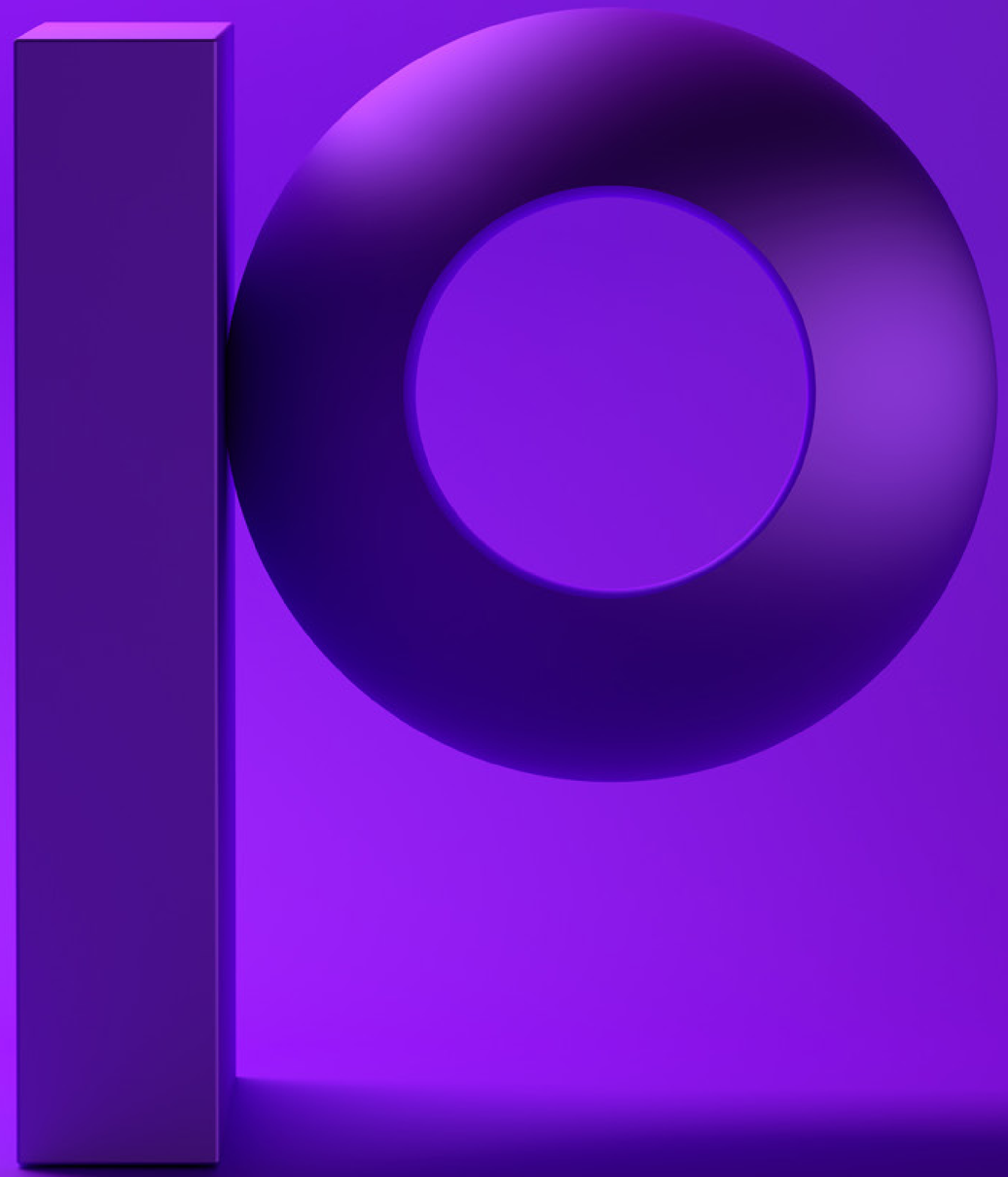
precisely

Managing the Top 5 Mainframe Security Vulnerabilities with Splunk Dashboards



Introduction

For a long time the IBM z/OS mainframe platform has been viewed as “inherently” secure, implying that the platform is secure by virtue of its foundational design. This myth has led many mainframe organizations to believe that hardly anything needs to be done to augment the platform to keep it secure. The assumption that the mainframe is “bulletproof,” combined with the slow but steady decline in mainframe-specific security expertise, has resulted in mainframe security being taken for granted in many organizations.

