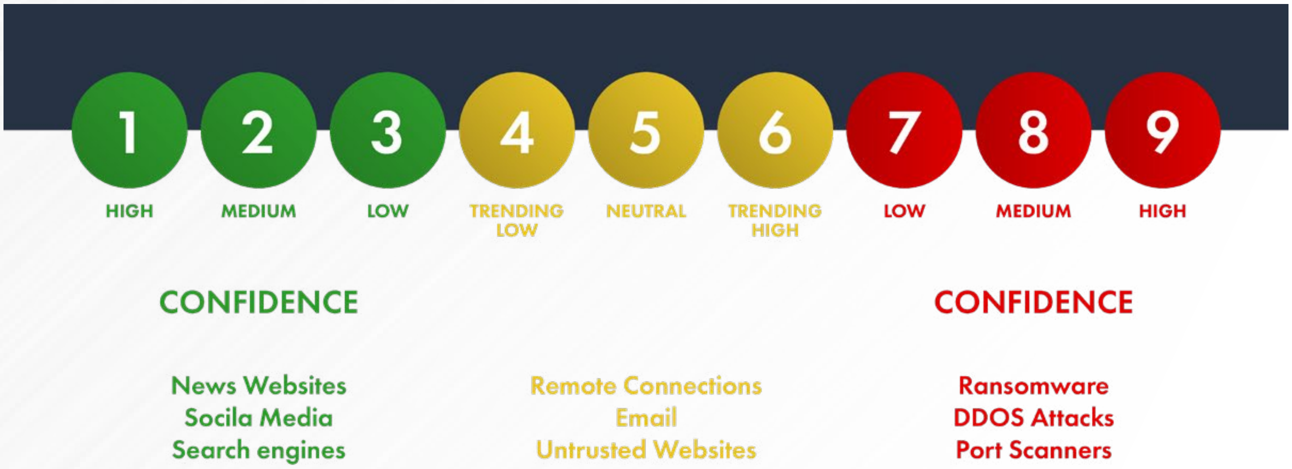
Implementation in 30 Minutes
Designed for Busy, Overloaded County IT Staff

- Works with popular public-facing perimeter firewalls.
- Non-intrusive implementation at the firewall -- no new hardware or black boxes to install and no software to download.
- Implementation connects your firewall to Celerium's **Decision Engine** hosted on the secure AWS cloud.
- Compromise Defender analyzes ingress data coming into the firewall to determine if traffic consists of network threats and threats such as malicious emails, phishing, and USBs. It also analyzes egress (outgoing) data to identify early-stage reconnaissance activity, pre-attack infrastructure, and potential customer data breach activity.

RISK ANALYSIS AND SCORING


External Threat Feed Analysis and Scoring
AWS Cloud Celerium Decision Engine
AWS Cloud Celerium Compromise Analysis Platform
AWS Cloud Celerium Reporting Platform
Syslog Data
NW Blocklist re-optimized every 15 minutes
COUNTY FIREWALLS
COUNTY PORTAL
My county activity
Summary of community activity
Control blocking

Syslog/netflow data from county firewalls is analyzed in the Decision Engine, hosted on the AWS cloud, and is compared against external threat feeds for analysis and scoring. The analysis is then shared via reports in the CDN (Cyber Defense Network) portal. If auto-blocking is turned on, the blocklist is re-optimized every 15 minutes.



The risk scoring scale is straightforward. Each score is a combination of risk and confidence. So, an IP scoring a 9 has been determined to be a high risk, and we have a high confidence level in that assessment. We recommend that our customers block all 9s as a best practice.

PILOT PROGRAM RESULTS

DEGREES OF RECONNAISSANCE (SCANNING) ACTIVITIES AGAINST COUNTIES

Scanner	2 events	2 events
	8	9

Scanner	11 events	15 events
	8	9

Scanner	63 events	
	8	9

Scanner	61 events	148 events	217 events
	7	9 🟥	9 🟥

Participating counties experienced a range of reconnaissance activity.

Reconnaissance activity consists of threat actors trying to explore your systems for two purposes:

1. To find vulnerabilities
2. To understand what systems they want to target

Counties experienced a range of reconnaissance activity from modest to moderate to high.

PARTICIPANT EXPERIENCES

Pilot participants defined four key areas of the pilot experience:

1. The implementation was the "easiest thing I've done in my career."

The solution really does take less than 30 minutes to implement. While one IT Director was skeptical of a sales guy making that statement, the implementation was indeed fast. In fact, the IT staff expressed that they wasted too much worrying about scheduling and getting ready for implementaton.

> *The hardest part of implementation was remembering the password to the firewall.*

Another participant was skeptical of the solution and, quite frankly, considered it a waste of time. "I thought, how much time is it going to take myself and my team?" As it turns out, not much at all.

2. Celerium's responsiveness to solution ideas

Throughout the pilot program, Celerium sought feedback from participants about the entire solution experience.

> *It's a big deal that we have a partner that collaborates.*

For example, Celerium developed reports on compromise activity. Participants gave feedback and insights, and the reports "are now at a place that gives me what I need," according to a pilot participant.

The Celerium team also enhanced the solution throughout the pilot based on participant feedback. For example, Celerium quickly added a download capability to enable users to download data on compromise activity.

3. Experience and insights regarding detection threats and compromise activity

One participant wondered if, “are we going to find anything at all given our existing security stack?” However, this same participant discovered a high threat almost immediately following implementation, and was able to take quick action to mitigate the threat.

