SF-SafeDump®

DUMP & LOG FILE ANONYMIZATION TO EFFECTIVELY PREVENT CONFIDENTIAL DATA LEAKAGE AND THEFT

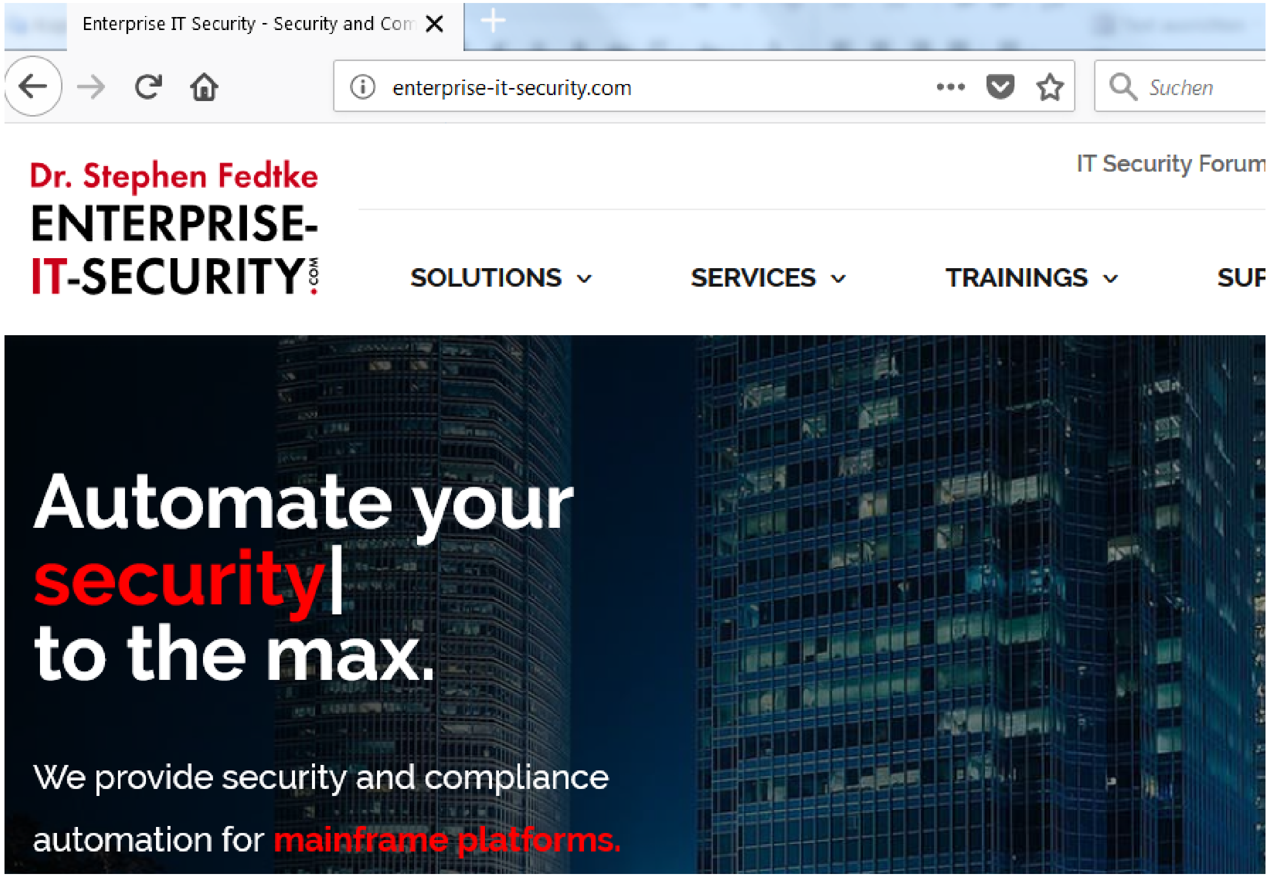
Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.COM

PREVENT CONFIDENTIAL DATA LEAKAGE VIA DUMP & LOG FILE ANONYMIZATION

Agenda “Dump Anonymization”

- **Enterprise-IT-Security.com** and our **Integrity 2.0** initiative
- **What’s the problem** with system dumps and logs?
- Why is it necessary to **combat these risks**?
- How **SF-SafeDump** helps you comply with the new security and privacy requirements
- How to **successfully integrate** dump and log security into your daily IT workflow
- No impact on cooperation with **software vendors**

Enterprise-IT-Security.com



Enterprise IT Security - Security and Com
enterprise-it-security.com
Suchen
IT Security Forum
Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.com
SOLUTIONS
SERVICES
TRAININGS
SUF

Automate your security| to the max.