However, the rise in data and security breaches worldwide has forced C-level executives to stand up and take notice. The risk of non-compliance with the growing mass of governmental regulations and industry standards is causing loss of sleep as the C-suite faces more rigorous levels of responsibility for the integrity of enterprise data than did its predecessors. Potential penalties for failure of oversight are greater – fines and potentially jail sentences, not to mention the damage to the corporate brand when a breach becomes public.

In this eBook we will examine some of the risks and threats to mainframe security along with the data sources that can be leveraged to help address the threats and contain the risks.

A Brief Overview of Mainframe Security Solutions

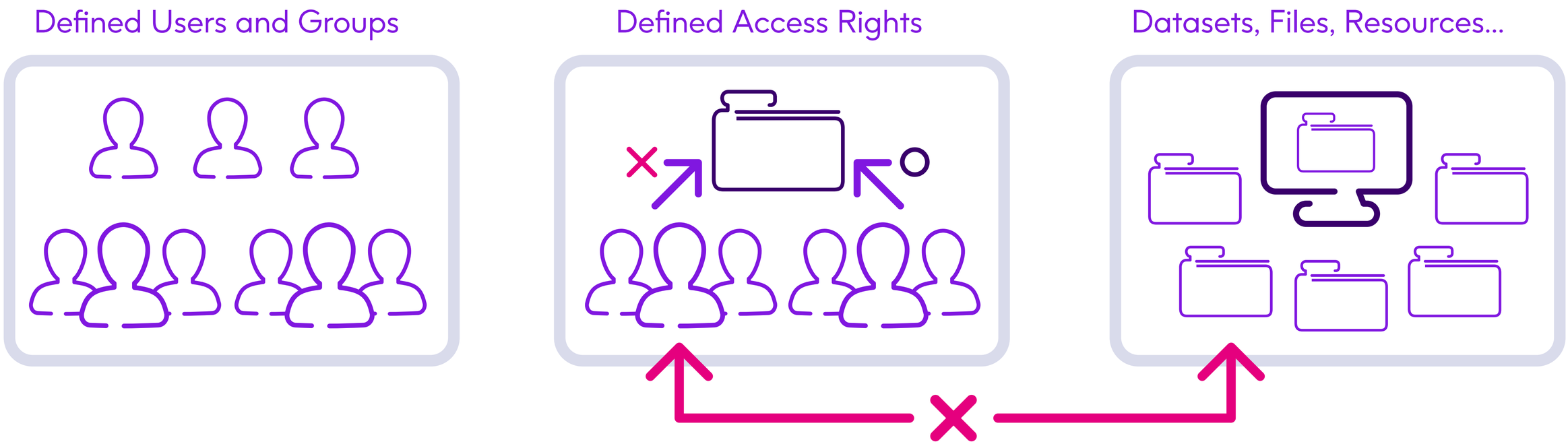
There are three primary security solutions that exist in the IBM z/OS mainframe environment: IBM Resource Access Control Facility (RACF), CA ACF/2, and CA Top Secret. All are similar in scope providing controls over what can be done within z/OS by protecting defined resources. Security is provided by:

1. Identifying and verifying users
2. Authorizing users to access protected resources
3. Recording and reporting access attempts

All require a security administrator to define resources, users, user groups, and the access rights to resources as well as access levels of individual users and groups. When access is attempted for a resource, the security system of choice is invoked to make a determination as to whether the user attempting access has rights to the resource. The security system either allows or denies the access, and records a security event for the access attempt.

Fundamentally the system works well provided that things are defined correctly and calls to the security package are made appropriately.

