Teradata Aster® Insider Threat Solution

TERADATA ASTER SOLUTIONS

Behavioral Analytics and Predictive Modeling to Identify Insider Threats

Information is everywhere

We rely on networks every minute of the day for just about everything including entertainment, communications, and security to name just a few. All the information stored and transmitted requires increased vigilance to safeguard against data leakage and malicious use in the wrong hands. Individual consumers have had their credit card numbers compromised. Corporations have had their internal communications made public. Governments have seen their top secret records copied and distributed. Current network security solutions are clearly not sufficient to safeguard the information we entrust to them.

The biggest problem? It's not what you think

While most businesses have fortified the perimeters of their networks to rebuff unauthorized access by hackers, the larger threat originates from individuals authorized to access and use the data. These insiders are responsible for the vast majority of information breaches that threaten our security on so many levels.

Consider the fact that insiders with valid credentials constantly access the network to fulfill their job requirements. Employees, contractors, and partners are all insiders, and their access does not set off any alarms. These insiders are all potential threats, especially as time passes. An employee may be planning to steal IP as they take a job with a competitor. A contractor may be nearing her end date. A partner may be inadvertently sharing confidential information with your competitors.

Key Highlights

Combine structured or unstructured data with personnel profiles and active directory logs to highlight rogue activity.

Understand multi-event patterns that constitute a potential threat coming from inside your network.

Discover unknown network behavior contrary to corporate security policy.

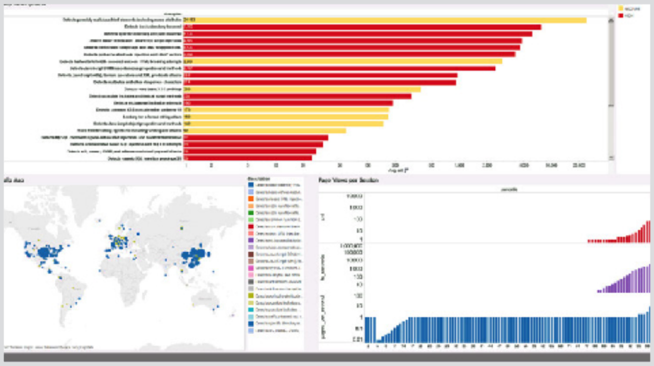


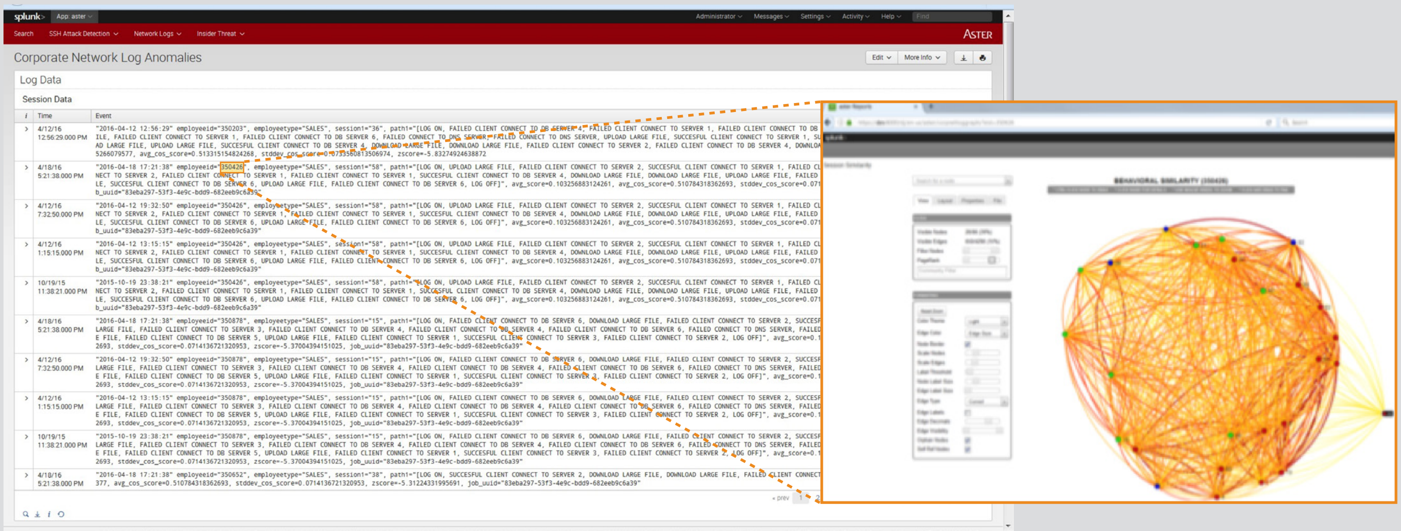
Figure 1. Create a prioritized risk dashboard in Tableau (or other BI tool).