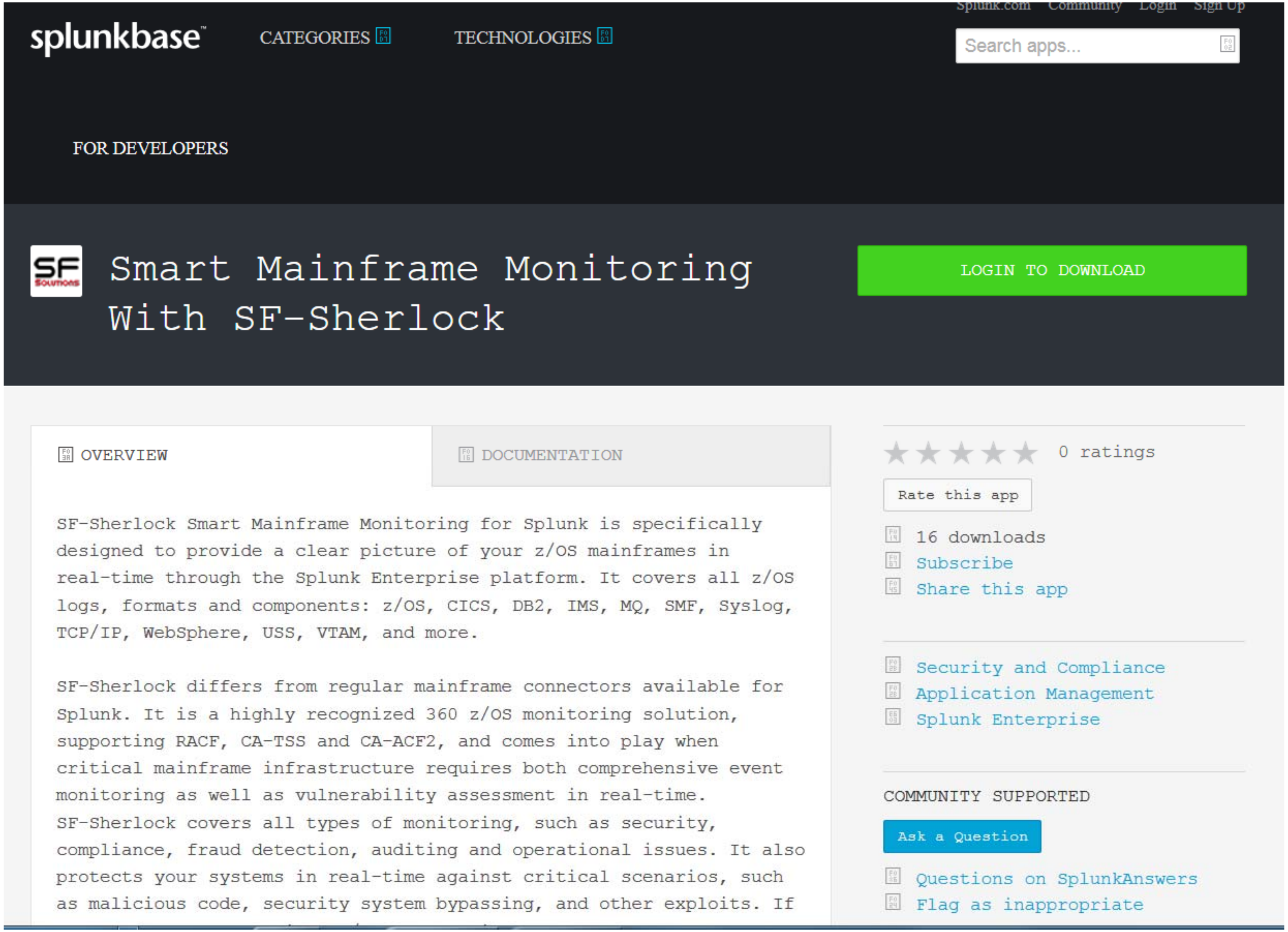
We provide security and compliance automation for mainframe platforms.

Welcome to

Integrity 2.0 for System z

Our “Integrity 2.0 for System z” solutions initiative focuses on today’s required new level of securing and protecting critical infrastructure

Naturally, we support RACF, CA-ACF2 and CA-TSS.



Smart Mainframe Monitoring With SF-Sherlock

SF-Sherlock Smart Mainframe Monitoring for Splunk is specifically designed to provide a clear picture of your z/OS mainframes in real-time through the Splunk Enterprise platform. It covers all z/OS logs, formats and components: z/OS, CICS, DB2, IMS, MQ, SMF, Syslog, TCP/IP, WebSphere, USS, VTAM, and more.

