The z Exchange – December 13, 2018

z/OS Encryption Readiness Technology (zERT)

Chris Meyer, CISSP (meyerchr@us.ibm.com)
z/OS Communications Server design and architecture

Please note

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice and at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

Agenda

- Background – why zERT?
- zERT overview
- Configuring zERT
- Coming in 4Q2018: zERT Network Analyzer
- zERT support in other products
- Considerations
- Summary

Agenda

- **Background – why zERT?**
- zERT overview
- Configuring zERT
- Coming in 4Q2018: zERT Network Analyzer
- zERT support in other products
- Considerations
- Summary

Background: Cryptographic network protection on z/OS

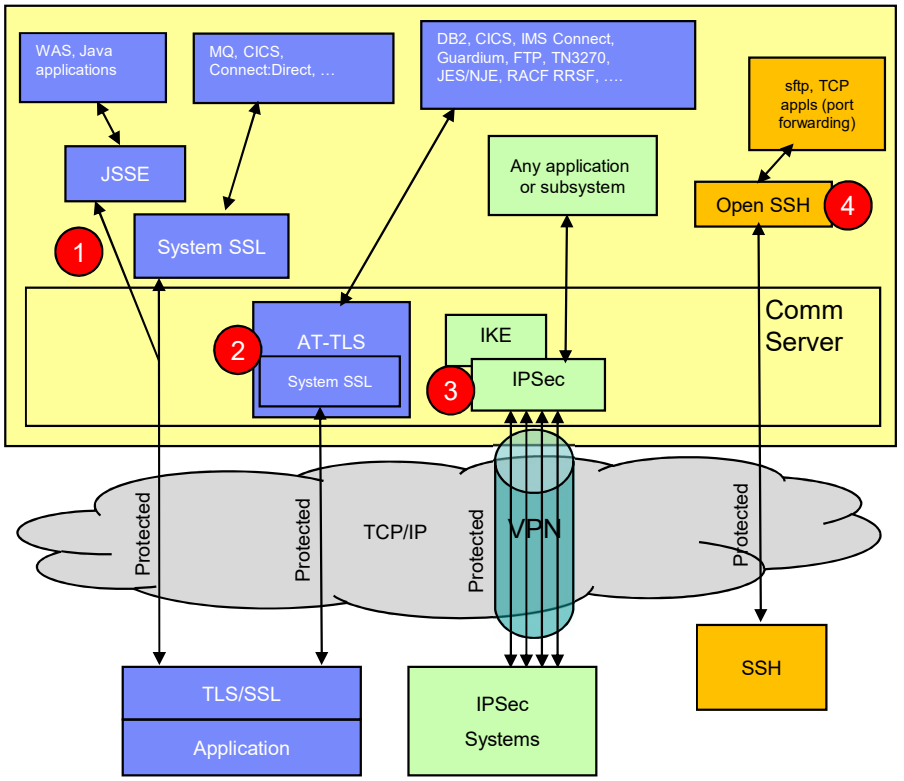
z/OS provides 4* main mechanisms to protect TCP/IP traffic:

1. **TLS/SSL direct usage**
   - Application is explicitly coded to use these
   - Configuration and auditing is unique to each application
   - Per-session protection
   - TCP only

2. **Application Transparent TLS (AT-TLS)**
   - TLS/SSL applied in TCP layer as defined by policy
   - Configured in AT-TLS policy via Configuration Assistant
   - Auditing through SMF 119 records
   - Typically transparent to application
   - TCP/IP stack is user of System SSL services

3. **Virtual Private Networks using IPSec and IKE**
   - "Platform to platform" encryption
   - IPSec implemented in IP layer as defined by policy
   - Auditing through SMF 119 records – tunnel level only
   - Completely transparent to application
   - Wide variety (any to all) of traffic is protected
   - Various topologies supported (host to host, host to gateway, etc.)
   - IKE negotiates IPSec tunnels dynamically

4. **Secure Shell using z/OS OpenSSH**
   - Mainly used for sftp on z/OS, but also offers secure terminal access and TCP port forwarding
   - Configured in ssh configuration file and on command line
   - Auditing via SMF 119 records
   - TCP only

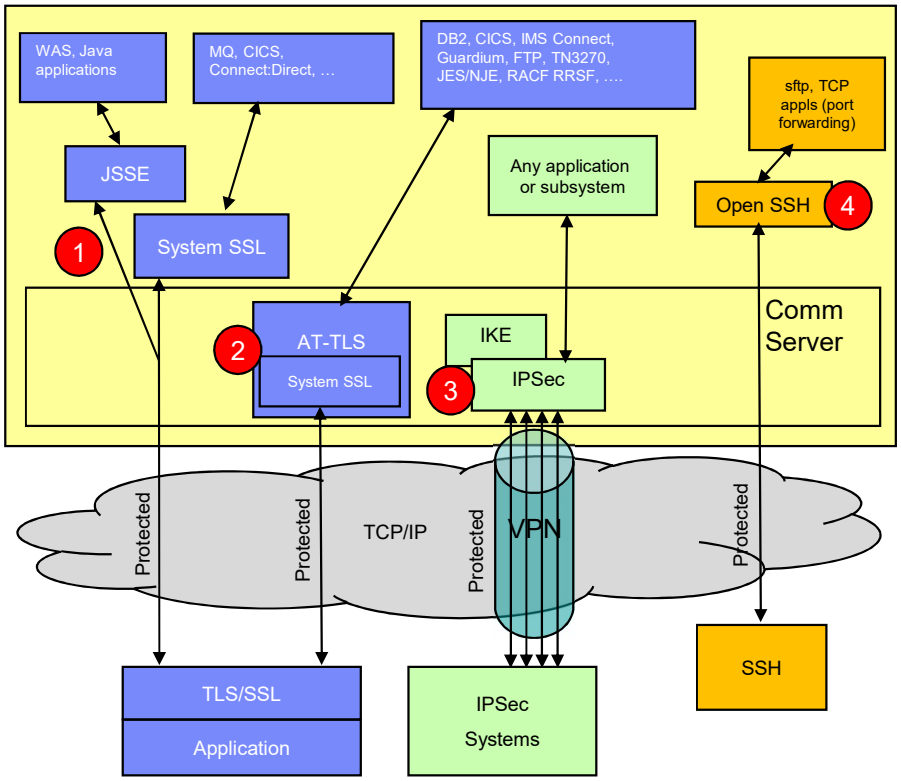


* - z/OS also provides Kerberos support, but that is not covered in this presentation

Background: …so which traffic do I have and how is it protected?

Given all these mechanisms, configuration methods and variation in audit detail…

- ***How can I tell…***
  - ***Which traffic*** is being protected (and which is not)?
  - ***How*** is that traffic being protected?
    - Security protocol?
    - Protocol version?
    - Cryptographic algorithms?
    - Key lengths?
    - …and so on
  - ***Who*** does on the traffic belong to in case I need to follow up with them?
- How can I ensure that new configurations adhere to my company's security policies?
- Once I've answered the above questions, how can I provide the information to my auditors or compliance officers?
- Many factors driving these questions:
  - Regulatory compliance (corporate, industry, government)
  - Vulnerabilities in protocols and algorithms
  - Internal audits
  - …and so on



Agenda

- Background – why zERT?
- **zERT overview**
- Configuring zERT
- Coming in 4Q2018: zERT Network Analyzer
- zERT support in other products
- Considerations
- Summary

Overview: z/OS Encryption Readiness Technology (zERT – 1 of 2)

- zERT positions the TCP/IP stack as a central collection point and repository for cryptographic protection attributes for:
  - **TCP** connections that are protected by **TLS, SSL, SSH, IPsec or** have **no recognized cryptographic protection**
  - **Enterprise Extender** connections that are protected by **IPsec or** have **no recognized cryptographic protection**
    - Each peer-to-peer UDP port is considered a separate EE connection
    - In this presentation, we'll focus on TCP examples
- Two methods for discovering the security sessions and their attributes:
  - Stream observation (for TLS, SSL and SSH) – the TCP/IP stack observes the protocol handshakes as they flow over the TCP connection
  - Advice of the cryptographic protocol provider (System SSL, OpenSSH, TCP/IP's IPsec support)
- Reported through new SMF 119 records via:
  - SMF and/or
  - New real-time NMI services

Overview: z/OS Encryption Readiness Technology (zERT – 2 of 2)