Popular Use Cases

- Aggregation and query of access logs to identify rogue events
- Flag unexpected lateral movement of data
- Detect possible data exfiltration events
- Identify out of policy resource usage

How can you combat it if you can't even see it?

Insiders' actions, malicious or not, are much more subtle and difficult to detect. Your sales people need access to your CRM system with customer information, but the minute one of them entertains an offer from a competitor, he becomes a potential source of data loss. How do you know when authorized access is cause for alarm?



Corporate Network Log Anomalies

Log Data

Session Data

```
i  Time                  Event
>  4/12/16               "2016-04-12 12:56:29" employeeid="350203", employeetype="SALES", session1="36", path1="[LOG ON, FAILED CLIENT CONNECT TO DB SERVER 4, FAILED CLIENT CONNECT TO SERVER 1, FAILED CLIENT CONNECT TO DB
   12:56:29.000 PM       ILE, FAILED CLIENT CONNECT TO SERVER 1, FAILED CLIENT CONNECT TO DB SERVER 6, FAILED CONNECT TO DNS SERVER, FAILED CONNECT TO DNS SERVER, UPLOAD LARGE FILE, SUCCESFUL CLIENT CONNECT TO SERVER 1, SU
                         AD LARGE FILE, UPLOAD LARGE FILE, SUCCESFUL CLIENT CONNECT TO DB SERVER 4, DOWNLOAD LARGE FILE, DOWNLOAD LARGE FILE, FAILED CLIENT CONNECT TO SERVER 2, FAILED CLIENT CONNECT TO DB SERVER 4, DOWNLOA
                         5266079577, avg_cos_score=0.513315154824268, stddev_cos_score=0.0733560813506974, zscore=-5.83274924638872
>  4/18/16               "2016-04-18 17:21:38" employeeid="350426", employeetype="SALES", session1="58", path1="[LOG ON, UPLOAD LARGE FILE, FAILED CLIENT CONNECT TO SERVER 2, SUCCESFUL CLIENT CONNECT TO SERVER 1, FAILED CL
   5:21:38.000 PM        NECT TO SERVER 2, FAILED CLIENT CONNECT TO SERVER 1, FAILED CLIENT CONNECT TO SERVER 1, SUCCESFUL CLIENT CONNECT TO DB SERVER 4, DOWNLOAD LARGE FILE, DOWNLOAD LARGE FILE, UPLOAD LARGE FILE, FAILED
                         LE, SUCCESFUL CLIENT CONNECT TO DB SERVER 6, UPLOAD LARGE FILE, FAILED CLIENT CONNECT TO DB SERVER 6, LOG OFF]", avg_score=0.103256883124261, avg_cos_score=0.510784318362693, stddev_cos_score=0.071
                         b_uuid="83eba297-53f3-4e9c-bdd9-682eeb9c6a39"
>  4/12/16               "2016-04-12 19:32:50" employeeid="350426", employeetype="SALES", session1="58", path1="[LOG ON, UPLOAD LARGE FILE, FAILED CLIENT CONNECT TO SERVER 2, SUCCESFUL CLIENT CONNECT TO SERVER 1, FAILED CL
   7:32:50.000 PM        NECT TO SERVER 2, FAILED CLIENT CONNECT TO SERVER 1, FAILED CLIENT CONNECT TO SERVER 1, SUCCESFUL CLIENT CONNECT TO DB SERVER 4, DOWNLOAD LARGE FILE, DOWNLOAD LARGE FILE, UPLOAD LARGE FILE, FAILED
                         LE, SUCCESFUL CLIENT CONNECT TO DB SERVER 6, UPLOAD LARGE FILE, FAILED CLIENT CONNECT TO DB SERVER 6, LOG OFF]", avg_score=0.103256883124261, avg_cos_score=0.510784318362693, stddev_cos_score=0.071
                         b_uuid="83eba297-53f3-4e9c-bdd9-682eeb9c6a39"
>  4/12/16               "2016-04-12 13:15:15" employeeid="350426", employeetype="SALES", session1="58", path1="[LOG ON, UPLOAD LARGE FILE, FAILED CLIENT CONNECT TO SERVER 2, SUCCESFUL CLIENT CONNECT TO SERVER 1, FAILED CL
   1:15:15.000 PM        NECT TO SERVER 2, FAILED CLIENT CONNECT TO SERVER 1, FAILED CLIENT CONNECT TO SERVER 1, SUCCESFUL CLIENT CONNECT TO DB SERVER 4, DOWNLOAD LARGE FILE, DOWNLOAD LARGE FILE, UPLOAD LARGE FILE, FAILED
                         LE, SUCCESFUL CLIENT CONNECT TO DB SERVER 6, UPLOAD LARGE FILE, FAILED CLIENT CONNECT TO DB SERVER 6, LOG OFF]", avg_score=0.103256883124261, avg_cos_score=0.510784318362693, stddev_cos_score=0.071
                         b_uuid="83eba297-53f3-4e9c-bdd9-682eeb9c6a39"
>  10/19/15              "2015-10-19 23:38:21" employeeid="350426", employeetype="SALES", session1="58", path1="[LOG ON, UPLOAD LARGE FILE, FAILED CLIENT CONNECT TO SERVER 2, SUCCESFUL CLIENT CONNECT TO SERVER 1, FAILED CL
   11:38:21.000 PM       NECT TO SERVER 2, FAILED CLIENT CONNECT TO SERVER 1, FAILED CLIENT CONNECT TO SERVER 1, SUCCESFUL CLIENT CONNECT TO DB SERVER 4, DOWNLOAD LARGE FILE, DOWNLOAD LARGE FILE, UPLOAD LARGE FILE, FAILED