SF-Sherlock differs from regular mainframe connectors available for Splunk. It is a highly recognized 360 z/OS monitoring solution, supporting RACF, CA-TSS and CA-ACF2, and comes into play when critical mainframe infrastructure requires both comprehensive event monitoring as well as vulnerability assessment in real-time. SF-Sherlock covers all types of monitoring, such as security, compliance, fraud detection, auditing and operational issues. It also protects your systems in real-time against critical scenarios, such as malicious code, security system bypassing, and other exploits. If

☆☆☆☆☆ 0 ratings

16 downloads

Security and Compliance
Application Management
Splunk Enterprise

COMMUNITY SUPPORTED

Forensic and Emergency Support for z

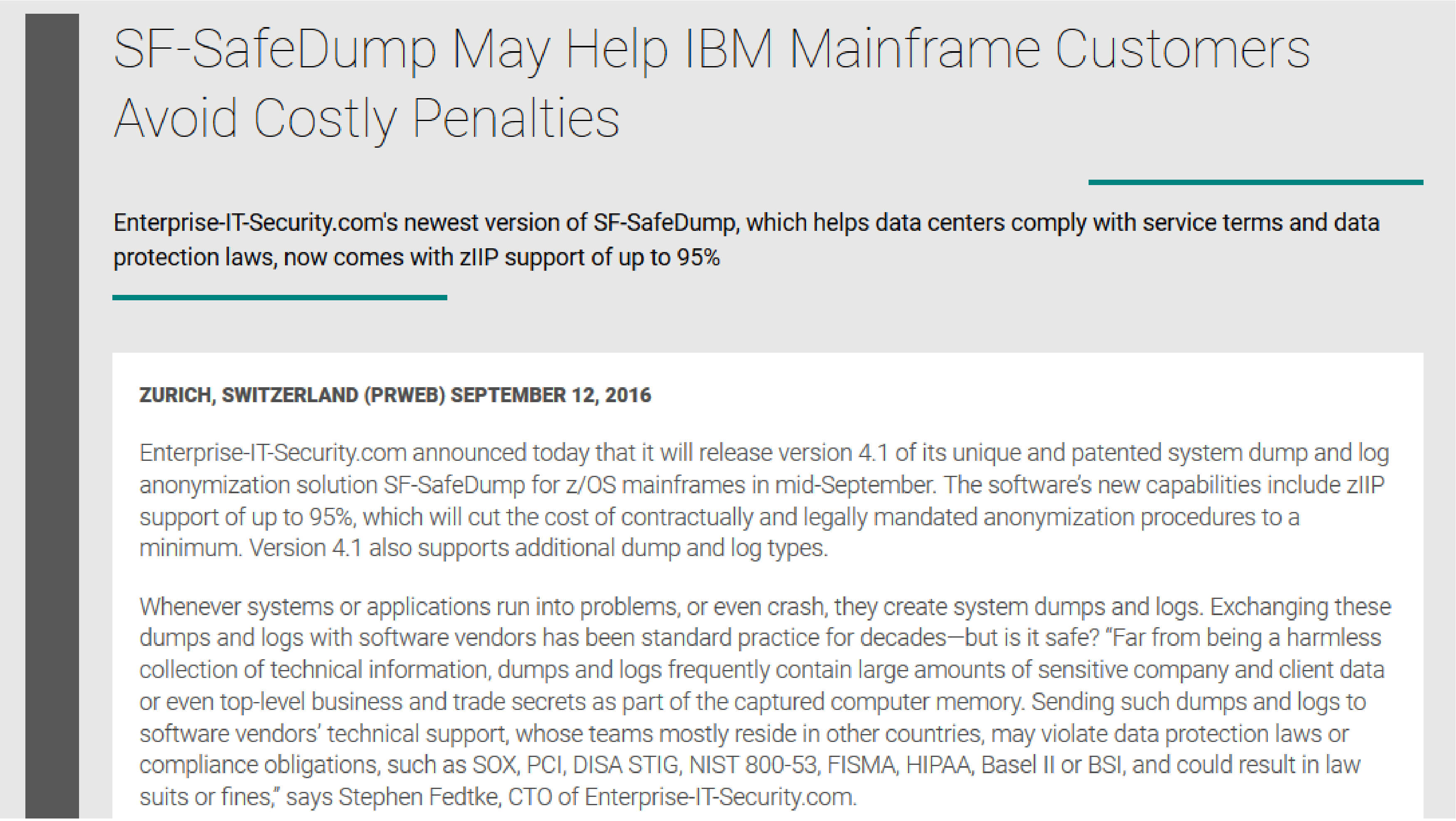
JUST IN CASE!

