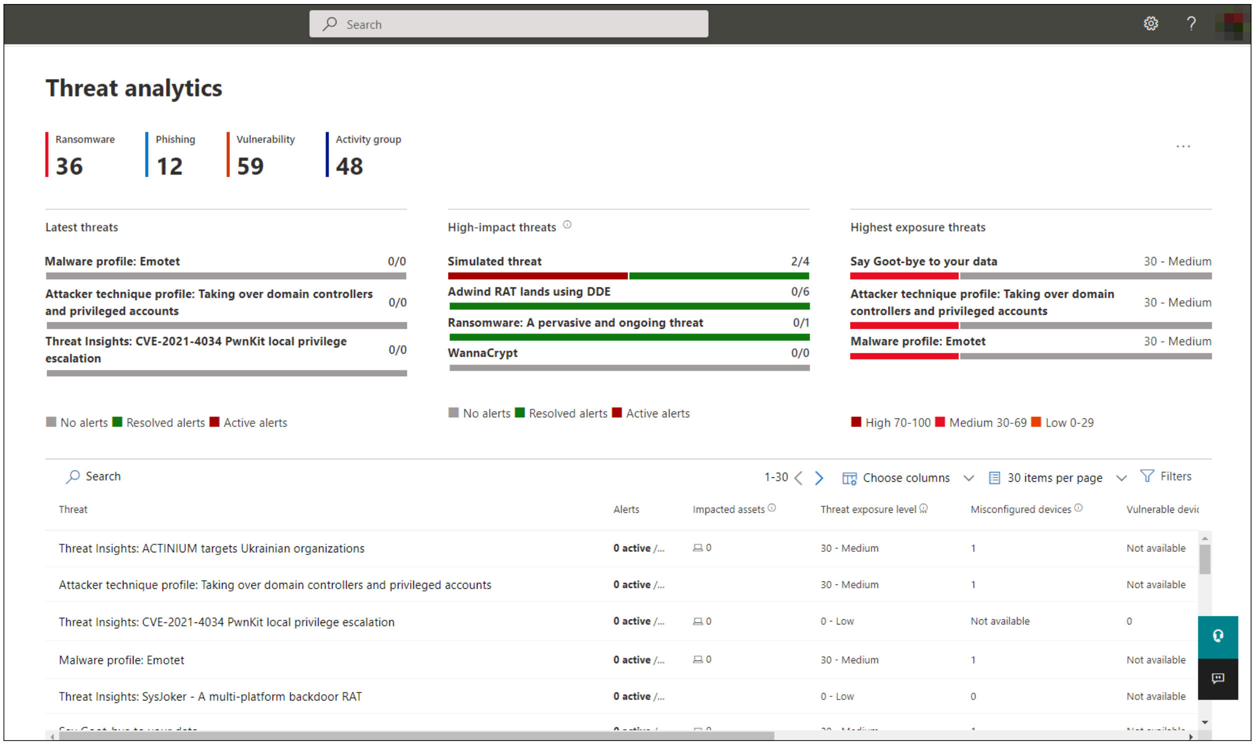
Analyze threat analytics

By: Ryan Stewart

Threat analytics is a threat intelligence solution from expert Microsoft security researchers. It's designed to assist security teams to be as efficient as possible while facing emerging threats, such as:

- Active threat actors and their campaigns
- Popular and new attack techniques
- Critical vulnerabilities
- Common attack surfaces
- Prevalent malware



Threat analytics

Ransomware	Phishing	Vulnerability	Activity group
36	12	59	48

Latest threats

Malware profile: Emotet	0/0
Attacker technique profile: Taking over domain controllers and privileged accounts	0/0
Threat Insights: CVE-2021-4034 PwnKit local privilege escalation	0/0

■ No alerts 🟩 Resolved alerts 🟥 Active alerts

High-impact threats

Simulated threat	2/4
Adwind RAT lands using DDE	0/6
Ransomware: A pervasive and ongoing threat	0/1
WannaCrypt	0/0

