<table>
<tr><td rowspan="2"><b>cases</b></td><th>doc_1</th><th>doc_2</th><th>decision</th><th>id</th></tr>
<tr>
<td>
<table>
<tr><th>authors</th><td>Dionisio, N.
Alves, F.
Ferreira, P.
Bessani, A.</td></tr>
<tr><th>title</th><td>Cyberthreat Detection from Twitter using Deep Neural Networks</td></tr>
<tr><th>publication_date</th><td>2019-01-01 00:00:00</td></tr>
<tr><th>source</th><td>SupportedSources.CROSSREF</td></tr>
<tr><th>journal</th><td></td></tr>
<tr><th>volume</th><td></td></tr>
<tr><th>doi</th><td>10.1109/ijcnn.2019.8852475</td></tr>
<tr><th>urls</th><td>http://xplorestaging.ieee.org/ielx7/8840768/8851681/08852475.pdf?arnumber=8852475
http://dx.doi.org/10.1109/ijcnn.2019.8852475</td></tr>
<tr><th>id</th><td>id2810697748031288549</td></tr>
<tr><th>abstract</th><td></td></tr>
<tr><th>versions</th><td></td></tr>
</table>
</td>
<td>
<table>
<tr><th>authors</th><td>Nuno DionÃsio
Fernando Alves
Pedro M. Ferreira
Alysson Bessani</td></tr>
<tr><th>title</th><td>Cyberthreat Detection from Twitter using Deep Neural Networks</td></tr>
<tr><th>publication_date</th><td>2019-04-01 22:04:29+00:00</td></tr>
<tr><th>source</th><td>SupportedSources.ARXIV</td></tr>
<tr><th>journal</th><td>None</td></tr>
<tr><th>volume</th><td></td></tr>
<tr><th>doi</th><td></td></tr>
<tr><th>urls</th><td>http://arxiv.org/pdf/1904.01127v1
http://arxiv.org/abs/1904.01127v1
http://arxiv.org/pdf/1904.01127v1</td></tr>
<tr><th>id</th><td>id-637264188375736908</td></tr>
<tr><th>abstract</th><td>To be prepared against cyberattacks, most organizations resort to security information and event management systems to monitor their infrastructures. These systems depend on the timeliness and relevance of the latest updates, patches and threats provided by cyberthreat intelligence feeds. Open source intelligence platforms, namely social media networks such as Twitter, are capable of aggregating a vast amount of cybersecurity-related sources. To process such information streams, we require scalable and efficient tools capable of identifying and summarizing relevant information for specified assets. This paper presents the processing pipeline of a novel tool that uses deep neural networks to process cybersecurity information received from Twitter. A convolutional neural network identifies tweets containing security-related information relevant to assets in an IT infrastructure. Then, a bidirectional long short-term memory network extracts named entities from these tweets to form a security alert or to fill an indicator of compromise. The proposed pipeline achieves an average 94% true positive rate and 91% true negative rate for the classification task and an average F1-score of 92% for the named entity recognition task, across three case study infrastructures.</td></tr>
<tr><th>versions</th><td></td></tr>
</table>
</td>
<td>DUPLICATES</td>
<td>146</td>
</tr>
</table>