

Operational Intelligence

Robert Panholzer,
Channel Sales Manager DACH

René Siekermann,
Senior Sales Engineer DACH



splunk

Macht Maschinendaten zugreifbar, nutzbar
und wertvoll für jedermann.

Wie sehen Maschinendaten aus?

Sources



ORDER,2013-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

Order Processing



May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213.
Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException:
weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The
DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port:
ACMEDB-01:1521. Reason: Connection refused

Middleware Error



Care IVR

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type
0:19:9, App 0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-
13ae51a6d092, Trunk T451.16
05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092
CUSTID 10098213
05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

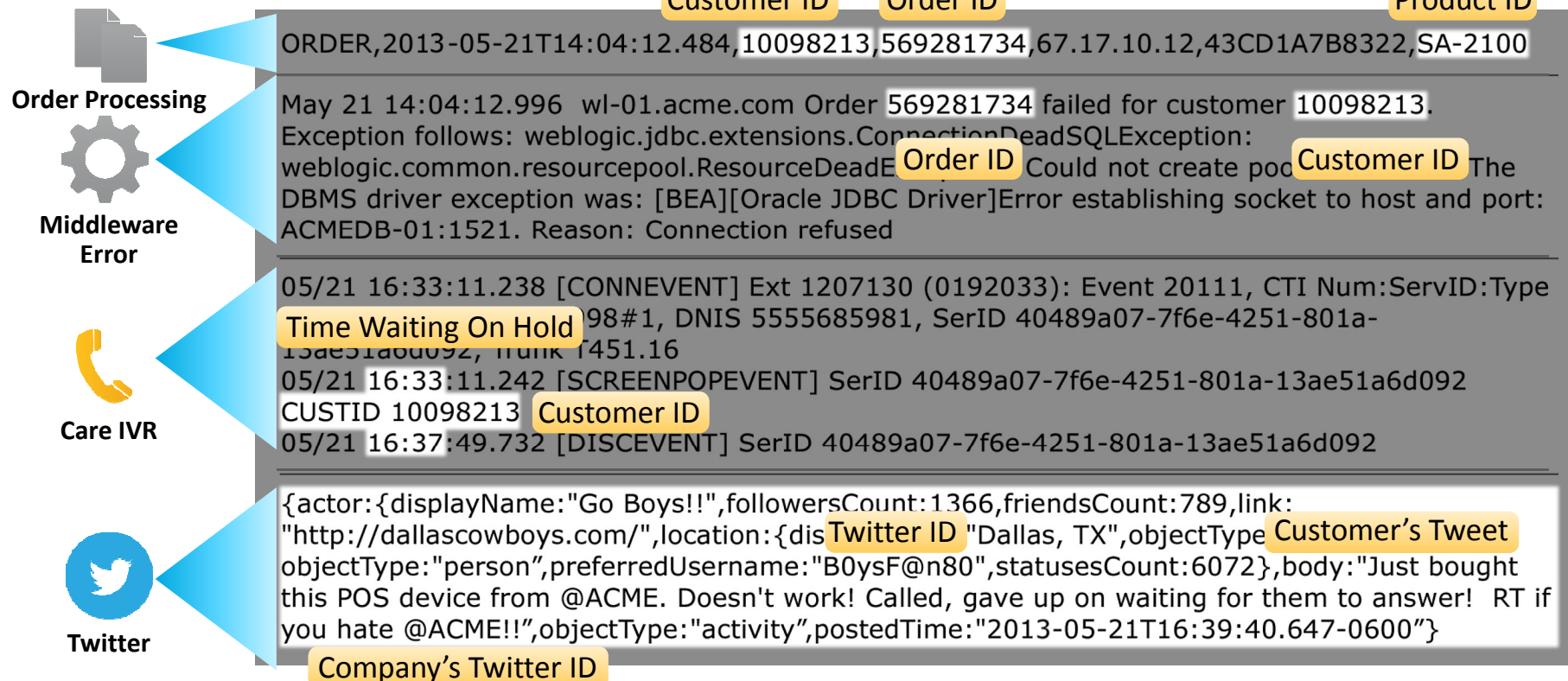


Twitter

{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:
"http://dallascowboys.com/",location:{displayName:"Dallas, TX",objectType:"place"},
objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought
this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if
you hate @ACME!!",objectType:"activity",postedTime:"2013-05-21T16:39:40.647-0600"}