A Brief Overview of Mainframe Security Solutions

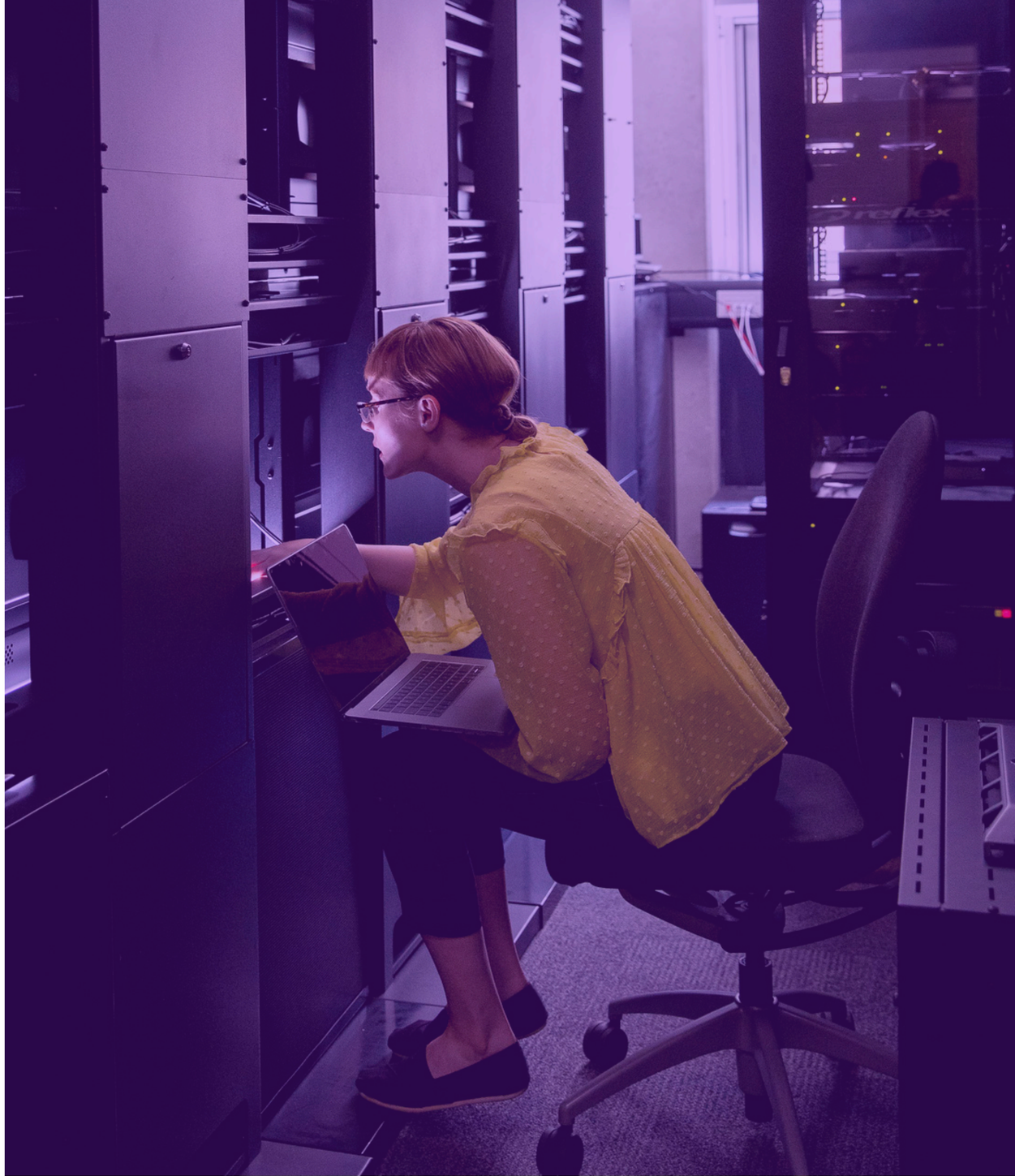


Splunk Enterprise Security Meets the Mainframe

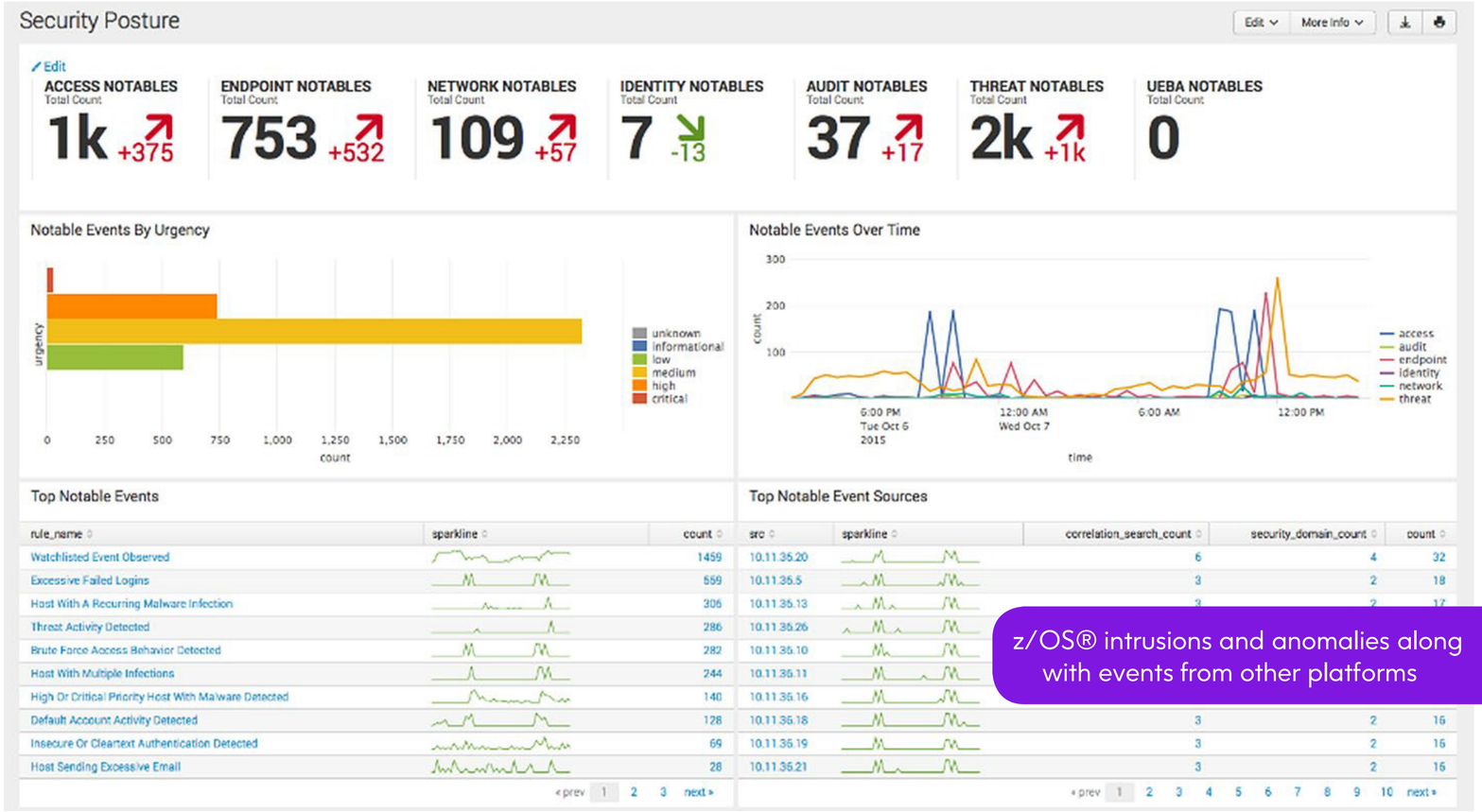
The Splunk® Enterprise data integration and indexing platform brings together machine data from all of an organization's IT systems, regardless of the nature of the operating systems or of any other platform-specific characteristics. Splunk Enterprise Security (ES) is a SIEM solution that allows you to gather all the context you need in one view to perform rapid security investigations and respond to them as soon as possible. The Splunk ES application provides insights into all manner of potential threat indicators generated by networks and endpoints across the enterprise. It delivers those insights through alerts, reports, and visualizations, including dozens of customizable dashboards. It streamlines all aspects of security operations and is suitable as the basis of a security operations center for organizations of all sizes and levels of expertise.

Mainframe customers needing to integrate their security information into Splunk ES need an additional solution to forward the important machine data from the mainframe to the Splunk installation. Precisely's Ironstream™ software for Splunk normalizes and streams z/OS log data (i.e., Syslog, SyslogD, SMF, RMF, Log4j, SYSOUT) as well as z/OS security information and maps it to the Splunk ES Common Information Model (CIM). This enables Splunk ES to provide a true enterprisewide view of security activity, threats, and intrusions.

The next section will highlight how the flexible dashboards in Spunk can be used to visualize and analyze the mainframe data to address the top mainframe security vulnerabilities.



Splunk Enterprise Security Meets the Mainframe



z/OS® intrusions and anomalies along with events from other platforms

Splunk Enterprise Security Meets the Mainframe

Managing the security issues for mainframe environments can be complex and challenging. There are many potential threats and vulnerabilities that a security adminstrator needs to consider. Let' take a look at the top five security issues for today's mainframe and how utilizing Splunk dashboards can provide critical help with monitoring and visualizing these security issues.

