Lumen® Managed Endpoint Detection and Response Threat Intelligence User Guide

User guide | November 2022

This document provides an overview of the Lumen Security Solutions portal and is used to convey to customers and prospects what to expect of Security Solutions portal. This document will be updated as necessary to reflect any changes made to the Security Solutions portal.

Lumen Security Solutions portal

The sophistication of cyber threats, and the complexity of maintaining traditional point network security solutions, is driving the adoption of managed security service solutions utilizing threat intelligence. As your organization upgrades your security posture to be more proactive, you want threat intelligence that is actionable. Lumen Security Solutions portal helps address these business challenges by providing analysts context about the incidents generated by managed security service solutions.

Security Solutions portal provides context about threats by correlating the information obtained about traffic flows between your network and the other end of the IP communication against the Lumen database of known malicious IPs. If the information obtained from the MEDR alert matches a malicious IP, a record is created in SSP (an “event”) that is forwarded in near real-time to the Security Solutions portal.

Lumen has made a major investment in developing a threat research and engineering group called Black Lotus Labs. The Black Lotus Labs team has developed threat sensing capabilities using one of the world’s largest IP backbones. Malicious behaviors are detected off the backbone and classified using sophisticated machine learning algorithms and automated validation infrastructure. Additionally, Black Lotus Labs validates Indications of Compromise (IOCs) that are conveyed using third-party resources. The extra effort pays off in the cultivation of a very high-fidelity threat set. Customers benefit in several ways including:

- Real-time visualization of their interactions with malicious entities
- Botnet research and take-down efforts keep the backbone safer
- Automated deployment of countermeasures when new threats are discovered via Black Lotus Labs
- Leading botnet research and publication

