For Immediate Release

Contact: **Brian Azzopardi, Rawstream**
Email: **press@rawstream.com**

*London, August 12th. Rawstream's new **Threat Huntr™**: now you can hunt cyber threats rather than wait for an attack*

Be Proactive with Cyber Security

Rawstream's new Threat Huntr™ proactively searches for unknown, active threats in an environment It is the new gold standard for endpoint security. Malware or attackers can be lurking in your network quietly siphoning off data, or working their way across the network jumping from host to host.

Your Endpoint Security Isn't Infallible

You don't need to read the news to know that your security is not infallible. Many major companies have been successfully attacked and it's often a matter of when, not whether, you will be too. Defense in depth can fail. While the majority of threats can be stopped with good security practices such as keeping systems updated with the latest patches, implementing network firewalls, and using web filtering to block phishing attempts, an attacker may still get through. And they often do. When traditional systems fail to stop the attacker, the proactive company needs to actively look for indicators of compromise using its logs and data sources.

Proactive Endpoint Security for Endpoints

Today's release of Rawstream Threat Huntr™ is the first in a series that will provide targeted, timely intelligence to the proactive company. Why wait for an attack when you can hunt the threat? From today you will have access to intelligence that will highlight potentially insecure new applications on your network, suspicious network access, and user activity.

New software that was previously unseen on the network can be a threat if the application was not sanctioned by your IT team. The new software may be harmless but your IT team still needs to be aware that it was installed on the network and take steps to ensure that its patches are installed in a timely manner. Plus, the fact that one of your employees was able to install software serves as an alert to IT that installation permissions may need to be tightened. In the worst case scenario, the software is malware that was not caught via traditional security means.

An industry first

In a first for the industry, Rawstream displays enriched domain reporting: the geographic location of the host, and domain age. Network access to servers in geographies where your company does not traditionally do business, for example, Russia, is a highly suspicious. In addition, a domain's age is a strong indicator about a domain's trustworthiness. Access to a domain that has only been registered for a few days is a strong sign of a phishing attack.

Internet Access is Essential: Rawstream Makes It Safe

With most business applications running in the cloud, internet access is essential. CRM, email, document sharing, communications and many other essential business applications need network access. All this network activity

generates a huge number of logs, making it practically impossible for your IT teams to find the needles in the very large haystacks of data. Traditional SIEM software generates many alerts. Fine-tuning the rules to minimize false-positives while still retaining detection capability requires a tremendous amount of time and resources.

Rawstream Threat Huntr™ Protects You in a New Way

With Rawstream Threat Huntr™ we've taken a different approach. In the first release Threat Huntr™ will report DNS MX lookups, and MX lookups to previously unseen domains. Your mail traffic should flow through only a very small number of servers, either internally for on-premise mail servers, or to Google's Gmail, Microsoft Office 365, or the like. MX lookups to other domains is highly suspicious and is a strong indicator of compromise or permissive firewall rules.

By anticipating threats, we provide a strong barrier of protection.

Future Updates Will Increase Your Endpoint Security

Today's Threat Huntr™ release is the first in a series of releases to increase expanded reporting and capability. The next major release will correlate processes running on the endpoint with each process's network activity. By building a model of process activity and their network traffic, Threat Huntr™ will provide reliable, actionable new indicators of compromise.

Our continued focus remains on providing timely intelligence without the high false-positives that is the bane of traditional security approaches.

Threat Huntr™ is Available Now

Threat Huntr™ is available right now for all customers. Just log in to your Rawstream account and click *Dashboard > What's New* to start using the new threat hunting functionality.

Sign up for Rawstream at https://app.rawstream.com/signup.

– ENDS –

For further information, please contact press@rawstream.com