- zERT **Discovery – available in z/OS V2R3**
  - Attributes are collected and recorded at the connection level
  - SMF 119 subtype 11 “zERT Connection Detail” records
  - These records **describe the cryptographic protection history of each TCP and EE connection**
  - Writes **at least one zERT Connection Detail record for every TCP and EE connection**
  - Measures are in place to minimize the number of subtype 11 records, but they could still be very voluminous
- zERT **Aggregation – available via V2R3 new function APAR PI83362**
  - Attributes collected by zERT discovery are aggregated by security session
  - SMF 119 subtype 12 “zERT Summary” records
  - These records **describe the repeated use of security sessions over time**
  - Writes **one zERT Summary record at the end of each SMF for each security session that was used during that interval**
  - Aggregation can greatly reduce the volume of SMF records while maintaining the fidelity of the information – well suited for reporting applications
- zERT **Network Analyzer – coming in 4Q2018** (more on this in a few minutes)

Overview: Important terms

- *Cryptographic Protocol Provider (CPP):* A z/OS-resident component that processes a specific cryptographic network security protocol (i.e., TLS/SSL, IPSec or SSH).
  - IBM zERT-enabled CPPs:
    - System SSL, OpenSSH and IPSec
    - ZERTJSSE provider - shipped with IBM SDK, Java Technology Edition 8.0.0 Service Refresh 5, Fix Pack 25 – wraps the standard Java 8 JSSE
  - IBM non-zERT enabled CPPs: JSSE in any form other than ZERTJSSE
  - 3rd party non-zERT-enabled: Tectia SSH, OpenSSL, etc.

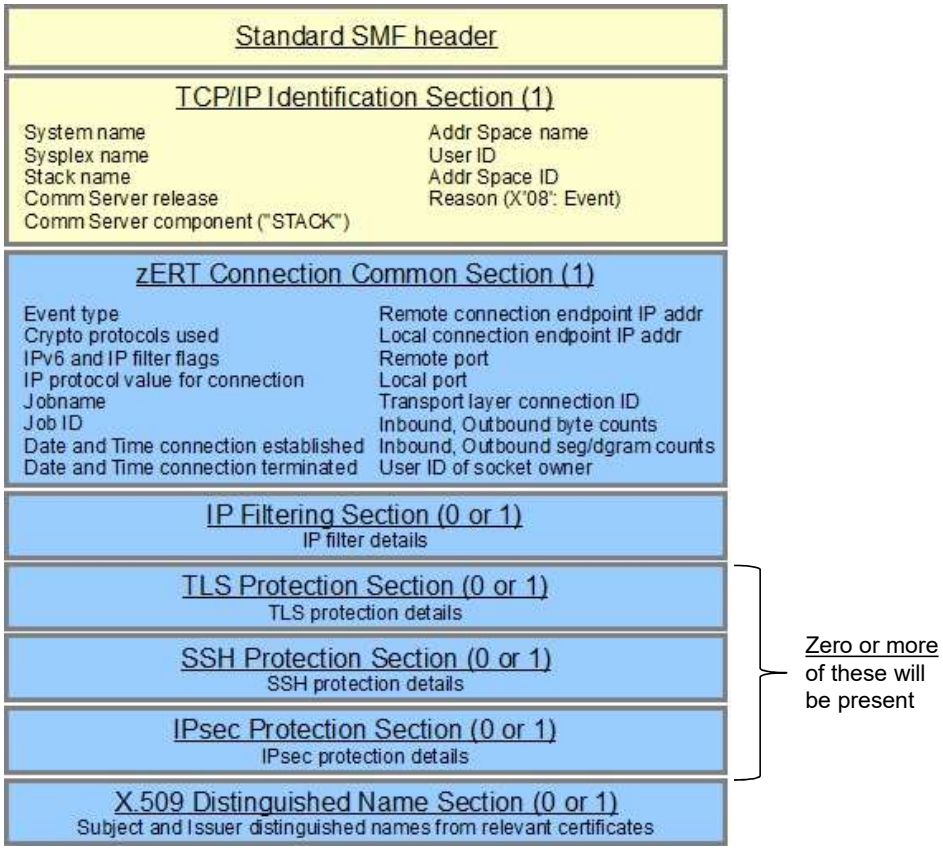
- *Protection state:* The cumulative state of cryptographic protection of a connection. There are numerous possible combinations here:
  - No cryptographic protection (connection is in cleartext mode)
  - Protection from a single cryptographic protocol (most common case)
  - Protection from multiple cryptographic protocols (for example, a TCP connection protected by both TLS and IPSec)
- *Application **connection**:* A sockets-based connection between two application programs. No security is implied or provided – just a cleartext path.
- *Security **session**:* The application (by a CPP) of an agreed-to set of security attributes (as defined by a cryptographic security protocol) to one or more application connections between the same client and server. Examples are TLS/SSL sessions, IPSec tunnels and SSH sessions.

Overview: zERT Discovery (1 of 2)

Written at various events in a TCP or EE connection's life:

- **Connection Initiation** (event type 1)
  - Describes protection state when connection was created (for TCP, state as established within the first 10 seconds of the connection's life)
  - Not usually written for short-lived TCP connections
- **Protection State Change** (event type 2)
  - Describes significant changes in protection state (security session added, deleted, or modified)
- **Connection Termination** (event type 3)
  - Describes protection state when connection terminated
  - Has an accompanying Connection Initiation record
- **Short Connection Termination** (event type 4)
  - Describes protection state when connection terminated
  - Written for short-lived TCP connections (less than 10 seconds long)

Also written when zERT is enabled (5) or disabled (6). Event type is the only zERT information in these records.



Overview: zERT Discovery (2 of 2)

What is collected and recorded?

- Attributes of the connection and its security sessions
  - **Significant attributes**
    - Identifying attributes like IP addresses, ports, jobname, userid, etc.
    - Protection attributes like protocol version, cryptographic algorithms, key lengths, etc. Changes in these cause a protection state change record to be written if they change
  - **Informational attributes** like protocol session identifiers, session or certificate expiry data and certificate serial numbers are recorded for informational purposes only. When recorded, the values of such attributes are taken at the time the SMF record is written. Changes in these attributes do not constitute a significant change and will not result in the creation of a change event record
- **zERT does not collect, store or record the values of secret keys, initialization vectors, or any other secret values that are negotiated or derived during cryptographic protocol handshakes**

See the z/OS Communications Server IP Programmer's Guide for all the details

Overview: zERT Aggregation (1 of 3)

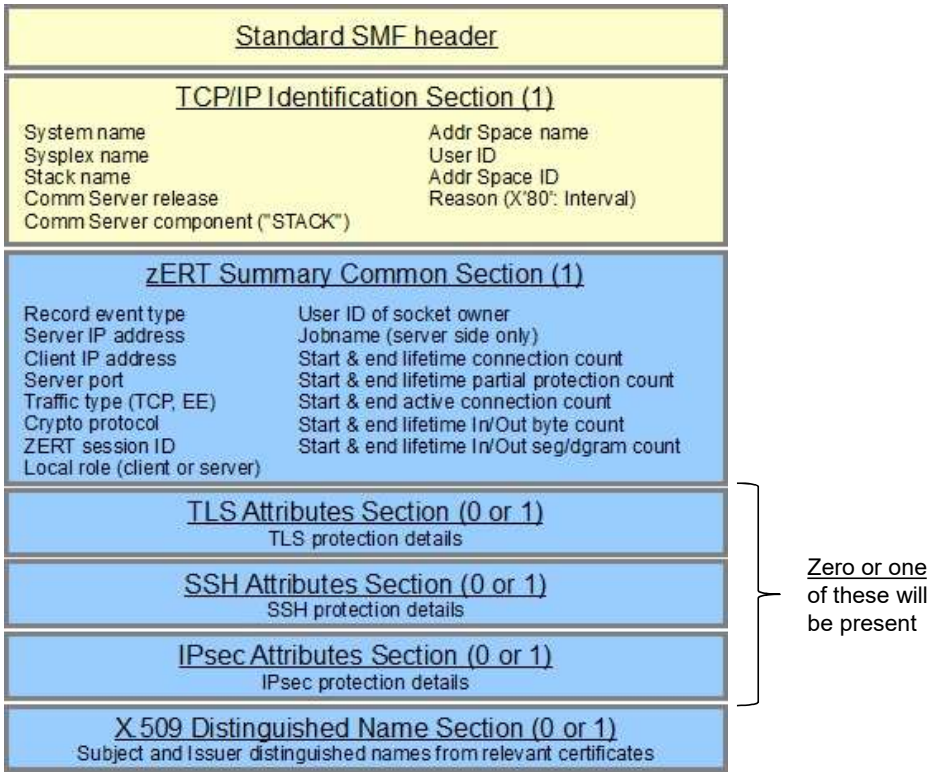
- Workloads that consist of large numbers of frequent short-lived connections could generate **huge volumes of zERT subtype 11 records**