■ No alerts 🟩 Resolved alerts 🟥 Active alerts

Highest exposure threats

Say Goot-bye to your data	30 - Medium
Attacker technique profile: Taking over domain controllers and privileged accounts	30 - Medium
Malware profile: Emotet	30 - Medium

🟥 High 70-100 🟥 Medium 30-69 🟧 Low 0-29

Threat	Alerts	Impacted assets	Threat exposure level	Misconfigured devices	Vulnerable devic
Threat Insights: ACTINIUM targets Ukrainian organizations	**0 active** /...	0	30 - Medium	1	Not available
Attacker technique profile: Taking over domain controllers and privileged accounts	**0 active** /...		30 - Medium	1	Not available
Threat Insights: CVE-2021-4034 PwnKit local privilege escalation	**0 active** /...	0	0 - Low	Not available	0
Malware profile: Emotet	**0 active** /...	0	30 - Medium	1	Not available
Threat Insights: SysJoker - A multi-platform backdoor RAT	**0 active** /...		0 - Low	0	Not available

High impact threats pose the greatest potential for causing harm, while high exposure threats represent the vulnerabilities most likely to affect your assets. Gaining visibility into active or ongoing campaigns and leveraging threat analytics is essential for empowering your security operations team with informed decision-making.

In the face of increasingly sophisticated adversaries and the emergence of new threats, it is crucial to swiftly:

- **Identify and respond to emerging threats**
- **Determine if your organization is currently under attack**
- **Assess the impact of threats on your assets**
- **Evaluate your resilience against or exposure to these threats**
- **Identify mitigation, recovery, or prevention actions to halt or contain threats**

Each threat analytics report offers an analysis of a tracked threat along with comprehensive guidance on defending against it, incorporating data from your network to indicate the threat's activity and the presence of applicable protections.

Explore the threat analytics dashboard to highlight reports relevant to your organization, categorized into:

- **Latest threats:** Most recently published or updated threat reports, with active and resolved alerts.
- **High-impact threats:** Threats with the highest impact, listing those with the highest number of active and resolved alerts first.
- **Highest exposure:** Threats with the highest exposure levels, considering the severity of vulnerabilities and the number of exploitable devices in your organization.

Choosing a threat from the dashboard leads to a detailed report featuring:

1. **Overview:** A preview of the detailed analyst report, with charts highlighting the threat's impact and exposure through misconfigured and unpatched devices.

2. **Assess Impact**: Charts providing information about the organizational impact of a threat, related incidents, alerts over time, impacted assets, and prevented email attempts.

3. **Review Security Resilience:** Charts offering insights into your organization's resilience against a threat, including secure configuration status and vulnerability patching status.

To further streamline your analysis, you can filter threat reports based on threat tags (categories) or report types, such as Ransomware, Phishing, Vulnerability, and Activity group. The Microsoft Threat Intelligence team has added these tags to enhance the categorization and efficiency of threat report reviews. The counters at the top of the threat analytics page provide an overview of available reports under each tag.

Configure Email Notifications for Report Updates

Stay informed about threat analytics reports by setting up email notifications. Follow these steps to enable email notifications for threat analytics reports:

1. Navigate to Settings in the Microsoft Defender XDR sidebar and select Microsoft Defender XDR from the settings list.

2. Choose Email notifications > Threat analytics, and click the "+ Create a notification rule" button to open a flyout.

3. Follow the instructions in the flyout. Start by giving your new rule a name. The description field is optional, but a name is mandatory. Use the checkbox under the description field to toggle the rule on or off.

- Note: The name and description fields for a new notification rule only accept English letters and numbers, excluding spaces, dashes, underscores, or any other punctuation.

4. Specify the type of reports for which you want to receive notifications. You can opt to be updated about all newly published or updated reports or only those with a specific tag or type.

5. Add at least one recipient to receive the notification emails. Additionally, you can use this screen to test the email delivery by sending a test email.

6. Review your new rule. If any adjustments are needed, select the Edit button at the end of each subsection. Once satisfied, click the "Create rule" button.

Your new rule is now successfully created. Click the "Done" button to finish the process and close the flyout. Your new rule will be added to the list of Threat analytics email notifications.