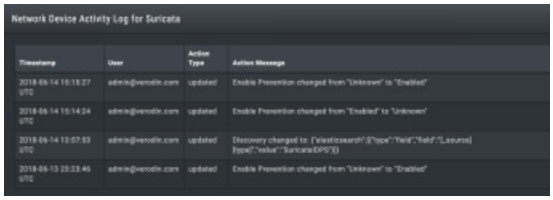
SECURITY TECHNOLOGY AUDITING AND DEFINITIONS

Security Technology Auditing

All modifications to the Security Technology definitions are recorded, whether done from the Security Technology page or from the Create New Security Technology page. This allows you to identify when a security technology definition is changed and who made that change. To view the change, click **Environment > Security Technologies**, then click Activity Log for the security technology you want to see.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880bb0445d5e3e714b3c2b/n/sec-tech-audit.png)

Audit log showing changes to the Suricata Security Technology

User-Defined Security Technology Definitions

The Validation Platform is preconfigured with an extended list of security technology definitions, including prevented and detected definitions for most security technologies. However, your network may be configured with different values in fields or different fields used to assign detected and prevented information. As you investigate the existing definitions, you may decide you want to add your specific security technology definitions to the Validation Platform. This would improve the data available in the platform.

If you want your definition to be part of the default definition set, you can download a local copy of your user-defined definition and share it with the Mandiant Advantage team. Go to **Settings > Director Settings**. The Systems Settings page opens. Select **Security Technologies** and then click **Download Backup**. This prepares and downloads a JSON file that you can then share with **Support (https://docs.mandiant.com/home/mandiant-support-cases)**.