- Consider an **example** where…
  - A local CICS region is serving 20 remote hosts, each connecting 1000 times per minute
  - SMF interval is set to 30 minutes
  - Each remote host uses the same IP address and TLS session attributes for each connection
- Would result in **at least 20,000 SMF 119 subtype 11 records per minute, or 600,000 per SMF interval** – at least one per connection

- Some measures are already taken in zERT Discovery to reduce the number (timers and "Short-lived Connection Termination" records), but these may be insufficient in environments that manage thousands of connections per hour or minute

Overview: zERT Aggregation (2 of 3)

- **zERT Aggregation summarizes the repetitive use of security sessions over time**
  - From the server's perspective (based on server IP address, server port, & client IP address)
  - Regardless of whether z/OS is the client or the server
- Summaries are written at the end of each SMF interval through new SMF 119 zERT summary (subtype 12) records which contain:
  - Connection attributes (Server IP addr, server port, client IP addr, transport protocol)
  - Significant security attributes
  - Statistics (connection counts, byte counts, etc.)
- With aggregation, **the same example scenario from the previous page would result in 20 SMF 119 subtype 12 records per interval** – one per client TLS session



Overview: zERT APIs (1 of 2)

Real-time network monitoring services

- **Used by 3rd party Network Monitor products to collect SMF data in near real-time**
- Two new Network Monitoring Interfaces (NMIs):
  - New SYSTCPER service for collecting zERT Connection Detail (subtype 11) SMF records
  - New SYSTCPES service for collecting zERT Summary (subtype 12) SMF records
- Both use the same programming model as existing SYSTCPCN (TCP connection) service
  - Clients connect to SYSTCPER/SYSTCPES service over an AF_UNIX socket
  - Access control via SAF: EZB.NETMGMT.sysname.tcpprocname.SYSTCPER or EZB.NETMGMT.sysname.tcpprocname.SYSTCPES
  - Newly-generated SMF records are written to the service in real time
  - Server sends sequence of token records, each of which describes a data buffer that contains requested SMF records
  - For each token record, client uses a built-in function to copy SMF data into own buffers

See the z/OS Communications Server IP Programmer's Guide for details

Overview: zERT APIs (2 of 2)

SIOCSHSNOTIFY IOCTL (for System SSL applications)

- For **System SSL application programs** that initiate TLS session **mid-stream**

- **Use this interface ONLY IF:**
  - **Your program calls the System SSL gsk_* APIs directly** for TLS/SSL protection (i.e., it is NOT protected by AT-TLS or another TLS/SSL provider like JSSE)
  - **TLS session is initiated after one or more bytes of application-specific data flow** over the TCP connection (this is not the typical case)

- Re-activates zERT stream observation immediately before a TLS/SSL handshake begins.
  - zERT stream observation is required for sessions created by System SSL
  - Stream observation automatically activated when a TCP connection is first established, but is disabled as quickly as possible
  - As such, handshakes that occur mid-stream will not be observed without an explicit notification from the program that's invoking System SSL APIs
  - Inbound and outbound buffers must be flushed before issuing this IOCTL
  - Note that AT-TLS internally provides the notification that zERT needs in the mid-stream handshake scenario.

IBM Sterling Connect:Direct relies on this interface.
Install Connect:Direct APAR PI77316 to ensure that C:D connections are properly monitored by zERT.

See the z/OS Communications Server IP Programmer's Guide for details and a coding example

Agenda

- Background – why zERT?
- zERT overview
- **Configuring zERT**
- Coming in 4Q2018: zERT Network Analyzer
- zERT support in other products
- Considerations
- Summary

Configuring: The steps

1. Enable SMF 119 records in SMF (PARMLIB)
2. Enable zERT in-memory monitoring (TCPIP profile)

```
GLOBALCONFIG ZERT [AGGRegation] | NOZERT
```

3. Specify recording destinations (TCPIP profile)

```
SMFCONFIG TYPE119 ZERTDetail | NOZERTDetail
SMFCONFIG TYPE119 ZERTSUMmary | NOZERTSUMmary
NETMONITOR ZERTService | NOZERTService
NETMONITOR ZERTSUMmary | NOZERTSUMmary
```

4. Verification (NETSTAT and DISPLAY TCPIP commands)

- Note that the discovery and aggregation in-memory functions are enabled independently of the destinations to which records are written.
- Profile parameters can be:
  - Dynamically enabled or disabled
  - Configured by hand or through the z/OSMF Network Configuration Assistant for z/OS Communications Server

Configuring: 4. Verifying zERT configuration

NETSTAT CONFIG or DISPLAY TCPIP,*tcpipprocname*,NET,CONFIG command shows current configuration:

```
*13.48.17 *IWM048E WLM RUNNING IN GOAL MODE WITH THE DEFAULT POLICY
*13.49.19 *$HASP190 VTAMAPPL SETUP - PRT1       - F=1185     - C=9    -
* T=PN
 SMF PARAMETERS:
 TYPE 119:
   TCPINIT:       NO    TCPTERM:       NO    FTPCLIENT:     NO
   TCPIPSTATS:    NO    IFSTATS:       YES   PORTSTATS:     NO
   STACK:         NO    UDPTERM:       NO    TN3270CLIENT:  NO
   IPSECURITY:    NO    PROFILE:       YES   DVIPA:         NO
   SMCRGRPSTATS:  NO    SMCRLNKEVENT:  NO
   SMCDLNKSTATS:  NO    SMCDLNKEVENT:  NO
   ZERTDETAIL:    YES   ZERTSUMMARY:   YES
 GLOBAL CONFIGURATION INFORMATION:
 TCPIPSTATS: NO    ECSALIMIT: 0000000K  POOLLIMIT: 0000000K
 MLSCHKTERM: NO    XCFGRPID:            IQDVLANID: 0
 SYSPLEXWLMPOLL: 060    MAXRECS:    100
 EXPLICITBINDPORTRANGE:  00000-00000   IQDMULTIWRITE:  NO
 AUTOIQDC: NO
 AUTOIQDX: ALLTRAFFIC                  ADJUSTDVIPAMSS: AUTO
 WLMPRIORITYQ: NO
00 SYSPLEX MONITOR:
   TIMERSECS: 0060  RECOVERY: NO   DELAYJOIN: NO   AUTOREJOIN: NO
   MONINTF:   NO    DYNROUTE: NO   JOIN:      YES
 ZIIP:
   IPSECURITY: NO   IQDIOMULTIWRITE: NO
 SMCGLOBAL:
   AUTOCACHE:  YES  AUTOSMC:  YES
 SMCR: NO
 SMCD: NO
 ZERT: YES
   AGGREGATION: YES
 NETWORK MONITOR CONFIGURATION INFORMATION:
 PKTTRCSRV: NO    TCPCNNSRV: NO    NTASRV: NO
 SMFSRV:    NO
 ZERTSRV:   NO
 ZERTSUM:   NO
 END OF THE REPORT

IEE612I CN=VS050A    DEVNUM=0009 SYS=MVS050
-
IEE163I MODE= RD
```