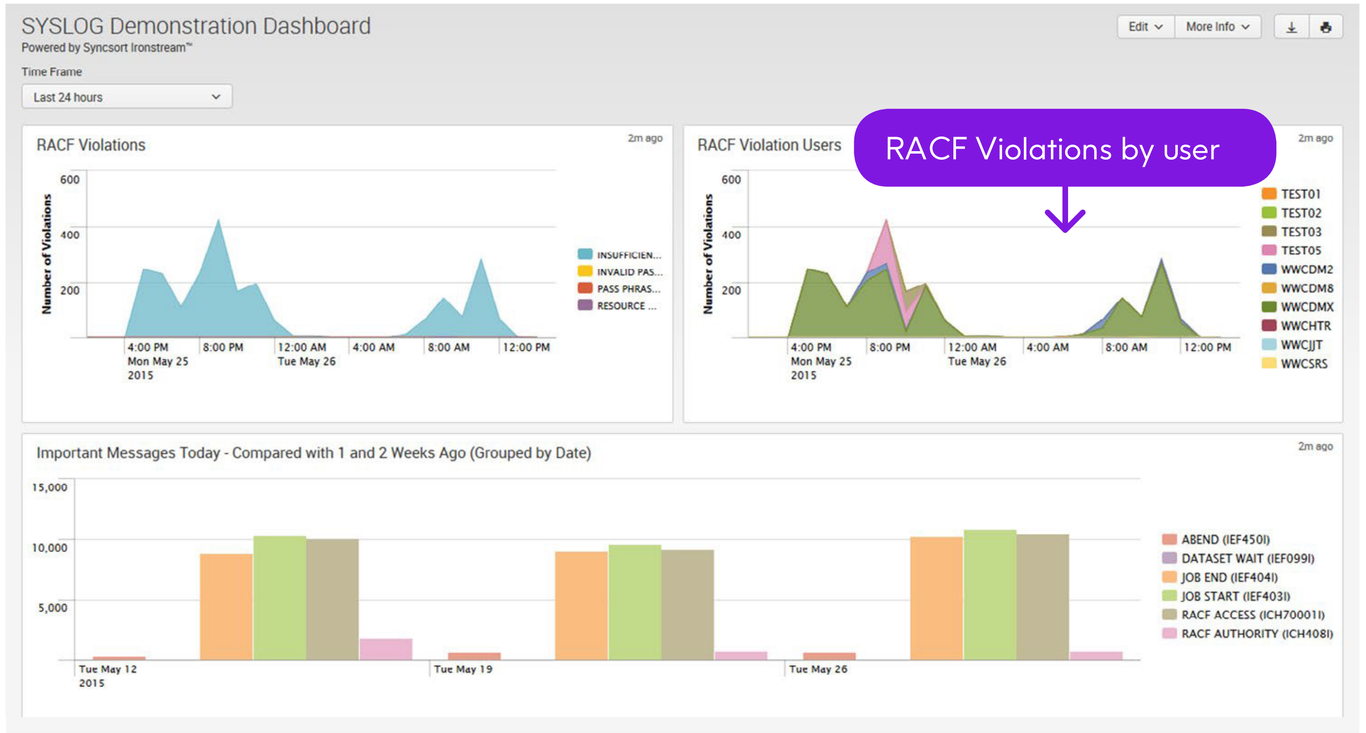
1. Weak Access Controls and Security Administration

As mentioned earlier, the security system works well provided that everything is defined correctly – resources, users, access rights, etc. Expertise in security administration is needed to setup resources, users, groups, and access rights correctly. It's no secret that we have experienced a decline in mainframe expertise over the past few years as an aging workforce continues to retire and be replaced by a new generation of technologists with less mainframe subject matter expertise.