As you can see, our company

is uniquely positioned to

eliminate your

mainframe’s top-level risks



SF-SafeDump May Help IBM Mainframe Customers Avoid Costly Penalties

Enterprise-IT-Security.com's newest version of SF-SafeDump, which helps data centers comply with service terms and data protection laws, now comes with zIIP support of up to 95%

ZURICH, SWITZERLAND (PRWEB) SEPTEMBER 12, 2016

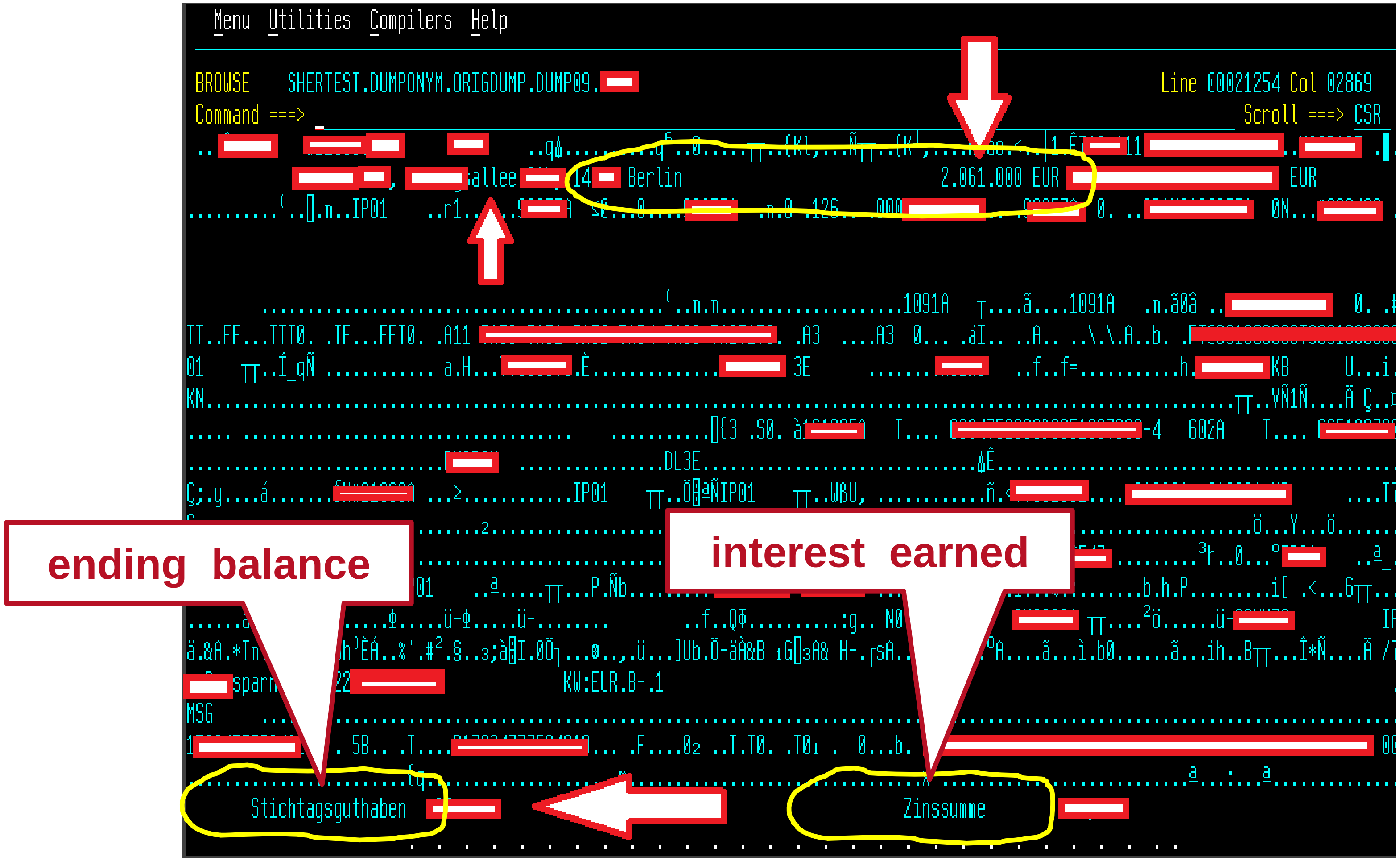
Enterprise-IT-Security.com announced today that it will release version 4.1 of its unique and patented system dump and log anonymization solution SF-SafeDump for z/OS mainframes in mid-September. The software's new capabilities include zIIP support of up to 95%, which will cut the cost of contractually and legally mandated anonymization procedures to a minimum. Version 4.1 also supports additional dump and log types.

Whenever systems or applications run into problems, or even crash, they create system dumps and logs. Exchanging these dumps and logs with software vendors has been standard practice for decades—but is it safe? "Far from being a harmless collection of technical information, dumps and logs frequently contain large amounts of sensitive company and client data or even top-level business and trade secrets as part of the captured computer memory. Sending such dumps and logs to software vendors' technical support, whose teams mostly reside in other countries, may violate data protection laws or compliance obligations, such as SOX, PCI, DISA STIG, NIST 800-53, FISMA, HIPAA, Basel II or BSI, and could result in law suits or fines," says Stephen Fedtke, CTO of Enterprise-IT-Security.com.

