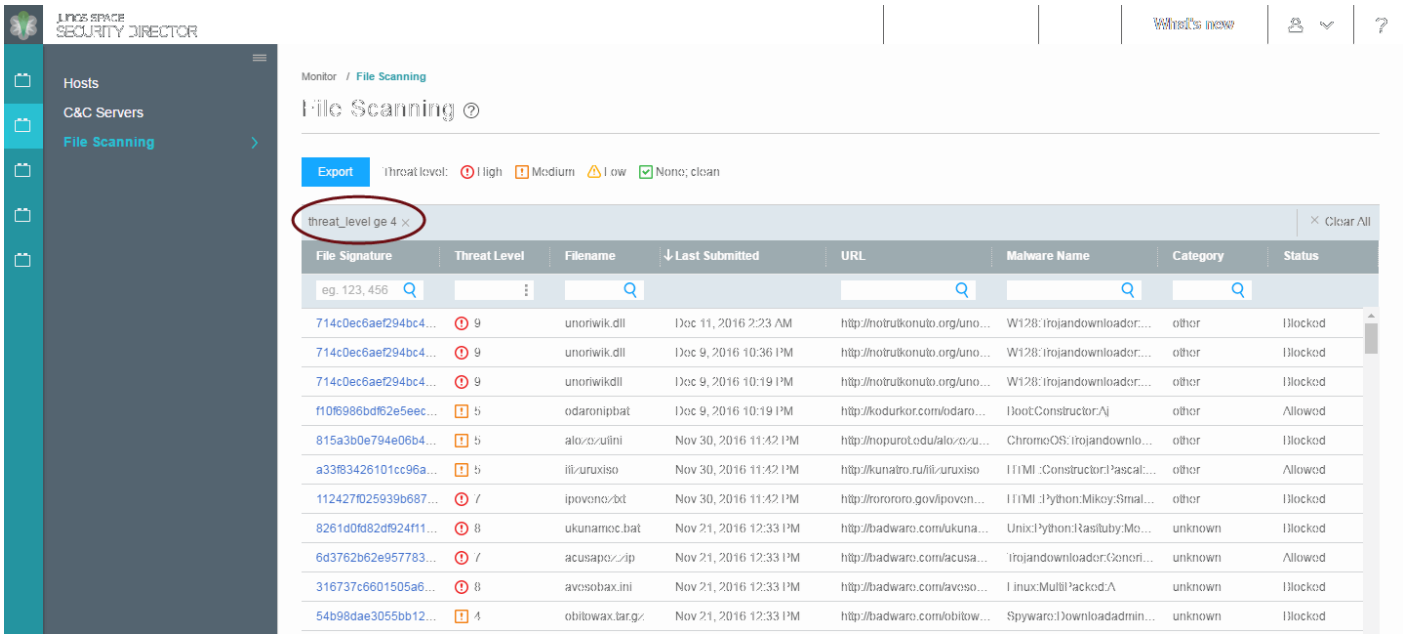
EXHIBIT 24

Sky Advanced Threat Prevention Scanned File Overview

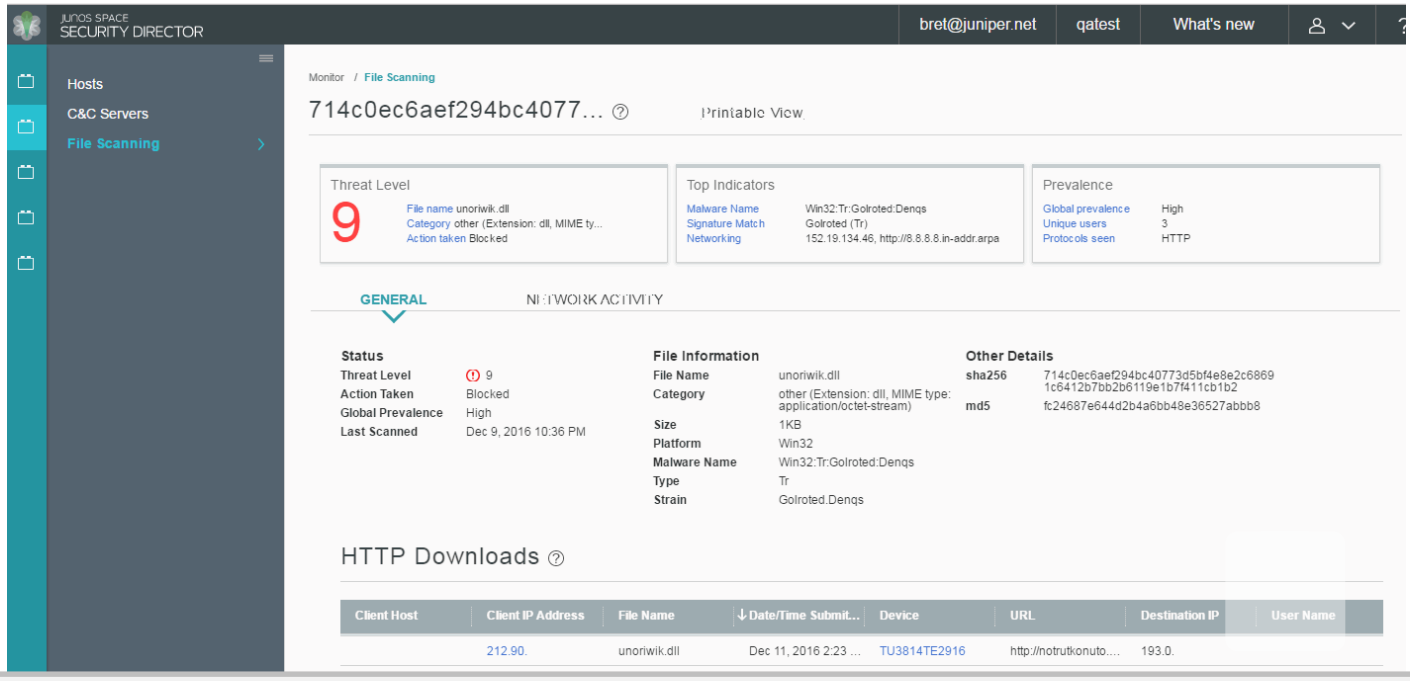
Sky ATP keeps a record of all file metadata sent to the cloud for inspection. You can view the files sent from your network by selecting **Monitor > File Scanning** in the Web UI. See Figure 1. Your firewall policy determines what to do if a file is suspected of being malware. For example, block that file from being downloaded to the client.

Figure 1: List of Inspected Files and Their Results



By default, threat levels 4 and above are shown. Click the file's signature to view more information, such as file details, what other malware scanners say about this file, and a complete list of hosts that downloaded this file. See Figure 2.

Figure 2: Viewing Scanned File Details



For more information on the file scan details page, see the Web UI tooltips and online help.

If you suspect a file is suspicious, you can manually upload it for scanning and evaluation. Click **Monitor** > **File Scanning** > **Manual Upload** to browse to the file you want to upload. The file can be up to 32 MB.

There is a limit to the number of files administrators can upload for manual scanning. File uploads are limited by realm (across all users in a realm) in a 24-hour period. You can upload two files per each active device enrolled and 10 files per each premium-licensed device in your account. For example, if you have two Sky ATP premium-licensed SRX Series devices and one other SRX Series device, Sky ATP will allow a maximum of 22 files to be allowed in a 24-hour window.

For more information on scanning files, see the Web UI infotips and online help.

Modified: 2017-01-10