Splunk Enterprise Security Meets the Mainframe

2. User IDs

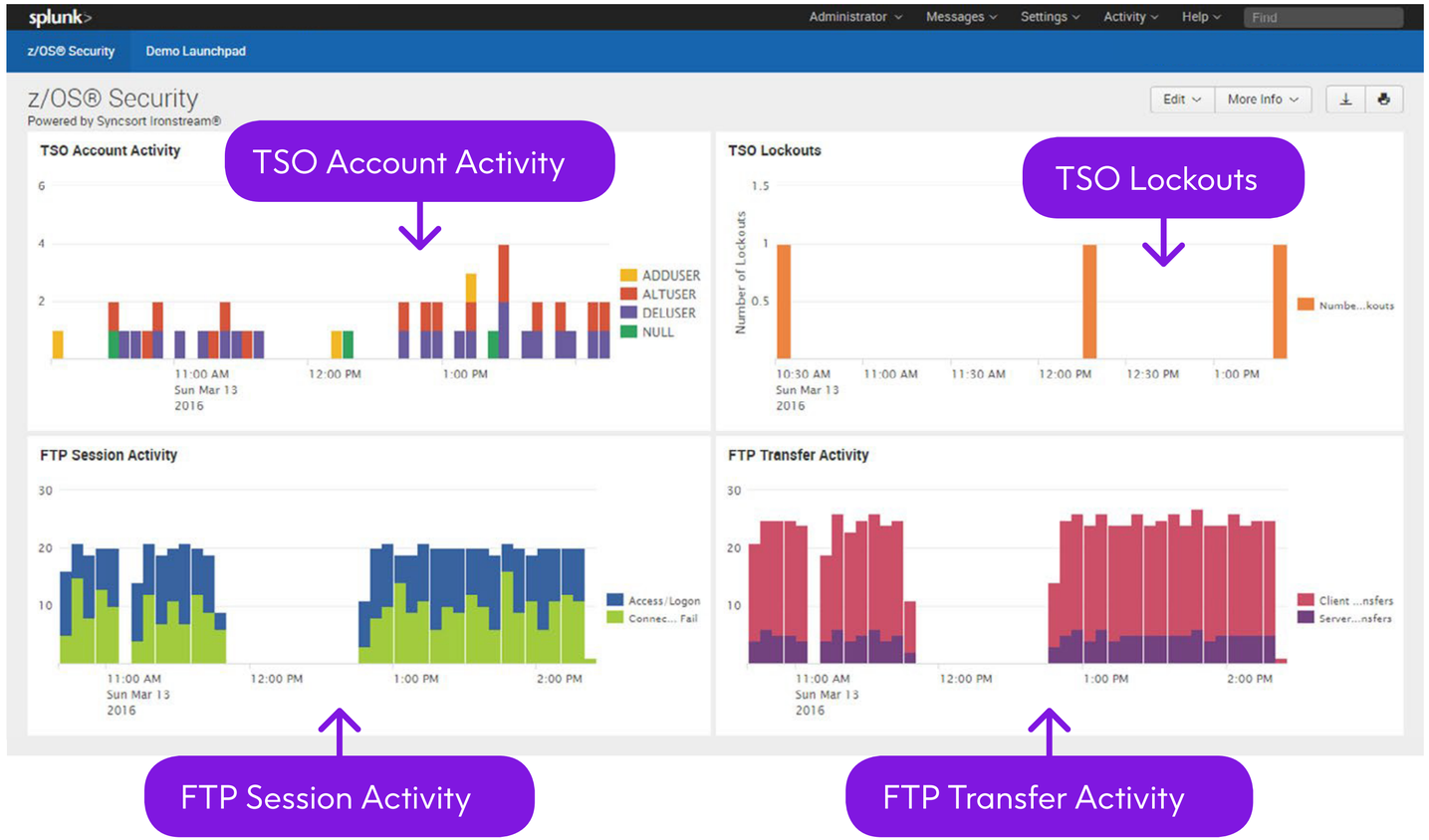
Incorrect definition of users including no password expiration for a defined user, incorrect or too high of a security privilege, along with weak passwords or default passwords that go unchanged due to no expiration, all create risk within the mainframe environment. It opens up a window or door for threat. Studies indicate 1/3 of all data breaches have been attributed to insiders within an organization. This might include employees, contractors, vendors, business partners, or others who have been granted access to resources within the organization. In a lot of cases, it is simply poor security administration resulting in unwarranted access that can be detected and resolved within an audit. However, in some cases an employee who has privileged access might simply neglect basic security precautions mandated by the organization. In worse scenarios a disgruntled or misguided ex-employee that still has credentials could pose a real threat,or employees simply get duped by an outsider phising for credentials to get at valuable data.