                         LE, SUCCESFUL CLIENT CONNECT TO DB SERVER 6, UPLOAD LARGE FILE, FAILED CLIENT CONNECT TO DB SERVER 6, LOG OFF]", avg_score=0.103256883124261, avg_cos_score=0.510784318362693, stddev_cos_score=0.071
                         b_uuid="83eba297-53f3-4e9c-bdd9-682eeb9c6a39"
>  4/18/16               "2016-04-18 17:21:38" employeeid="350878", employeetype="SALES", session1="15", path1="[LOG ON, FAILED CLIENT CONNECT TO DB SERVER 6, DOWNLOAD LARGE FILE, FAILED CLIENT CONNECT TO SERVER 2, SUCCESF
   5:21:38.000 PM        LARGE FILE, FAILED CLIENT CONNECT TO SERVER 3, FAILED CLIENT CONNECT TO DB SERVER 4, FAILED CLIENT CONNECT TO DB SERVER 4, FAILED CLIENT CONNECT TO DB SERVER 6, FAILED CONNECT TO DNS SERVER, FAILED
                         E FILE, FAILED CLIENT CONNECT TO DB SERVER 5, UPLOAD LARGE FILE, FAILED CLIENT CONNECT TO SERVER 1, SUCCESFUL CLIENT CONNECT TO SERVER 3, FAILED CLIENT CONNECT TO SERVER 2, LOG OFF]", avg_score=0.1
                         2693, stddev_cos_score=0.0714136721320953, zscore=-5.37004394151025, job_uuid="83eba297-53f3-4e9c-bdd9-682eeb9c6a39"
>  4/12/16               "2016-04-12 19:32:50" employeeid="350878", employeetype="SALES", session1="15", path1="[LOG ON, FAILED CLIENT CONNECT TO DB SERVER 6, DOWNLOAD LARGE FILE, FAILED CLIENT CONNECT TO SERVER 2, SUCCESF
   7:32:50.000 PM        LARGE FILE, FAILED CLIENT CONNECT TO SERVER 3, FAILED CLIENT CONNECT TO DB SERVER 4, FAILED CLIENT CONNECT TO DB SERVER 4, FAILED CLIENT CONNECT TO DB SERVER 6, FAILED CONNECT TO DNS SERVER, FAILED
                         E FILE, FAILED CLIENT CONNECT TO DB SERVER 5, UPLOAD LARGE FILE, FAILED CLIENT CONNECT TO SERVER 1, SUCCESFUL CLIENT CONNECT TO SERVER 3, FAILED CLIENT CONNECT TO SERVER 2, LOG OFF]", avg_score=0.1
                         2693, stddev_cos_score=0.0714136721320953, zscore=-5.37004394151025, job_uuid="83eba297-53f3-4e9c-bdd9-682eeb9c6a39"
>  4/12/16               "2016-04-12 13:15:15" employeeid="350878", employeetype="SALES", session1="15", path1="[LOG ON, FAILED CLIENT CONNECT TO DB SERVER 6, DOWNLOAD LARGE FILE, FAILED CLIENT CONNECT TO SERVER 2, SUCCESF
   1:15:15.000 PM        LARGE FILE, FAILED CLIENT CONNECT TO SERVER 3, FAILED CLIENT CONNECT TO DB SERVER 4, FAILED CLIENT CONNECT TO DB SERVER 4, FAILED CLIENT CONNECT TO DB SERVER 6, FAILED CONNECT TO DNS SERVER, FAILED
                         E FILE, FAILED CLIENT CONNECT TO DB SERVER 5, UPLOAD LARGE FILE, FAILED CLIENT CONNECT TO SERVER 1, SUCCESFUL CLIENT CONNECT TO SERVER 3, FAILED CLIENT CONNECT TO SERVER 2, LOG OFF]", avg_score=0.1
                         2693, stddev_cos_score=0.0714136721320953, zscore=-5.37004394151025, job_uuid="83eba297-53f3-4e9c-bdd9-682eeb9c6a39"
>  10/19/15              "2015-10-19 23:38:21" employeeid="350878", employeetype="SALES", session1="15", path1="[LOG ON, FAILED CLIENT CONNECT TO DB SERVER 6, DOWNLOAD LARGE FILE, FAILED CLIENT CONNECT TO SERVER 2, SUCCESF
   11:38:21.000 PM       LARGE FILE, FAILED CLIENT CONNECT TO SERVER 3, FAILED CLIENT CONNECT TO DB SERVER 4, FAILED CLIENT CONNECT TO DB SERVER 4, FAILED CLIENT CONNECT TO DB SERVER 6, FAILED CONNECT TO DNS SERVER, FAILED
                         E FILE, FAILED CLIENT CONNECT TO DB SERVER 5, UPLOAD LARGE FILE, FAILED CLIENT CONNECT TO SERVER 1, SUCCESFUL CLIENT CONNECT TO SERVER 3, FAILED CLIENT CONNECT TO SERVER 2, LOG OFF]", avg_score=0.1
                         2693, stddev_cos_score=0.0714136721320953, zscore=-5.37004394151025, job_uuid="83eba297-53f3-4e9c-bdd9-682eeb9c6a39"
>  4/18/16               "2016-04-18 17:21:38" employeeid="350652", employeetype="SALES", session1="38", path1="[LOG ON, SUCCESFUL CLIENT CONNECT TO SERVER 2, DOWNLOAD LARGE FILE, DOWNLOAD LARGE FILE, FAILED CLIENT CONNECT
   5:21:38.000 PM        377, avg_cos_score=0.510784318362693, stddev_cos_score=0.0714136721320953, zscore=-5.31224331995691, job_uuid="83eba297-53f3-4e9c-bdd9-682eeb9c6a39"
```