Support contacts

Access security support contacts

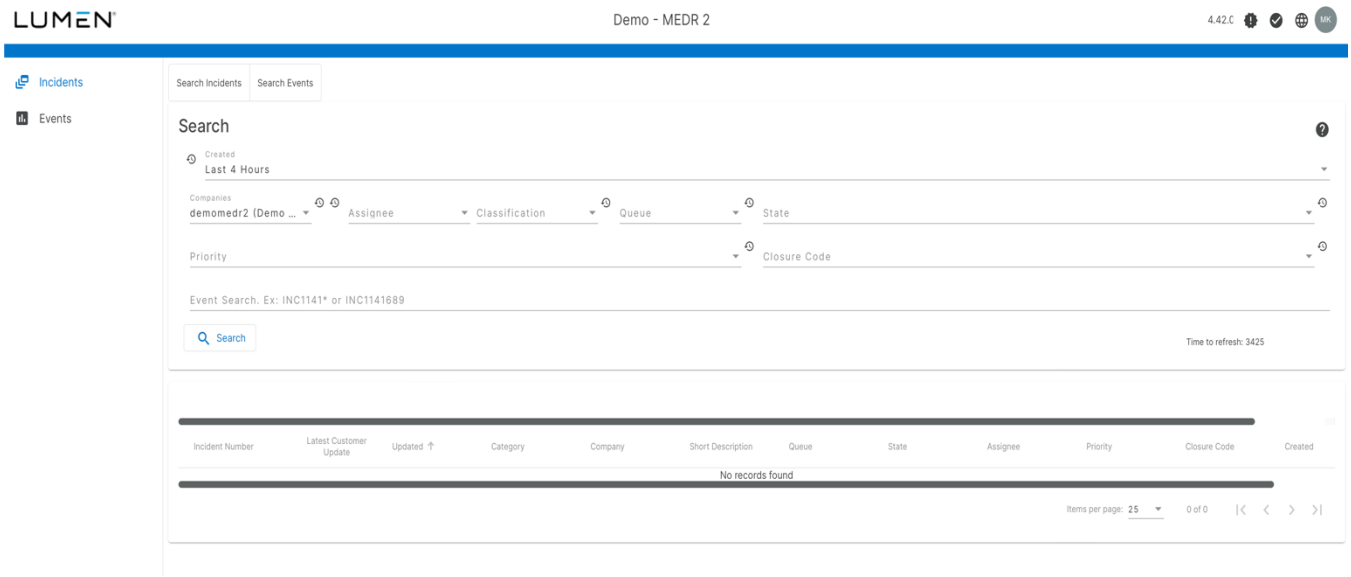
Accessing the Security Solutions portal

Note: Only users who have been set up with the managed security services permission and two-factor authentication can access the Lumen Security Solutions section of Control Center. Supported internet browsers are Chrome, Safari, and Firefox. Use of unsupported browsers will result in reduced functionality.

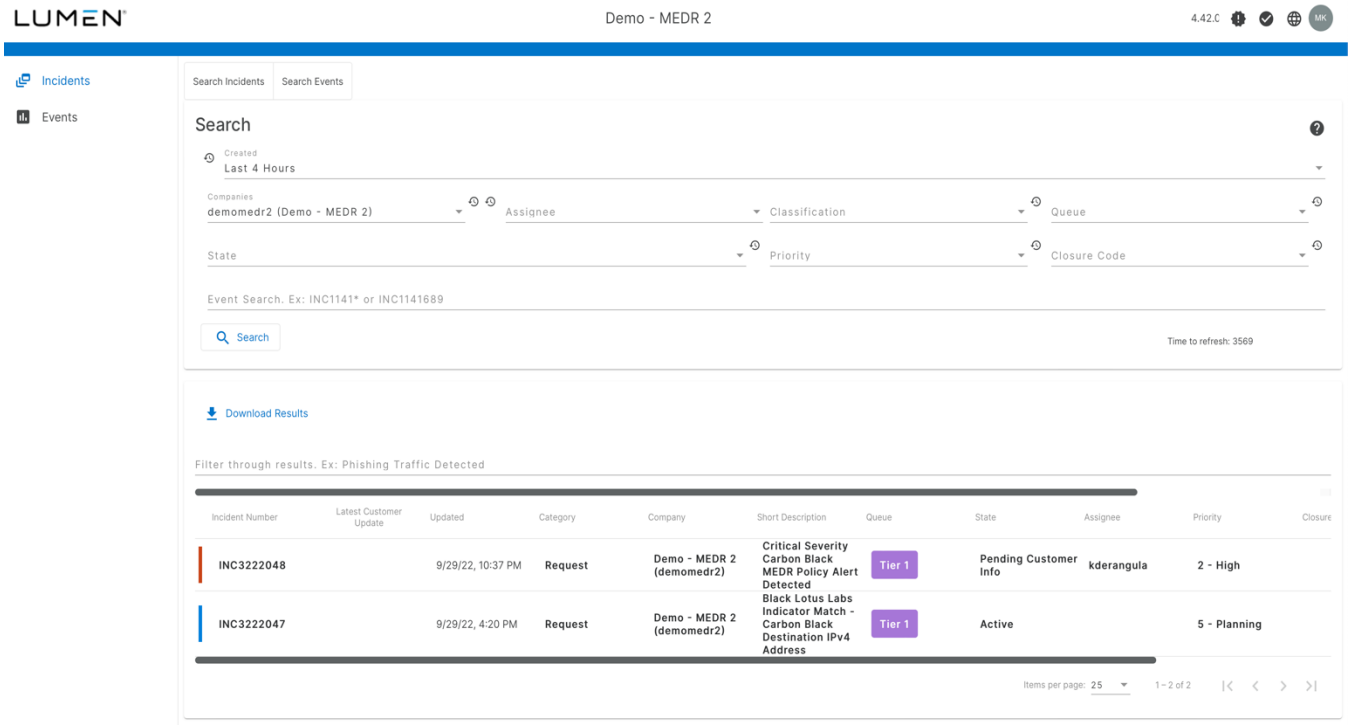
Learn how to sign in to the Security Solutions portal