Splunk Enterprise Security Meets the Mainframe

3. Dataset and Resource Access

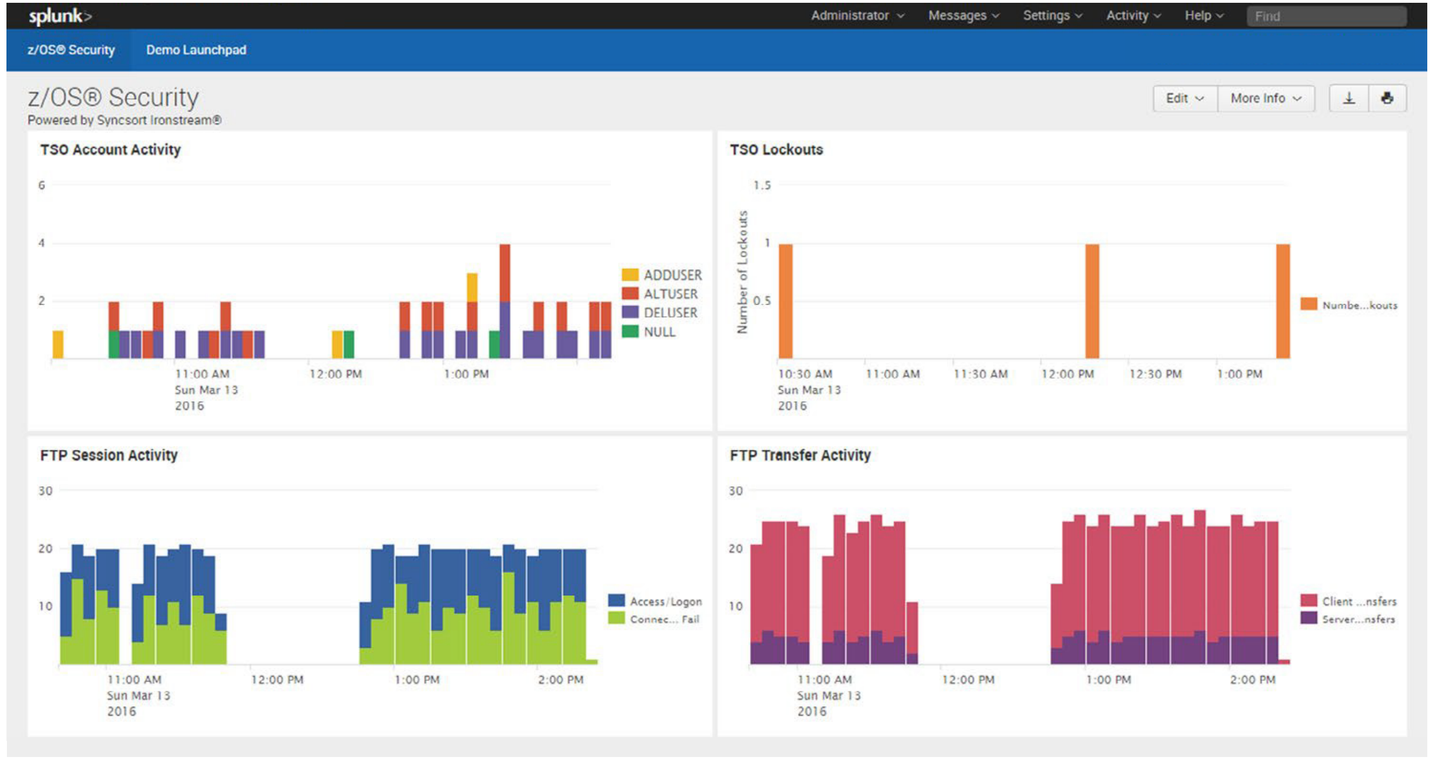
It's not just incorrect user definitions or weak security administration for users that results in risk. Many times the resources themselves are not protected appropriately. Protection might be too general, with too many users and applications being granted access that shouldn't have the rights. Therefore, it might be essential to provide an additional level of security monitoring to ensure that critical dataset resources are not being accessed by undesired users.