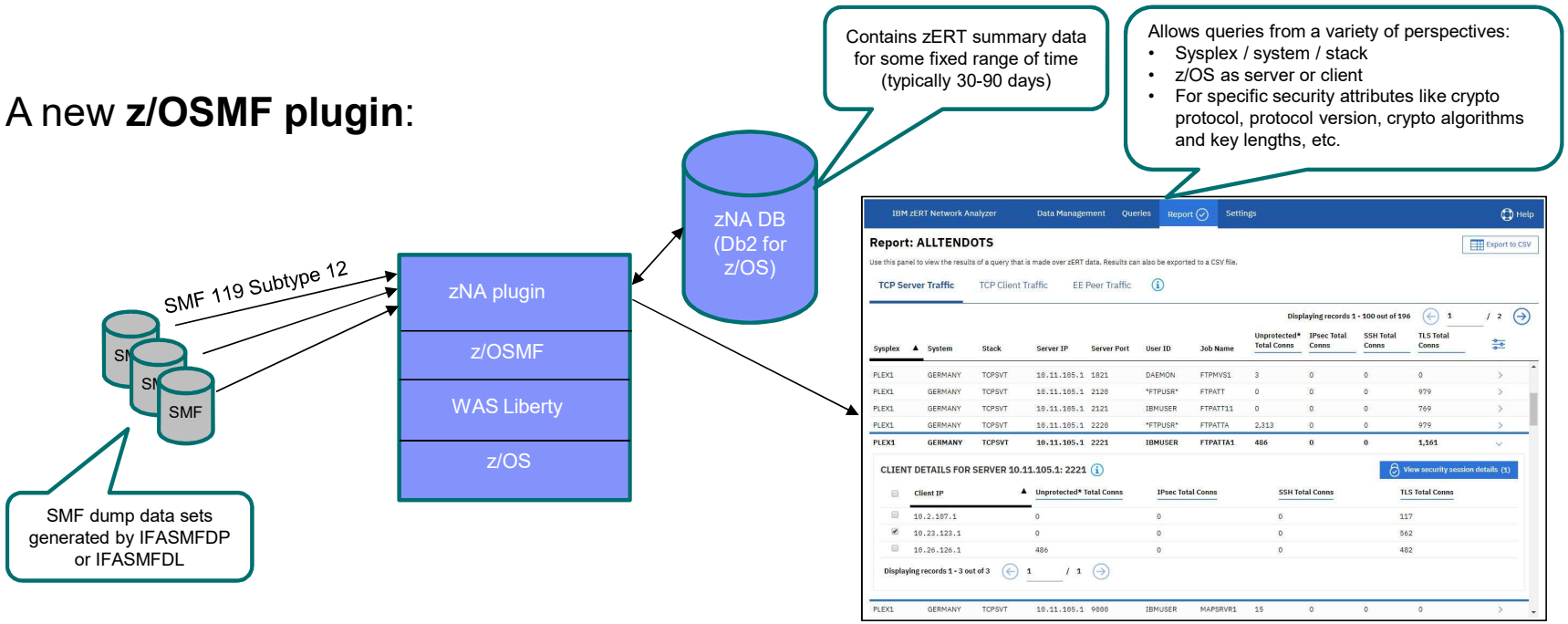
Agenda

- Background – why zERT?
- zERT overview
- Configuring zERT
- **Coming in 4Q2018: zERT Network Analyzer**
- zERT support in other products
- Considerations
- Summary

zERT Network Analyzer Overview

New!

- A new **z/OSMF plugin**:



- **Web UI** makes zERT data consumable for **z/OS network security administrators** (typically systems programmers)
- Used primarily to investigate specific network encryption questions (but could also be used for periodic report generation)
- The **IBM zERT Network Analyzer will be shipped in 4Q2018 via new function APAR PH03137** (announced in the November 13, 2018 IBM z/OS Version 2 Release 3 enhancements and statements of direction)

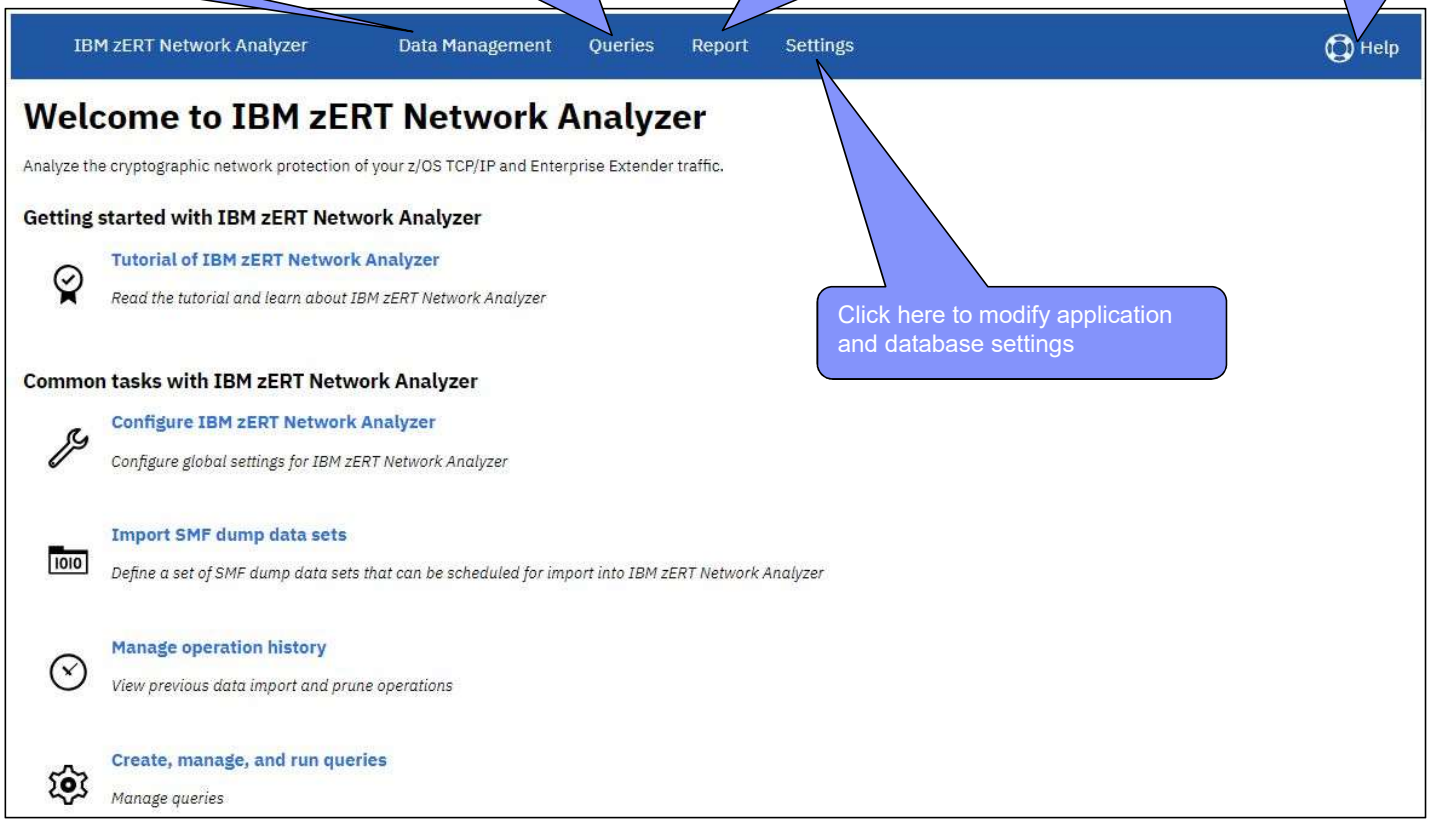
zERT Network Analyzer Overview: Sneak peek: Welcome page and layout

Click here to import SMF dump data sets and to prune old data out of the database

Click here to create, modify, and run queries over the imported data

Click here to view the query results (more on this in the following slides)