1. In the **Reports** section, select **Security Solutions Portal:**

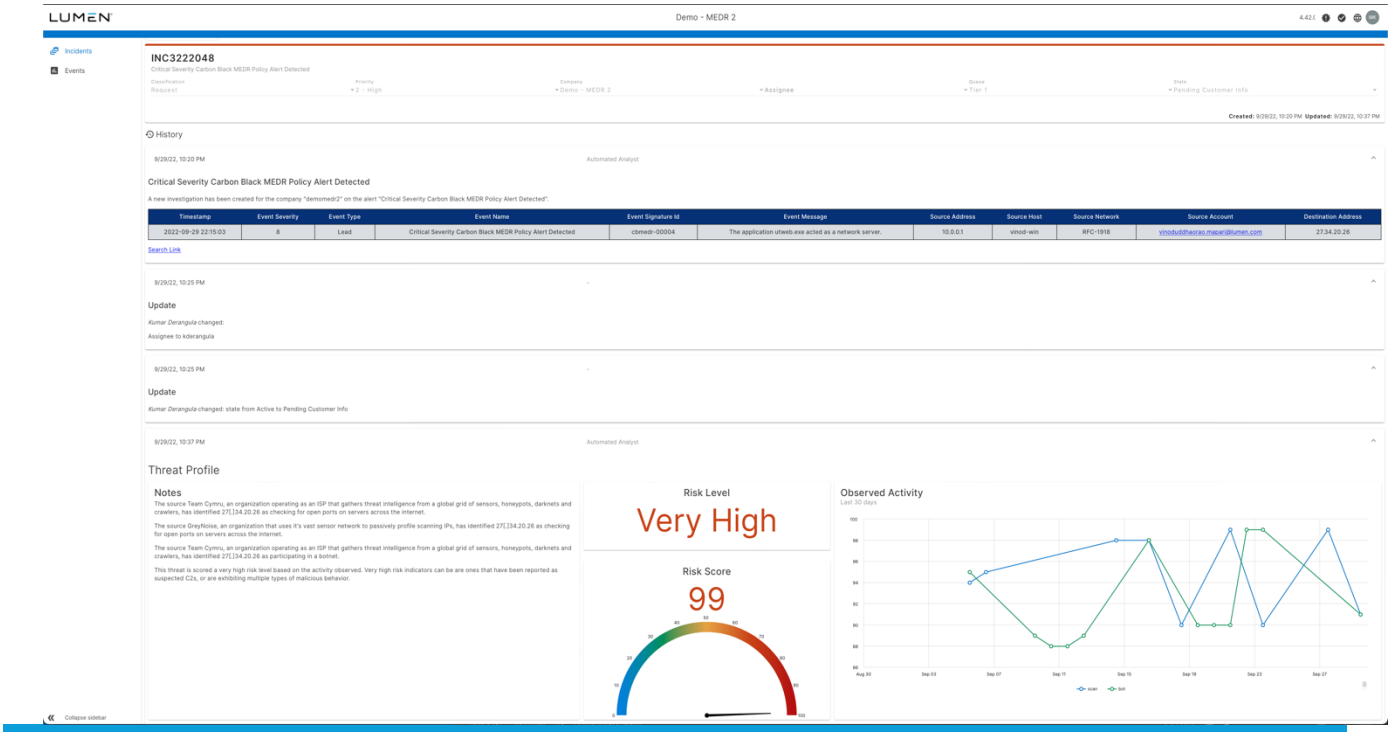
2. Once on the landing page of the Security Solutions Portal, click on “Incidents” on the left side of the page. The incidents page will allow you to search for incidents based on incidence creation interval, priority, incident state and other search criteria.



3. Select the company you want to see the incidents for and click on “Search”. This search will show you the incidents matching the search criteria.