So let’s start and talk in detail about the risks that result from forwarding system dumps and logs

to third parties (e.g., software vendors)

A Picture is Worth a Thousand Words ...



```
 Menu  Utilities  Compilers  Help
BROWSE    SHERTEST.DUMPONYM.ORIGDUMP.DUMP09.[redacted]                Line 00021254 Col 02869
Command ===> _                                                              Scroll ===> CSR
..[redacted]  [redacted]  [redacted]   ..q∅........q ..0.....╥┬..{K},...Ñ┬┬..{K },......00.<..│1 Ê[redacted]11[redacted].[redacted] .
        [redacted], [redacted]allee[redacted] 14[redacted] Berlin                      2.061.000 EUR [redacted]  EUR
.........'..▯.n..IP01    ..r1....[redacted]  s0...0.....[redacted]  .n.0 .126.. 000[redacted]  [redacted] 0. ..[redacted]  0N...[redacted] .


     ............................................'..n.n.....................1091A   ┬....ã....1091A   .n.ã0â ..[redacted]   0. .‡
TT..FF...TTT0. .TF...FFT0. .A11 [redacted]. .A3   ....A3  0... .äI.. ..A.. ..\.\.A..b. .[redacted]
01    ╥┬..Í_qÑ ........... a.H...[redacted]È.............[redacted] 3E      .......[redacted]  ..f..f=..........h.[redacted]KB     U...i.
KN.....................................................................................................╥┬..VÑ1Ñ....Ã Ç..
..... ...............................   ..........▯{3 .S0. à[redacted]   T.... [redacted]-4   602A    T.... [redacted]
...........................[redacted]  ................DL3E.................................∅Ê.................................
Ç;.y....á.......[redacted]  ...≥............IP01    ╥┬..Ö▯ªÑIP01    ╥┬..WBU, ............ñ.<[redacted]....[redacted]      ....T
Ç                         .......2.......................                        ........................ö...Y...ö.......
                          ........................................               [redacted]........³h..0...°[redacted]    ..ª_
                          01     ..ª.....╥┬...P.Ñb......                          .........b.h.P.........i[ .<...6╥┬...
......ä                ....ϕ.....ü-ϕ.....ü-........      ..f..Qϕ..........:g.. N0          [redacted]  ╥┬....²ö......ü-[redacted]       IF
ä.&A.*Tn               h⁾ÈÁ..%'.#².§..₃;à▯I.0Ö┐...ø..,.ü...]Ub.Ö-äÀ&B ıG▯₃A& H-.┌sA..      ºA....ã...ì.b0......ã...ih..B╥┬...Î*Ñ....Ã /
[redacted]sparn        22[redacted]                   KW:EUR.B-.1                                                          .
MSG       ........................................................................................................................
1[redacted]           . 5B.. .T....[redacted]... .F....0₂ ..T.T0. .T0₁ .  0...b.   [redacted]   00
.......................................{q.......................................................ª.....ª.........................
        Stichtagsguthaben [redacted]                                Zinssumme            [redacted]
                             . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
```

ending balance

interest earned

Risks associated with dump and log files concern BOTH your customers' privacy as well as your data center's security

All in all, system dumps and logs include such a wide spectrum and high volume of sensitive information

that you absolutely shouldn’t share them – not even with your “best friends.”

What’s even worse: You are ultimately responsible for any secret you send out!

“… You will not send or provide IBM access to any personally-identifiable information, whether in data or any other form, and will be responsible for reasonable costs and other amounts that IBM may incur relating to any such information mistakenly provided to IBM or the loss or disclosure of such information by IBM, including those arising out of any third party claims. …"

http://www-05.ibm.com/de/support/ecurep/terms.html

Formal & Legal Risks Resulting from Non-Anonymized Dumps & Logs

- Violating data and privacy protection laws
- Violating compliance obligations

Violations may result in corresponding penalties.

Your risk score may be affected negatively from the perspective of a cyber risk insurance provider.

The ultimate “motivation”

is currently coming

from the GDPR and

its deadline and penalties

GDPR “Highlight” Summary

Requirements and related risks

- On May 25th, data protection will change substantially, because the GDPR that will become effective on that day will demand a **risk-based, proactive approach** with secure processes and controls for the protection of sensitive **personal information** regarding both your customers and employees.

- In particular, the following is new: for your customers, there is a right to the publication, deletion, and emendation of their data. That means that **you must always know “where” their data is located and stored.**

- **Penalties** and thus the risks are substantially increased.

Risks associated with handing over dumps

Conditions and facts that increase risk

- A given dump potentially **goes through many hands,** may be **sent offshore,** or "travel the globe" – most likely, your data will leave your country or even continent!
- There is **no way to keep track of or audit** dump handling activities. You simply don't know who exactly will access your dumps and logs: internal and external employees, sub-contractors, etc.
- **No one can detect** whether sensitive data were extracted.
- The extraction process could be **fully automated.**
- The software vendor may **mistakenly forward** the dump to the wrong party.