Click here for topical help in the IBM Knowledge Center



Click here to modify application and database settings

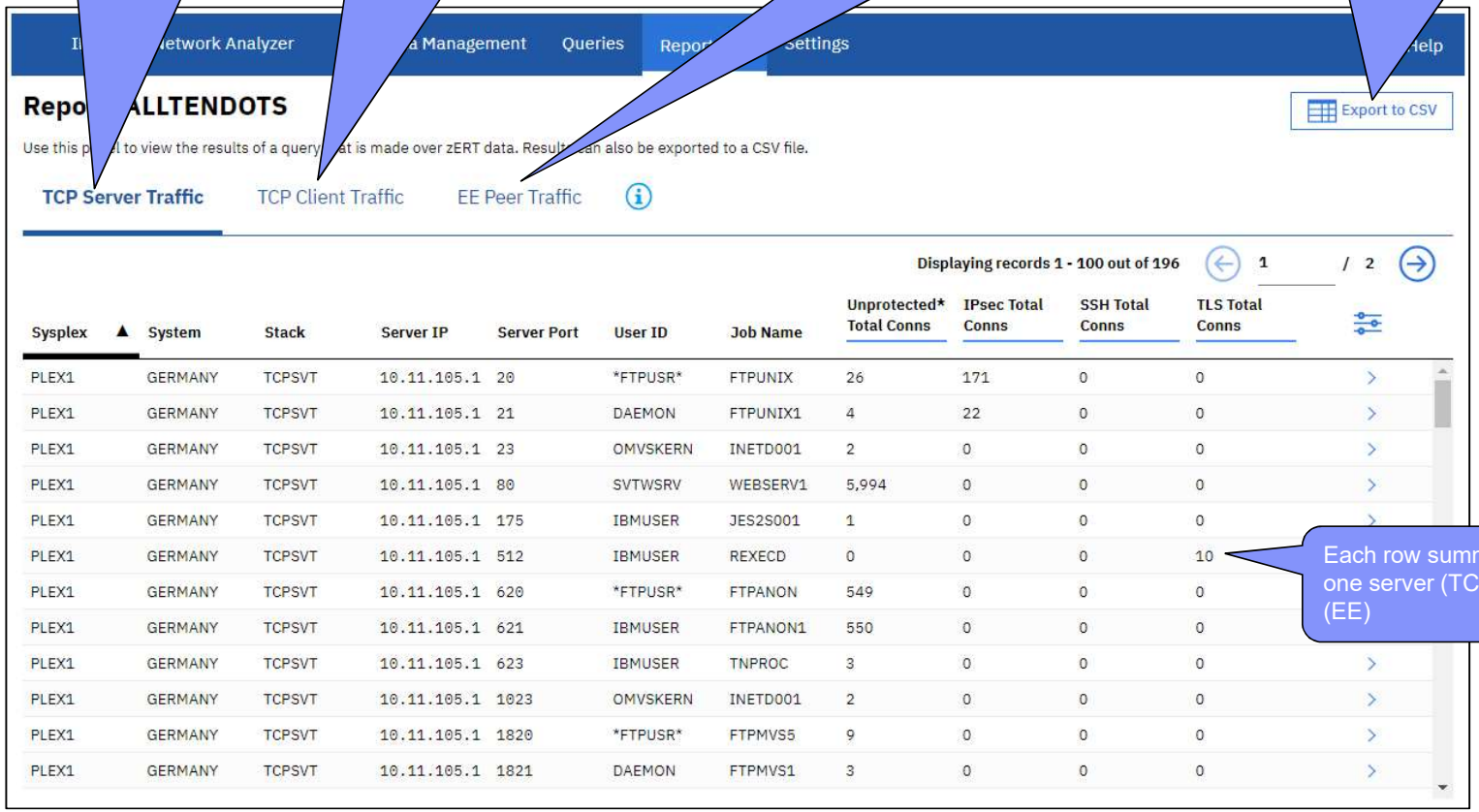
zERT Network Analyzer Overview: Sneak peek: Report summary view (1 of 2)

TCP Server Traffic: Summary of all the traffic connecting in to servers running on local z/OS systems

TCP Client Traffic: Summary of all the traffic connecting out to servers running on other systems

EE Peer Traffic: Summary of all EE traffic connected to local z/OS systems

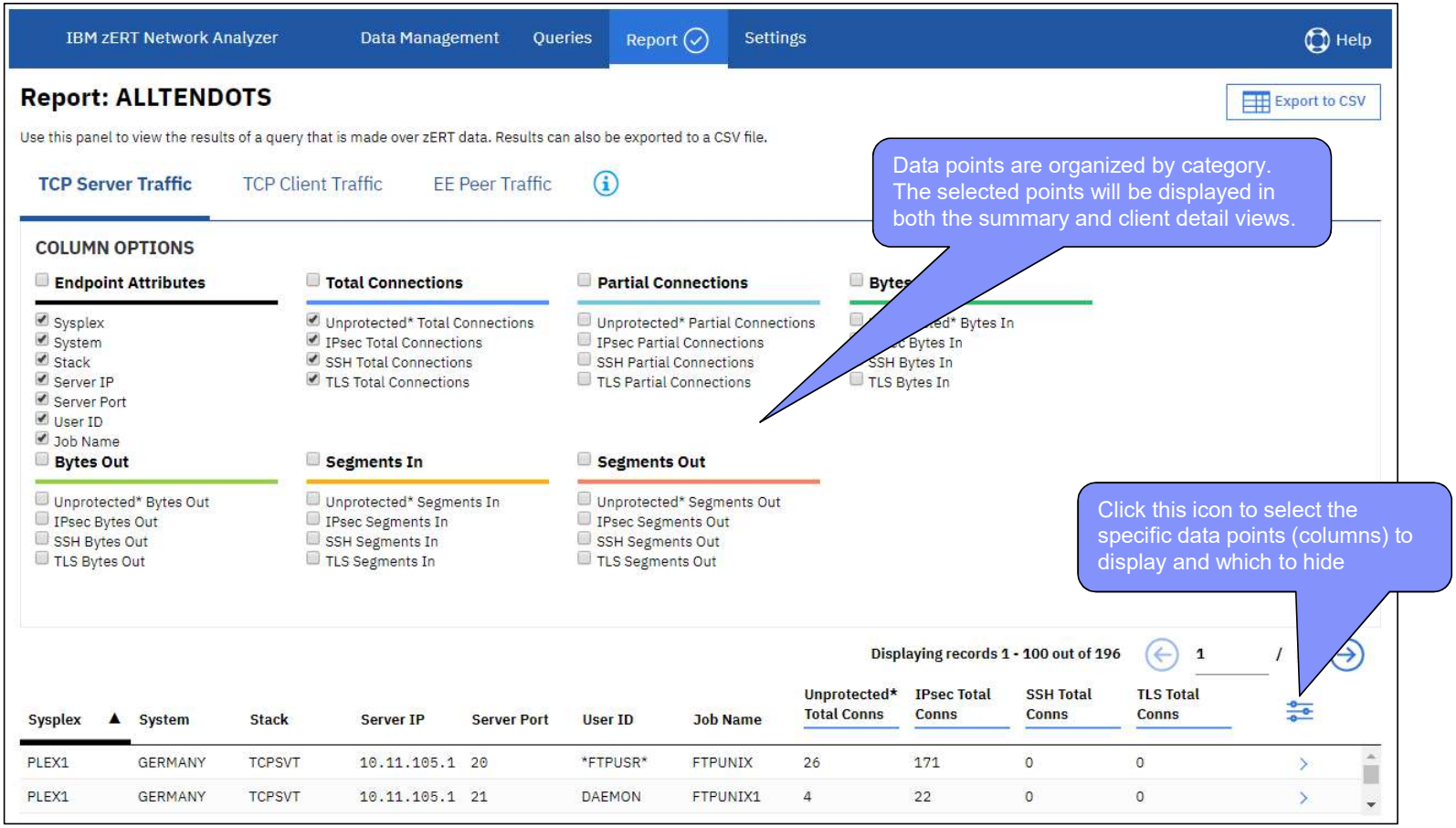
Exports the query results and all related details to a comma separated value file