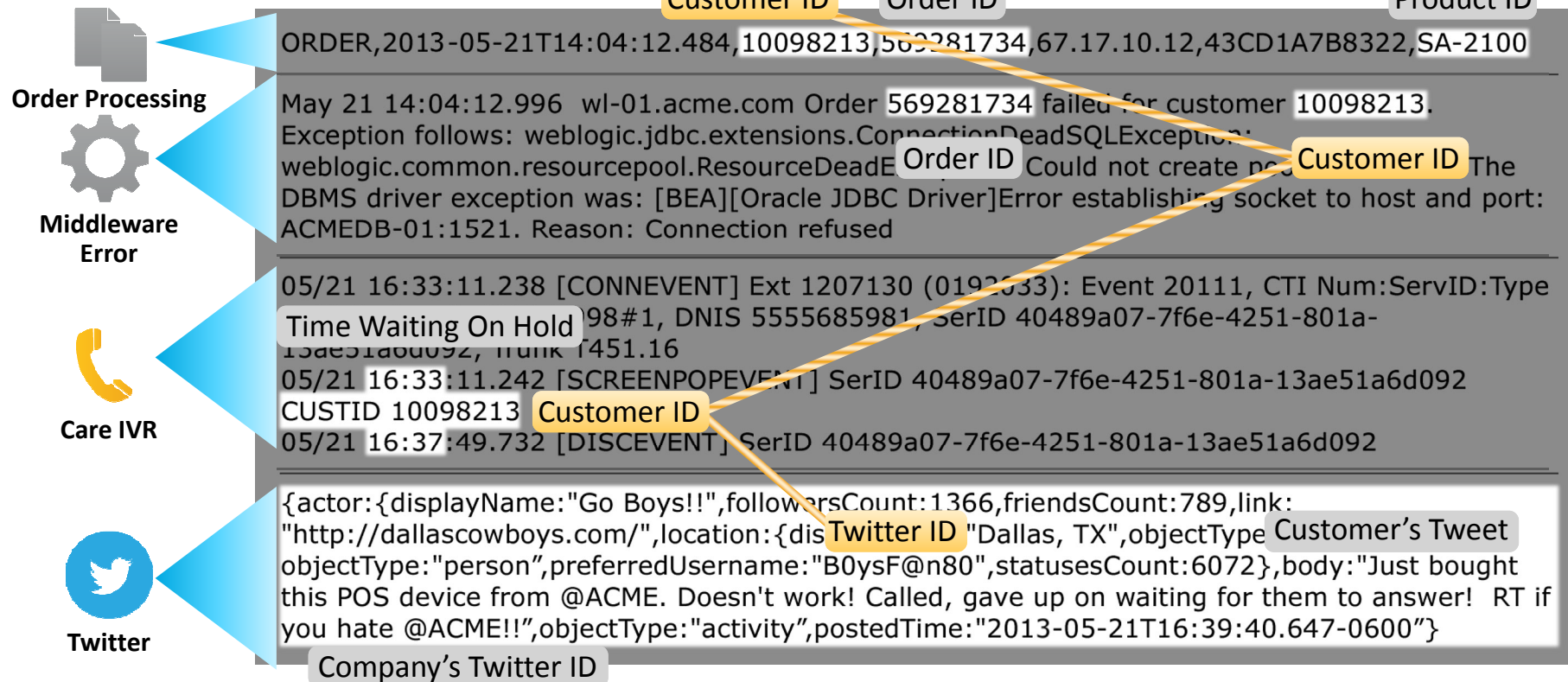
Maschinendaten enthalten wertvolle Informationen