“BUT ...”

“We have very strict policies and contracts with our software vendors regulating the exchange of data. Shouldn’t that also cover dumps and logs? We are fine!”

“We encrypt our dumps before transfer. We are fine!”

“We send out only a few dumps a year. It’s not worth it to …”

“We are no Swiss bank, and our government knows everything anyway. Our data isn’t that sensitive.”

“We’ve finally cut down our number of vendors to close to 1!”

These arguments may

sound convincing,

but let’s take a closer look

99% of sensitive data sent with any given dump is absolutely unnecessary for analyzing and identifying the actual problem (“bug”).

There is simply no “return on trust” when handing out so much information.

And you never know

what happens “behind the curtains.”

It’s a fact: One dump in the wrong hands is enough to expose your company’s or even country’s IT platforms to significant risk!

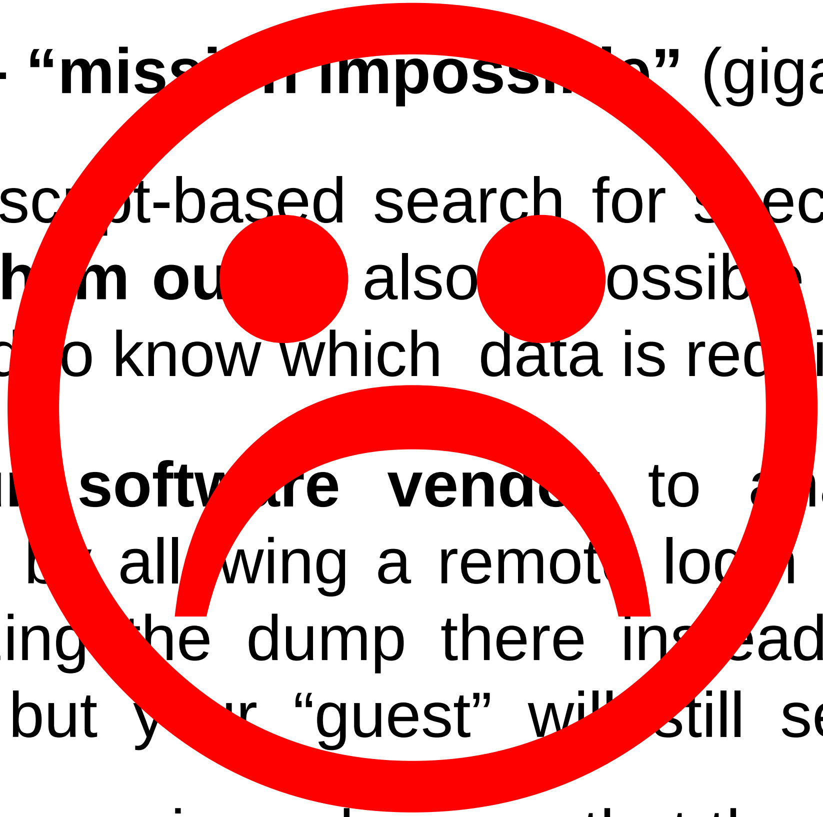
z/OS dumps are alluringly substantial.

“But that’s horrible!”

What are my options?

It’s simple! Dumps and logs need to be thoroughly anonymized before they are sent out – just “take them to the cleaners!”

Manual Options for Dump Anonymization



- **Manually – “mission impossible”** (giga bytes of data!)
- Manual or script-based search for specific strings followed by **“X’ing them out”** also impossible and risky since you would need to know which data is required to fix the “bug”
- **Invite your software vendor** to analyze the problem locally, i.e., by allowing a remote login to your data center and analyzing the dump there instead of handing it out. Good idea, but your “guest” will still see your secrets!

Anonymizing dumps in such a way that they aren’t damaged is a **highly complex task** and challenging from both a technical as well as an algorithm-related perspective.

Effective Dump Anonymization

Basic requirements

- A dump needs to **keep its technical value**
- At the same time, it has to become **"secret-free"**
- **Easy whitelisting** – just in case any memory area with sensitive content is required to analyze the bug
- The entire anonymization procedure needs to be **fully automated** and part of regular system automation
- An **anonymization protocol** needs to be created to prove compliance – "great, it's auditable!"

Effective Dump Anonymization

Technical requirements

- The anonymization has to be easy, automated, and a simple **1-step procedure** before compression (“terse”).
- An **ISPF application** has to support manual handling and processing of selected dumps where required.
- The entire anonymization process needs to be fully **transparent and auditable.**
- All dumps in the **“IPCS format”** need to be supported.
- The process has to include a **comprehensive quality assurance** feature – a final search for “left-overs.”