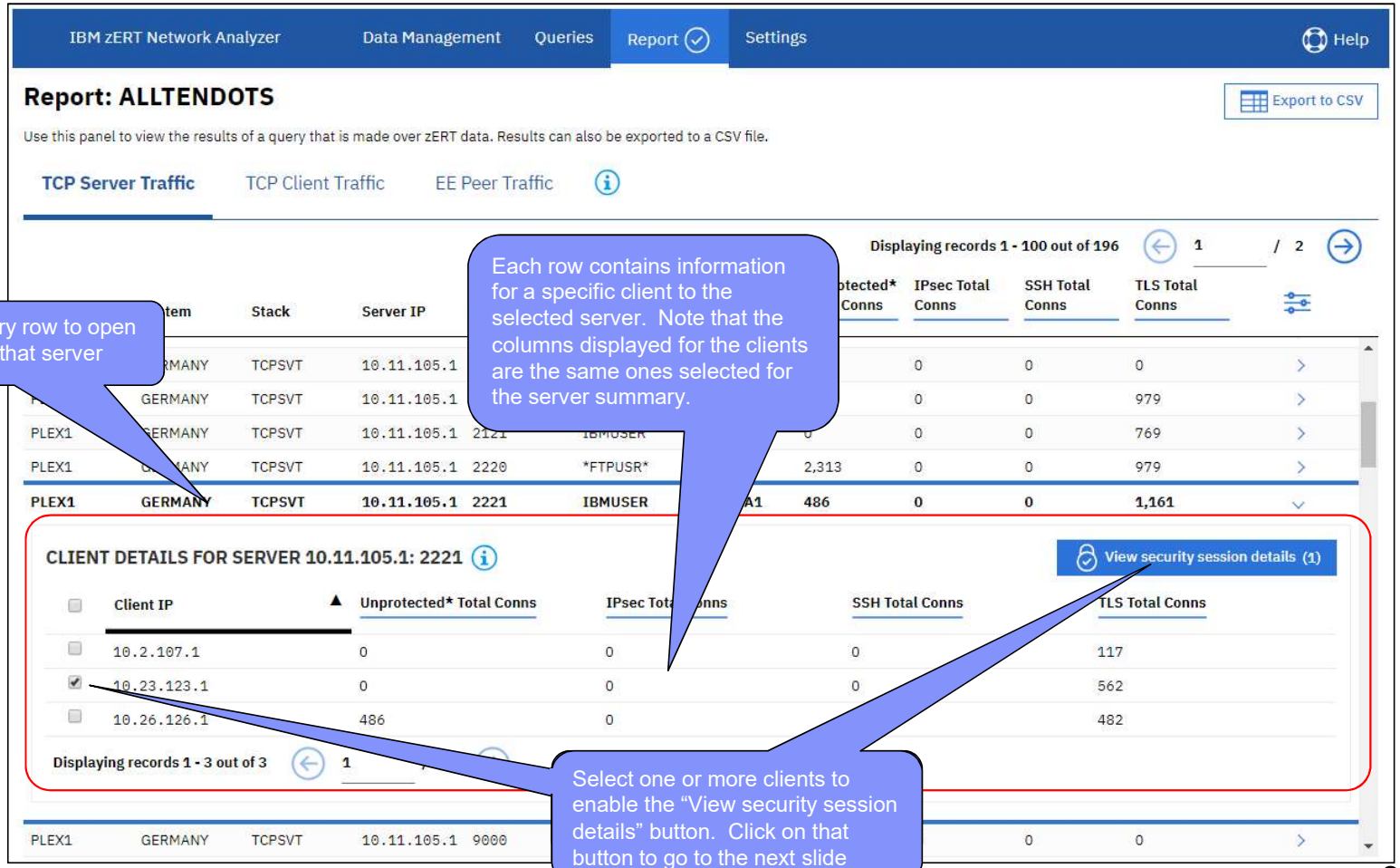
Sysplex	System	Stack	Server IP	Server Port	User ID	Job Name	Unprotected* Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
PLEX1	GERMANY	TCPSVT	10.11.105.1	20	*FTPUSR*	FTPUNIX	26	171	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	21	DAEMON	FTPUNIX1	4	22	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	23	OMVSKERN	INETD001	2	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	80	SVTWSRV	WEBSERV1	5,994	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	175	IBMUSER	JES2S001	1	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	512	IBMUSER	REXECD	0	0	0	10
PLEX1	GERMANY	TCPSVT	10.11.105.1	620	*FTPUSR*	FTPANON	549	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	621	IBMUSER	FTPANON1	550	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	623	IBMUSER	TNPROC	3	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	1023	OMVSKERN	INETD001	2	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	1820	*FTPUSR*	FTPMVS5	9	0	0	0
PLEX1	GERMANY	TCPSVT	10.11.105.1	1821	DAEMON	FTPMVS1	3	0	0	0

Each row summarizes traffic for one server (TCP) or local peer (EE)

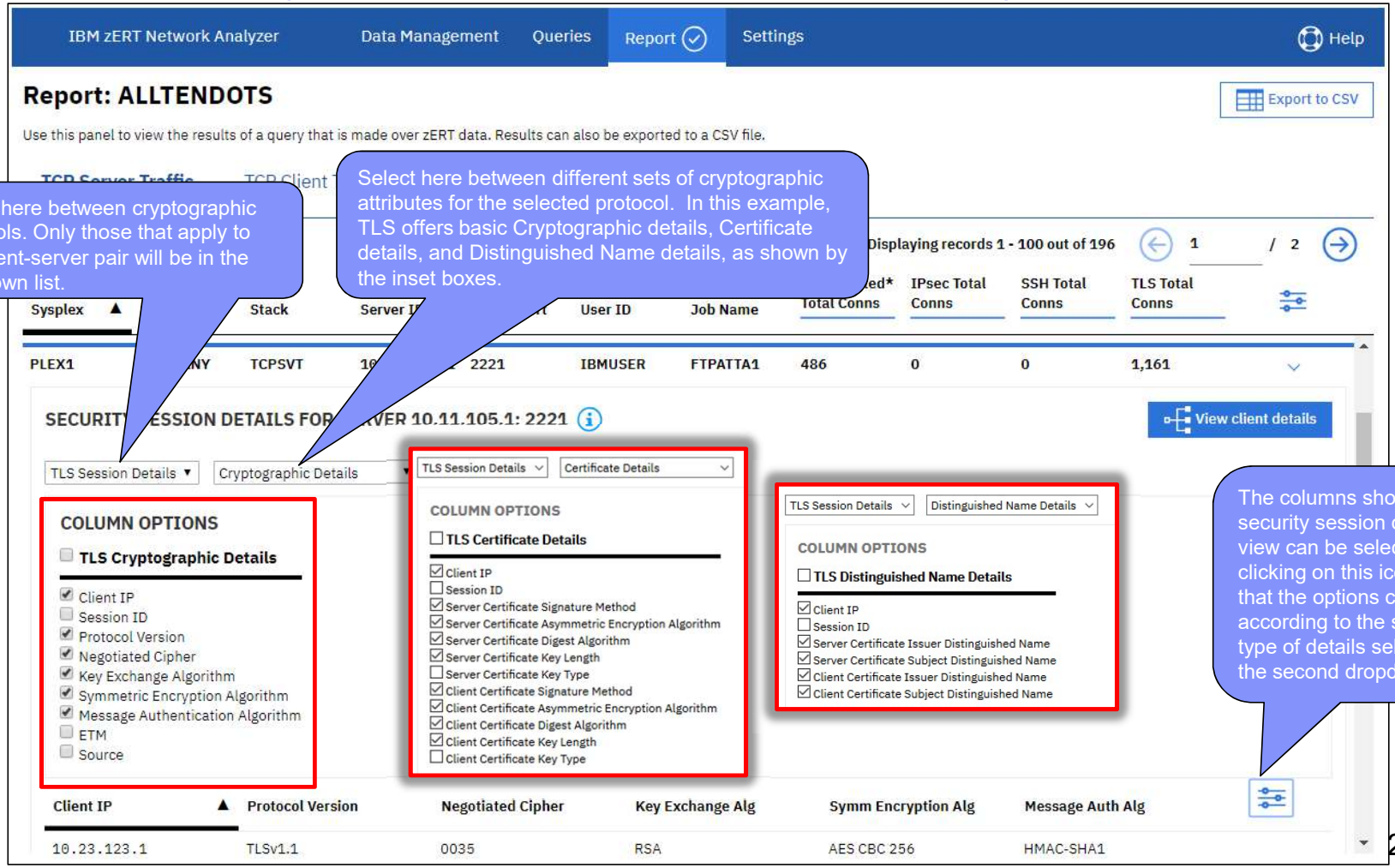
zERT Network Analyzer Overview: Sneak peek: Report summary view (2 of 2)



zERT Network Analyzer Overview: Sneak peek: Client detail view for a given server