Figure 2. Drill down and access advanced analytics directly from your Splunk console.

The Teradata Aster® approach to threat detection leverages our unique ability to combine multiple data sources into data sets that reveal the complete story. Security analysts and business users alike can get a comprehensive view of an insider's activity and the context in which it occurs. A simple fact in isolation may appear benign, but when viewed in the larger context, the threat becomes apparent. The result is unmatched multi-dimensional analyses that illuminate patterns of suspicious activity invisible to less sophisticated point solutions.

Get more from what you already know

Something as simple as combining a list of recently terminated employees, their VPN credentials, and a network usage log can highlight undesired behaviors that signal malicious intent. You could combine these results with employee behavioral clustering to formulate predictive models that identify previously unknown threat patterns. Over time, the accumulation of additional training data will improve the accuracy of your predictive models.

Advanced analytics where you need it

As with all Teradata analytic solutions, Insider Threat comes with a suite of pre-built applications that outputs interactive visualizations. Our open architecture allows you to surface these results wherever you and your team want to consume them.

Learn more

For information about the Teradata Aster Insider Threat Solution, visit **Aster-Community.Teradata.com**.

All Industries, All Sectors Addressed

Every enterprise of any scale relies on a network and needs to ensure its security. The need is acute in commercial enterprises and governments.

10000 Innovation Drive, Dayton, OH 45342   **Teradata.com**

Teradata, Aster, and the Teradata logo are registered trademarks of Teradata Corporation and/or its affiliates in the U.S. and worldwide. Teradata continually improves products as new technologies and components become available. Teradata, therefore, reserves the right to change specifications without prior notice. All features, functions, and operations described herein may not be marketed in all parts of the world. Consult your Teradata representative or Teradata.com for more information.

08.16   EB7193