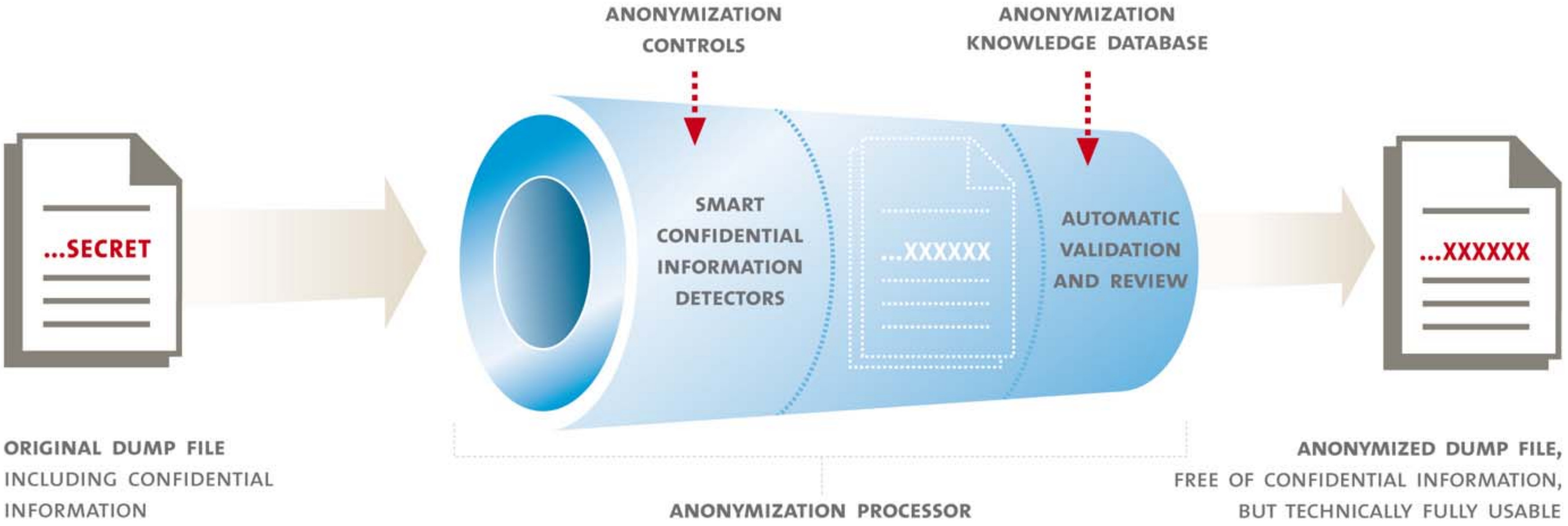
Effective Dump Anonymization

Challenges

- Identifying secrets in a dump is like **“finding a needle in a haystack.”** Approx. 5 to 15% of the dump’s content is sensitive; and this data is randomly distributed.
- Different **codings and character sets** occur.
- **The complex IPCS format must never be invalidated;** all checksums, etc., need to remain valid.
- The **dump’s “technical value”** needs to be fully preserved so that the actual problem (“bug”) can be fixed.
- The process may not require excessive **CPU time.**

SF-SafeDump is the innovative, patented and high-performance solution to anonymize system dumps & logs

Process of Dump & Log Anonymization



ANONYMIZATION CONTROLS

ANONYMIZATION KNOWLEDGE DATABASE

SMART CONFIDENTIAL INFORMATION DETECTORS

AUTOMATIC VALIDATION AND REVIEW

ORIGINAL DUMP FILE INCLUDING CONFIDENTIAL INFORMATION

ANONYMIZATION PROCESSOR

ANONYMIZED DUMP FILE, FREE OF CONFIDENTIAL INFORMATION, BUT TECHNICALLY FULLY USABLE

By the way,
SF-SafeDump also anonymizes
system logs, such as
EREP, syslog, SMF, etc.

How does it work?

- First things first – SF-SafeDump **works**, and achieving our patented Version 5.1 is the result of a multi-year research and development process, and lots of hard work, to accomplish this mission.

- More than 67 **smart algorithms** (January 2018) scan the entire dump according to its type. They have to work hard to achieve a dump free of secrets!

- The dump's cleanup happens in an automated sequence of **5 passes**, incl. high-level quality assurance (“re-scan”).

- **SF-SafeDump learns and adapts** to your installation's specific dump and log contents, usually after 3–6 dumps.

Very important:
SF-SafeDump is easy to install and use - and it keeps getting smarter!

It’s almost as simple as copying – it takes just a little bit longer than TERSE.

Organizational Integration

- You may appoint an internal **main contact (“dump handling agent or manager”)**. This person is responsible for anonymizing any dump that leaves your data center and serves as a contact for software vendors, for example, when a dump’s proper analysis requires particular dump areas in a non-anonymized form.