zERT Network Analyzer Overview: Sneak peek: Security session details view

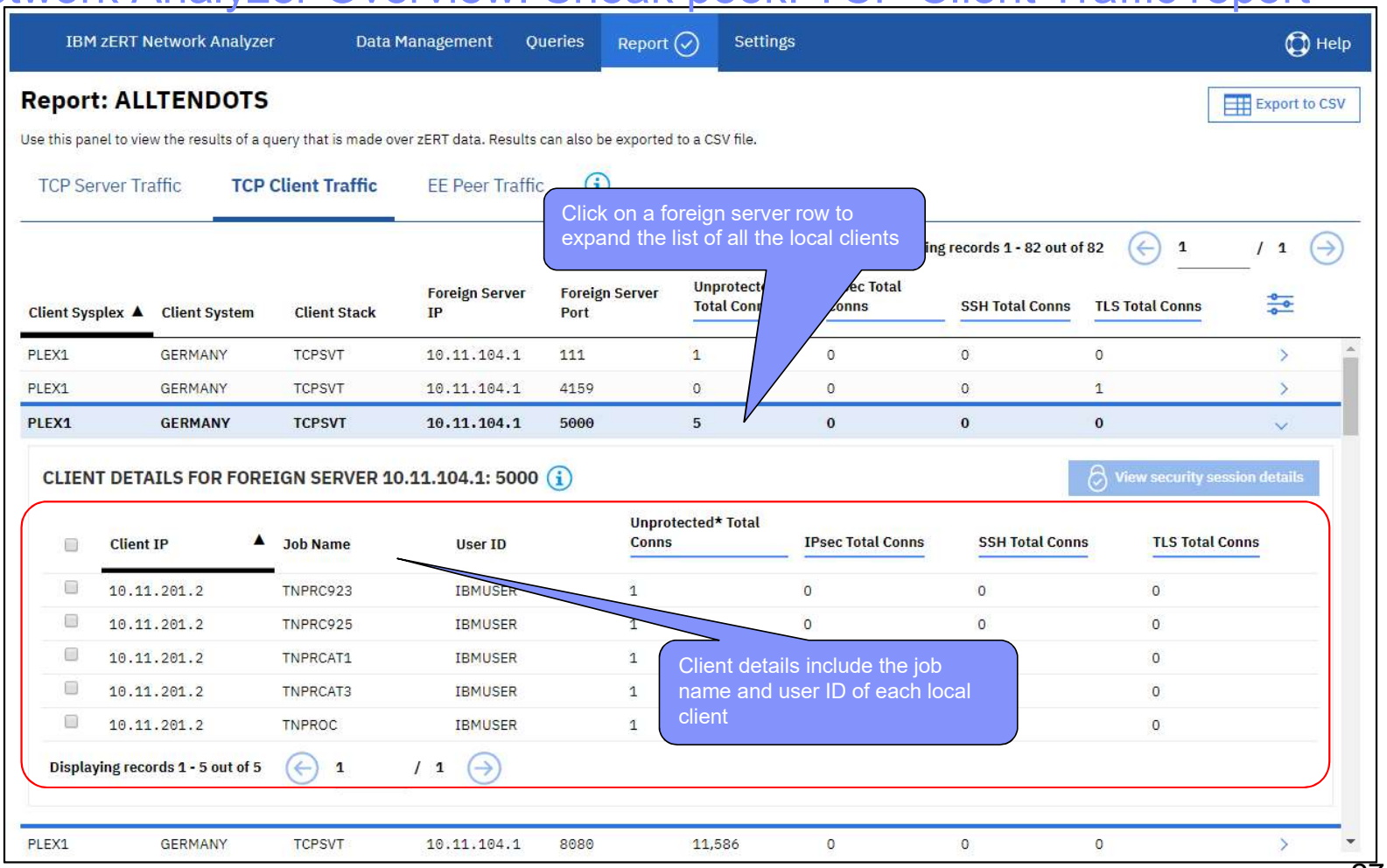


Select here between cryptographic protocols. Only those that apply to this client-server pair will be in the dropdown list.

Select here between different sets of cryptographic attributes for the selected protocol. In this example, TLS offers basic Cryptographic details, Certificate details, and Distinguished Name details, as shown by the inset boxes.

The columns shown in the security session details view can be selected by clicking on this icon. Note that the options change according to the specific type of details selected in the second dropdown.

zERT Network Analyzer Overview: Sneak peek: TCP Client Traffic report



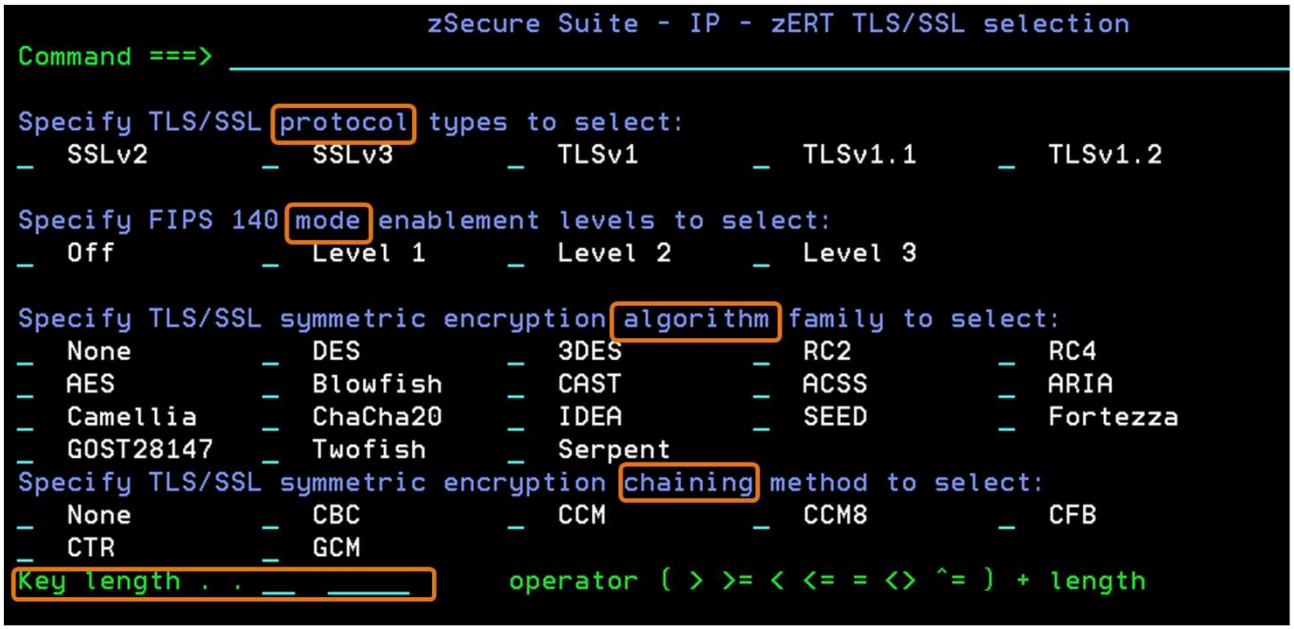
Agenda

- Background – why zERT?
- zERT overview
- Configuring zERT
- Coming in 4Q2018: zERT Network Analyzer
- **zERT support in other products**
- Considerations
- Summary

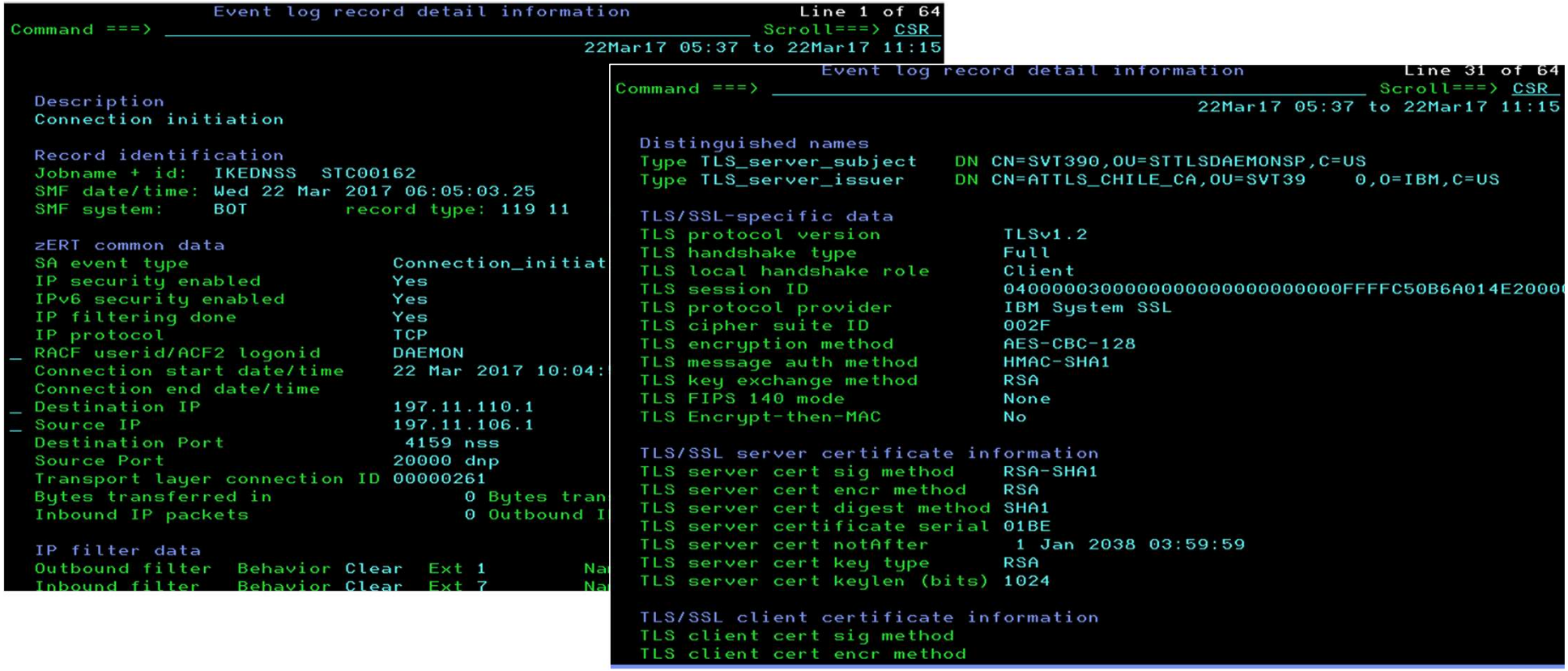
Overview: zSecure Audit V2.3 support for zERT (1 of 3)