Sources

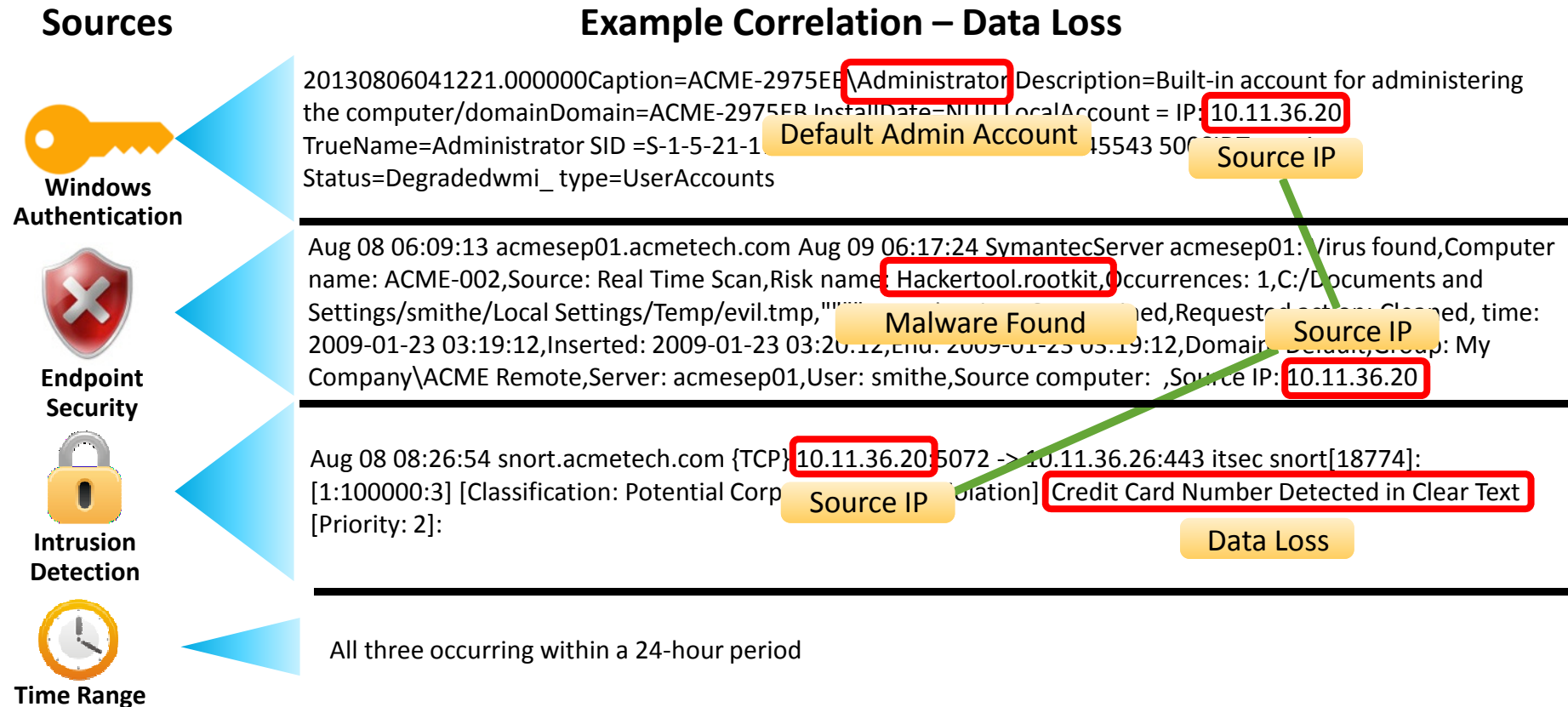


Maschinendaten enthalten wertvolle Informationen

Sources



Real-time Monitoring of *Known* Threats



Real-time Monitoring of *Unknown* Threats

Sources



Email Server

2013-08-09T12:40:25.475Z,,exch-hub-den-01,,exch-mbx-cup-
00,,,STOREDRIVER,DELIVER,79426,<20130809050115.18154.11234@acme.com>,johndoe@acme.com,685191,1
,,hacker@neverseenbefore.com Please open this attachment with payroll information,, ,2013-08-
0

Rarely seen email domain



Web Proxy

201 [Rarely visited web site] .29 98483 148 TCP_HIT 200 200 0 622 -- OBSERVED GET
www.neverbeenseenbefore.com HTTP/1.1 0 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR
2.0.50727; InfoPath.1; MS-RTC LM 8; .NET CLR 1.1.4322; .NET CLR 3.0.4506.2152;) User John Doe"



Endpoint Logs

08/09/2013 10:00:00 AM [User Name] sent_status="(0)The operation completed successfully. "pid=1300
process_image="\\John Doe\\Device\\HarddiskVolume1\\Windows\\System32\\(neverseenbefore.exe" registry_type
="CreateKey"key_path="\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ Printers
Print\\Providers\\ John Doe-PC\\Printers\\{\\ NeverSeenbefore" data_type=" Rarely seen service



Time Range

All three occurring within a 24-hour period



Demo

splunk>