- Of course, you may also assign an **individual contact for each dump file** instead of appointing one central contact.

- All **contact information** required is kept within the dump and can easily be accessed by the analyzing party.

Organizational Integration

- **Compression ("terse") as well as encryption** will be handled exactly as before.

- The entire anonymization process is easy to integrate into your **system automation procedure**.

- It's easy to integrate your **data protection department** into an automated control loop together with your system programming department.

- If your **mainframes are outsourced,** your service provider will need to anonymize dumps that include your secrets.

How are my software vendors affected?

- Most of the time, **there is no real change or impact** since their software support continues to receive fully usable dumps and logs.

- **Only rarely** do software vendors contact the “dump manager” to ask for non-anonymized dump content.

- After receiving such a request, the dump manager may **choose among two options**: a) a new anonymization may be performed from scratch, or b) only those dump parts that are relevant may be sent over. The method your system programmers prefer is a “matter of taste” and depends primarily on the required level of urgency.

How are my software vendors affected?

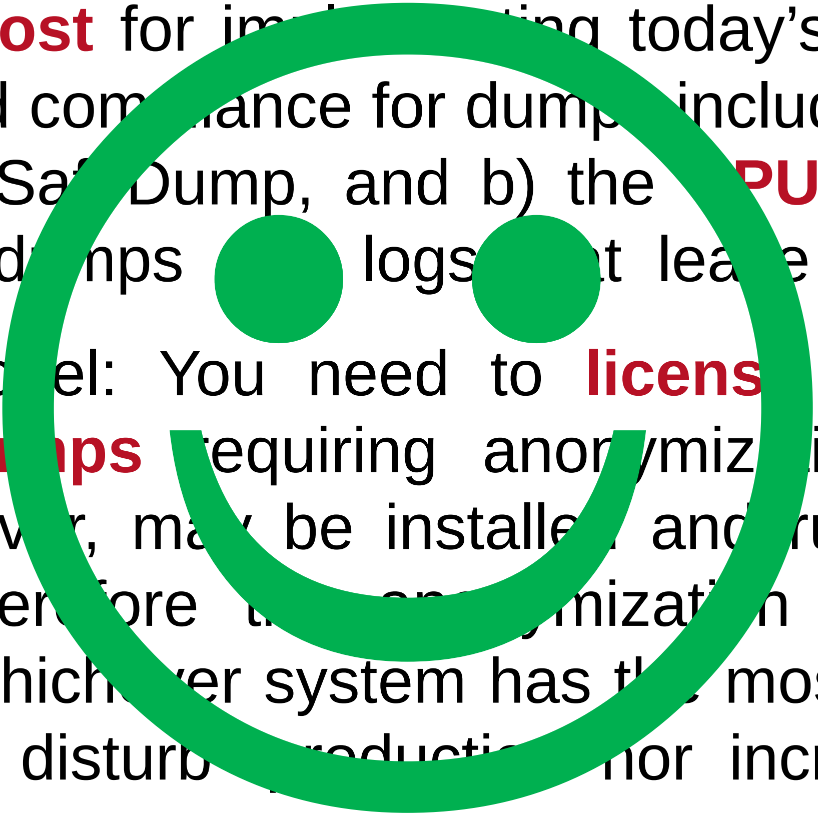
- All software vendors have free access to our **toolkit,** which allows automatic, safe and correct merging of partial dump file content.

- All in all, the way you cooperate with your software vendors will **not change much** – you will just be more secure.

Other platforms than z/OS?

Yes, we are already developing SF-SafeDump for other platforms, and we look forward to keeping you updated. Just let us know about your OS preferences.

What will it cost to handle our dumps safely?



- The **total cost** for implementing today’s required level of security and compliance for dumps includes a) the **license fee** for SF-SafeDump, and b) the **CPU time** required to anonymize dumps and logs that leave your house.

- License model: You need to **license each LPAR that creates dumps** requiring anonymization. The software itself, however, may be installed and run on any of your LPARs. Therefore the anonymization workload can be moved to whichever system has the most capacity left and will neither disturb production nor increase CPU costs.

- **CPU time:** A regular SVC dump will require approx. 0,5 CPU hours per GB to execute all passes. The **zIIP offload** may achieve levels of **up to 95%** or more.

Conclusion

SF-SafeDump meets all best practice requirements and shifts your cooperation with software vendors to a completely new level of trust.

Be ready for GDPR & Integrity 2.0!

Don’t forget to tell your cyber risk insurance provider!

Thank you for attending our presentation!

ENTERPRISE-IT-SECURITY.COM

Dr. Stephen Fedtke
ENTERPRISE-
IT-SECURITY.COM

TEL.++800-DRFEDTKE (WORLDWIDE TOLL-FREE) » ++800-37333853