4. Selecting the incident number, will open the incident on a new page with the Black Lotus Labs correlated threat profile and MEDR alert details.



5. The alert details include the timestamp of correlation with Black Lotus Labs threat intelligence data, severity, brief description of the alert, source, and destination IP address, etc. The Threat Profile section provides details about the threat indicator such as the sources that have identified the malicious IP address as a threat, threat categories associated with the indicator, and risk level. The observed activity graph displays the risk level and categories associated with the threat indicator over a period.

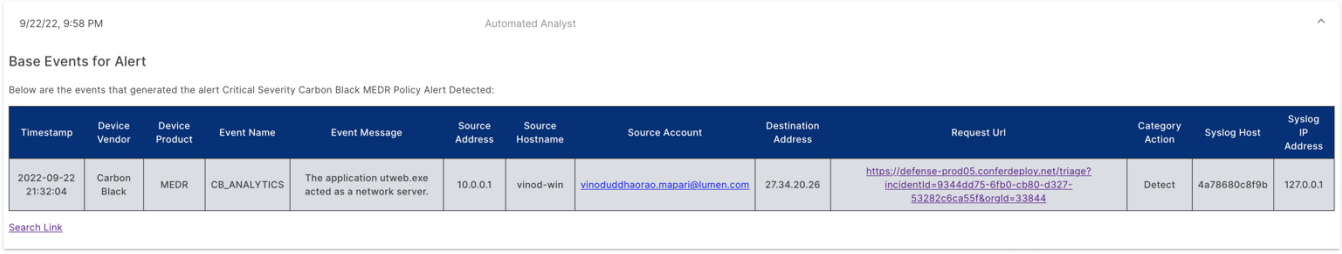
6. The additional information table column headings are described in the following table:

Column	Description
First Seen	The date and time this indicator was first reported. Note, for clarity, the time zone offset from GMT is included.
Last Seen	The date and time this indicator was last reported. Again, the time zone offset from GMT is included
Category	SSP associates a threat category for each indicator that is listed. An indicator may be associated with multiple threat categories.

The threat categories are described in the table below:

Category	Description
C2	C2 is shorthand for “command and control”. Each botnet has a C2 entities that manage the activities of the botnet.
Attack	These entities attempt to penetrate the peripheral defenses of an enterprise typically using “dictionary” attacks to crack passwords on publicly addressable assets.
Bot	Entities that have been compromised to participate in the activities a botnet
Malware	Entities that distribute malware for the purpose of compromising assets to gain access to intellectual property
Phish	Entities that proliferate communications for the purpose of collecting credentials to valuable assets. Phishing can use email, phone calls, text, IM, and other vectors for this purpose
Scan	Entities that probe the peripheral defenses of an enterprise for the purpose of discovering accessibility, typically pinholes in firewalls.
Spam	Entities that distribute communications for the purpose of attracting attention to services that are considered irrelevant to the business of the enterprise targeted.

7. The MEDR events that generated the alert creation are listed under the “Base Events for Alert” section. Each event includes the event creation timestamp, device and product source for the event, source and destination IP address, link to the event on the Carbon Black MEDR portal, etc.


9/22/22, 9:58 PM Automated Analyst

Base Events for Alert

Below are the events that generated the alert Critical Severity Carbon Black MEDR Policy Alert Detected:

Timestamp	Device Vendor	Device Product	Event Name	Event Message	Source Address	Source Hostname	Source Account	Destination Address	Request Url	Category Action	Syslog Host	Syslog IP Address
2022-09-22 21:32:04	Carbon Black	MEDR	CB_ANALYTICS	The application utweb.exe acted as a network server.	10.0.0.1	vinod-win	vinoduddhaorao.mapari@lumen.com	27.34.20.26	https://defense-prod05.conferdeploy.net/triage?incidentId=9344dd75-6fb0-cb80-d327-53282c6ca55f&orgId=33844	Detect	4a78680c8f9b	127.0.0.1

Search Link