Additional feedback about the detection was related to the lack of noise that is typical of cybersecurity solutions. “Usually, you get a lot of noise, but this shows you the 9s… the high threats that you need to be aware of.”

4. Automated Blocking

Some participants receive lists of risky IP addresses and IOCs from other places, but those lists are in the thousands and, given the staff time available, the counties struggle to implement in this area.

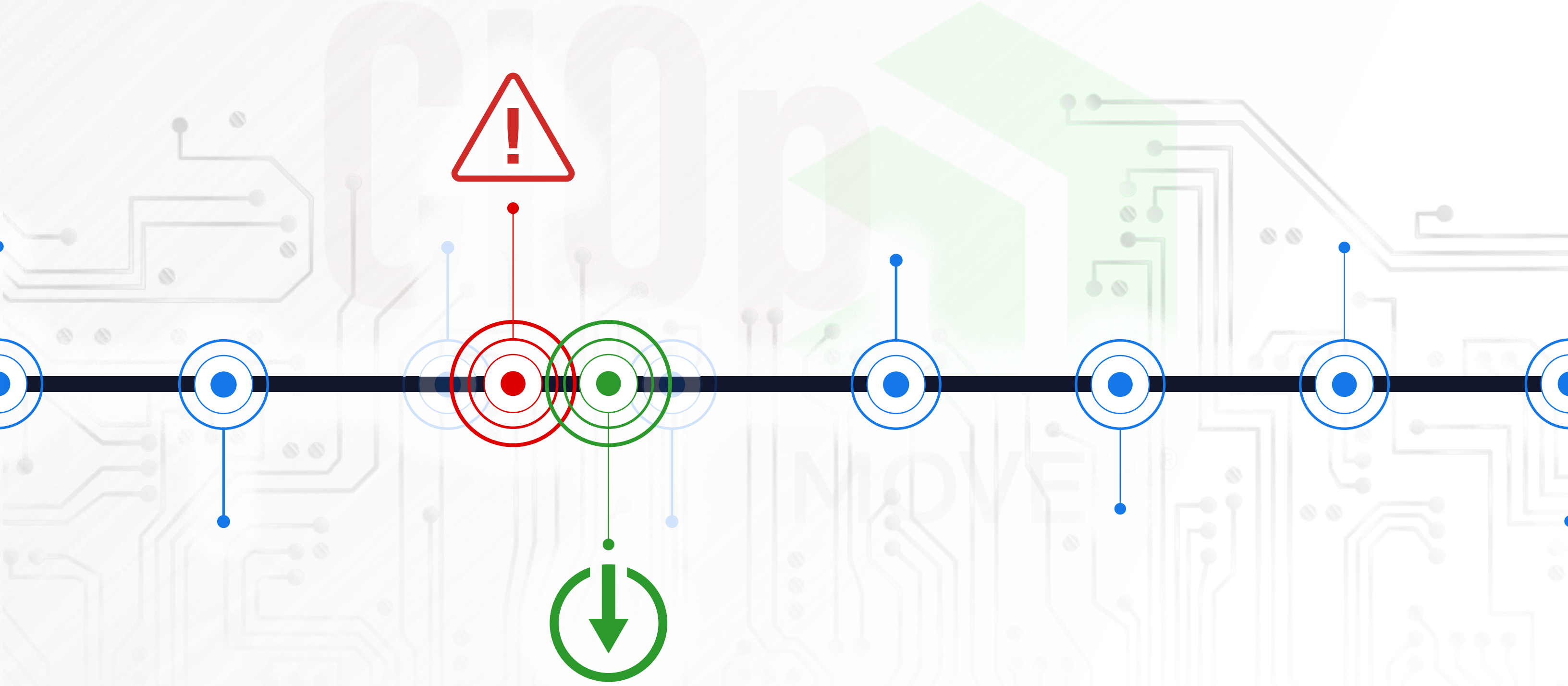
The Compromise Defender solution enables automated blocking of threats, based on a scoring threshold set by the organization’s IT staff. This blocking is re-optimized every 10-15 minutes, providing a near real-time response to cyber threats and compromise activity.

> *It comes down to real-time.*
> *I haven’t found any other resource that allows me to close that gap.*

HIGH-PROFILE THREATS DURING THE PILOT

During the pilot term, the Cl0p ransomware gang exploited a MOVEIt vulnerability. Compromise Defender quickly integrated more than 1,500 IOCs provided by CISA, an agency of the Department of Homeland Security, and other organizations to deliver prompt and efficient protection for organizations in the pilot. Several organizations observed reconnaissance (scanning) activity associated with MOVEit infrastructure, and Compromise Defender blocked that activity. The system's ability to rapidly respond to the Cl0p/MOVEit ransomware threat helped prove the solution's effectiveness.

Later in the pilot, CISA released an advisory on increased Truebot activity infecting U.S. networks. This was another example of Compromise Defender moving quickly to add relevant IOCs to provide protection for participants.



CONCLUSION

> *We don't always know the gaps we have, and the ease with which we can close those gaps.*

The four-month pilot program did help county governments detect, disrupt, and deter network threats and cyber compromise activity. The solution was easy to implement, efficient in its operation, and improved throughout the course of the pilot based on participant feedback.

Going forward, Compromise Defender is primed to protect organizations from current and future attacks, malware campaigns, and phishing attacks – including those that ChatGPT and other AI-enabled technologies and threat actors automatically generate.