Supports subtype 11 records in two ways:

- Ability to pass records to SIEM like QRadar in near real-time
- Event reporting (adds 118 new fields) Example:



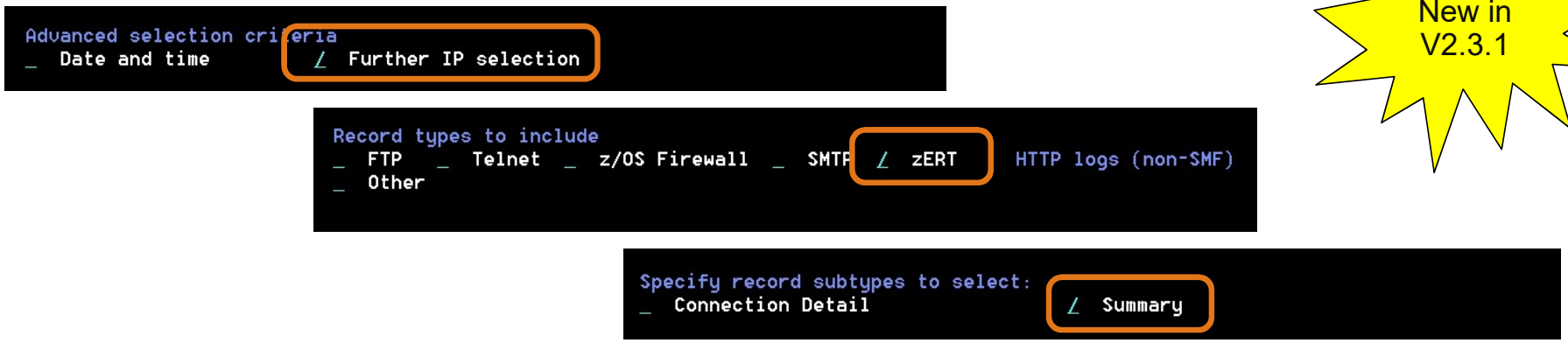
Overview: zSecure Audit V2.3 support for zERT (2 of 3)



Overview: zSecure Audit V2.3 support for zERT (3 of 3)

- Support for SMF 119-12 connection encryption summary records
  - Populates 76 existing fields same as 119-11 for zERTcommon, TLS, SSH, IPsec, and DN sections
  - 17 new fields added
    SUMMARY_INTERVAL, LOCAL_SOCKET_CLIENT, LOCAL_SOCKET, EE_SESSION, OUTBOUND_FTP_IPV4
    LOCAL_AT_TLS_BYPASS, SERVER_BEGIN_PORT, SERVER_END_PORT, SA_SESSION_ID, SA_CONNECTION_CNT_BEG,
    SA_CONNECTION_CNT_END, SA_PARTIAL_CONN_CNT_BEG, SA_PARTIAL_CONN_CNT_END, SA_SHORT_CONN_CNT_BEG,
    SA_SHORT_CONN_CNT_END, SA_ACTIVE_CONN_CNT_BEG, SA_ACTIVE_CONN_CNT_END

- ISPF User interface EV.I



New in V2.3.1

Other products with zERT support (as of today)

The following products have shipped new support for zERT data:

- IBM zSecure Audit V2.3 (supports subtype 11 and subtype 12 records)
- IBM QRadar SIEM (supports what zSecure feeds it)
- Merrill Technologies MXG (feeds subtype 11 and subtype 12 records into SAS)
- CA Technologies NetMaster Network Management for TCP/IP 12.2.03 (supports subtype 11 records through NMI)
- BMC Mainview for IP 3.6 (supports subtype 11 and subtype 12 records through NMI)
- We hope this list continues to grow…

Agenda

- Background – why zERT?
- zERT overview
- Configuring zERT
- Coming in 4Q2018: zERT Network Analyzer
- zERT support in other products
- **Considerations**
- **Summary**

Considerations (1 of 2)

- **zERT can generate very large volumes of subtype 11 records, depending on the number of connections supported by your z/OS system.**
  - **Please plan accordingly**
  - **Consider only capturing subtype 12 records on a regular basis and only capture subtype 11s for limited times when investigating specific traffic.**
- zERT monitors TCP and Enterprise Extender traffic. All other IP protocols are unmonitored.
- zERT monitors traffic that terminates at the local TCP/IP stack. It does not monitor routed traffic
- **zERT does not store or record the values of secret keys, initialization vectors, or any other secret values that are negotiated or derived during cryptographic protocol handshakes.**
- Regardless of the prior point, the zERT data that is recorded provides a fairly complete picture of the z/OS system's network cryptographic protection profile. As such, you should take appropriate steps to **protect the recorded SMF data as well as access to the zERT real-time network monitoring services.**

Considerations (2 of 2)

- zERT only monitors connections that are established after zERT is enabled (or re-enabled).
  - If you disable and later re-enable zERT, it will no longer monitor any of the connections that existed before re-enabling.
  - To ensure the most complete monitoring, enable zERT in your TCP/IP profile
- TCP traffic protected by other TLS/SSL implementations (JSSE, OpenSSL, other SSH, etc.) will only be reported through stream observation. Limitations:
  - Only reports initial handshake as long as it is the first thing to flow over the connection. zERT stream observation has no visibility to rehandshakes or early termination of security sessions
  - zERT has no visibility to attributes that are negotiated during the initial handshake using encrypted messages
- There are a small number of System SSL applications that cannot be monitored and are therefore reported as being unprotected. These are applications that:
  - Send or receive application-specific data before initiating the TLS/SSL session
  - Do not use the SIOCSHSNOTIFY ioctl
- In certain mixed-release environments, some IPSec-related attributes will not be available for reporting

Summary: Customer value

- zERT SMF 119 Connection Detail (subtype 11) records:
  - Provide ample opportunity for correlation to records (SMF or otherwise) from other applications, workloads and devices to help build an larger picture of individual network connections to z/OS
  - Can reveal traffic that is being double-protected
  - Can be used to verify use of refreshed digital certificates (when zERT-enabled CPPs are used)
- zERT SMF 119 Summary (subtype 12) records:
  - Provide the same level of cryptographic detail in a condensed format, typically with a great reduction in the volume of SMF records vs. Connection Detail records
- Several network monitoring and audit-related products now support zERT data – some of them providing near real-time views based on Connection Detail records
- The zERT Network Analyzer (coming in 4Q2018):
  - Makes it much easier for z/OS network security admins to consume, query and search zERT data
  - Great flexibility in creating queries that zero in on the specific systems, endpoints, time spans, and security attributes of interest. These queries can be built for regular compliance checks or for special purpose investigations
  - Query results can be viewed through a browser or exported to a CSV file for post-processing

For more information

URL	Content
http://tinyurl.com/zoscsblog	IBM Communications Server blog 
https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.cs3/cs3.htm	IBM Communications Server library 

Thank you!

Notices and disclaimers (1 of 2)

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts.
In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those

customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers (2 of 2)

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

.