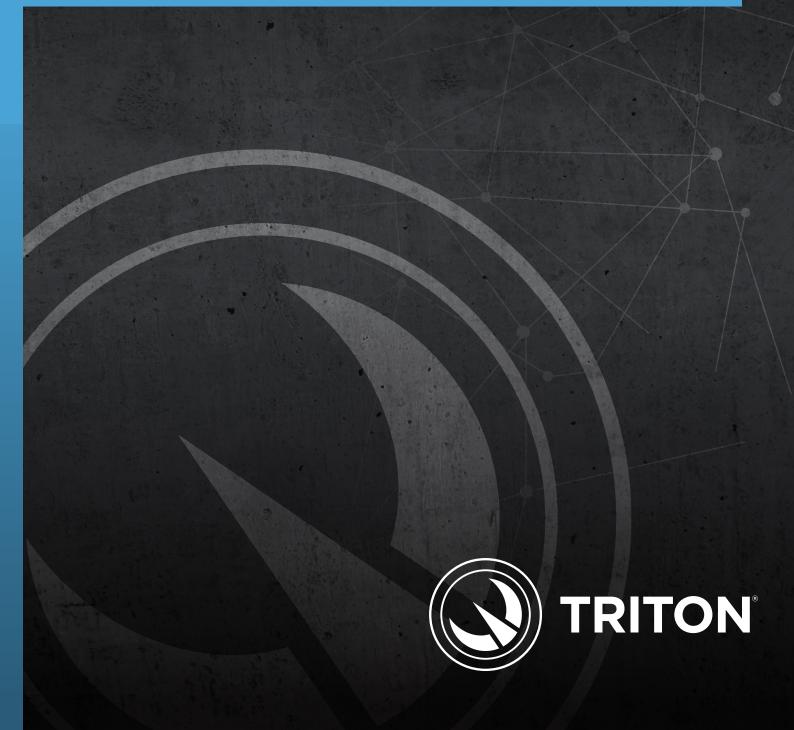# websense®

NEW WEBSENSE DATA SECURITY POLICY TEMPLATE:

CYBER BULLYING AND SELF-DESTRUCTIVE (SUICIDAL) THOUGHTS

TRITON®

New Websense Data Security Policy Template:
Cyber Bullying and Self-Destructive (Suicidal) Thoughts

This document provides a brief introduction to the new *Cyber Bullying and Self-Destructive (Suicidal) Thoughts rules* now available within the Websense® Data Identification & Classification Engine (DICE). We will explain how to implement these rules via a Websense Web Security Gateway Anywhere deployment.*

The latest Web Security Gateway Anywhere license includes data leakage prevention (DLP) features that enable the proxy solution to detect the data patterns contained within the *Cyber Bullying and Self-Destructive (Suicidal) Thoughts rules*, among many other data patterns. Turning on DLP analysis is as simple as ticking a single radio button and entering a password to link the proxy to the DLP policies. You can then create policies as you see fit.

Rules and dictionaries are ready to go "out of the box," once again enabled with only a few mouse clicks. The policies can work in numerous ways depending on what you're looking for and how strict you want to be. The pattern dictionaries comprise a combination of keywords, regular expressions and context awareness. In terms of policy enforcement, they provide a higher degree of accuracy than a standalone keyword search.

You can also choose from three versions of each dictionary: narrow, wide and default. These provide stricter or more relaxed versions of the rule and what then determines incident creation.
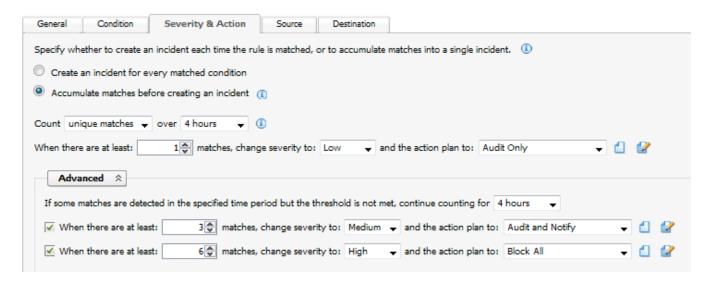

The Incidents can be created either each time contravening content is detected, or over time. For example, you can create an incident if you see more than three posts from one person in a 24-hour period. This second option is especially useful for, say, differentiating between a campaign of abuse and a careless one-off comment.

You may also have multiple versions of the same rule, each triggered under different circumstances. This allows an administrator to monitor the results in different queues and have background data for reference. You can restrict administrator access according to any number of criteria.

Once an incident is created, there are a number of subsequent actions you can choose from, including:

- » Audit
- » Block
- » Audit and Notify (anyone you choose can be notified, including multiple people)
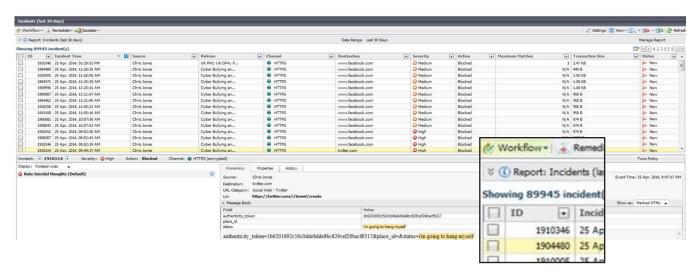- » Any other action you want to create

You can create thresholds within the policy to provide better and more manageable thresholds to a rule. For example, when milder content is detected, the action can simply be to audit the content. If harsher content is detected, then the action can be to block the content and send notifications.

You can set policies to target only certain users or groups, and set multiple versions of similar policies so that different users get a milder or stricter version as appropriate.

Once incidents are created they are visible within reports. Users are identified in the same way as they are with standard web usage. You can see all data regarding exactly what has happened, including destination, time, what Websense technology has done with it and which rule was triggered.

When looking into the forensics, you can also see the specific content that set this rule off – this actual typed-in content is highlighted in the example below.

We hope this has provided you with a brief overview of our capabilities in this difficult area. Please contact Websense if you would like to learn more.

Tom Happé, Education Account Manager, **thappe@websense.com**

Tel. 0118 938 8694 or 07920497788 **www.websense.com/contactme**

websense®

* Please note that while only the web channel is covered under the Web Security Gateway Anywhere licence, we do have the capability to monitor end-point and other common network communication channels such as email, FTP, ActiveSync and others. This additional coverage would of course be part of a larger licence and may require other integration points, but Web Security Gateway Anywhere provides the base framework necessary to do so.

websense®

We hope this has provided you with a brief overview of our capabilities in this difficult area. Please contact Websense if you would like to learn more.

Tom Happé

Education Account Manager

thappe@websense.com

Tel. 0118 938 8694 or 07920497788

www.websense.com/contactme

TRITON STOPS MORE THREATS.
WE CAN PROVE IT.

TRITON®