Splunk Enterprise Security Meets the Mainframe

4. Data Vulnerability

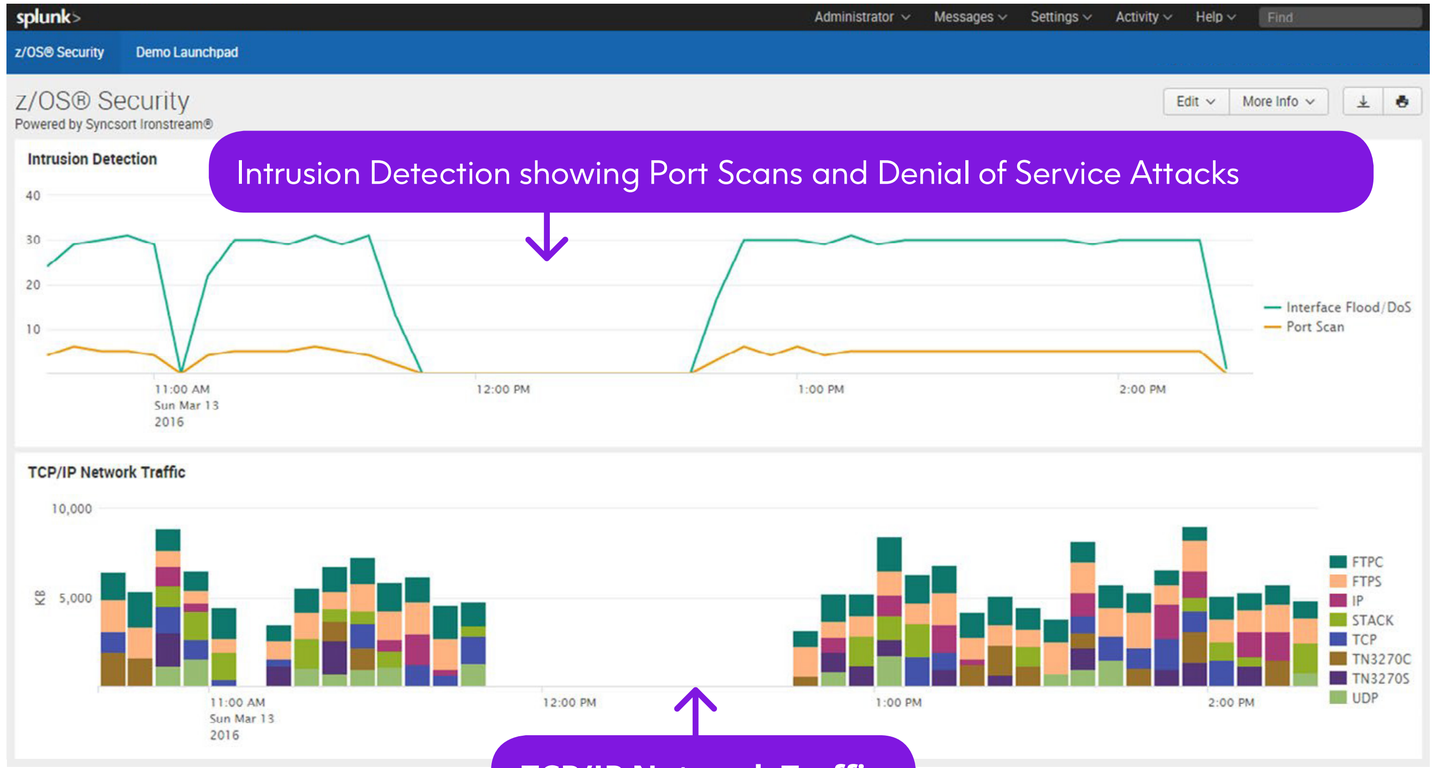
The mainframe no longer operates as an isolated component. In most organizations the mainframe is part of a complex IT infrastructure that includes distributed systems all networked together to enable a highly efficient processing environment with data moving freely between the different platforms. Incorrect data coming into the mainframe or secure data leaving the mainframe is a real threat for these type of infrastructures. Files being transferred between platforms must be well monitored so we can effectively identify what is coming in, what is going out, who is sending it in, and who is sending it out, to ensure the integrity of valuable data assets within an organization.



Splunk Enterprise Security Meets the Mainframe

5. Network Intrusion

As mentioned earlier, the mainframe is no longer an isolated component, but part of a larger IT infrastructure with a network ecosystem making it susceptible to outside attacks. Networks are the single biggest point of attack, and therefore they must be diligently monitored to look for unwanted port scans, Denial of Service (DoS) attacks, network flood attacks, malformed network packets, and other intrusions whereby someone from the outside is trying to block access to critical services or get in to compromise an organization and its critical data assets.



Mainframe Security Checklist

TSO Logon Activity
- Monitor for high “invalid” logon activity and locked user IDs for attempted breaches
- Monitor logon activity for users based on location and time of day
- Detect logon pattern anomalies that could indicate a breach

TSO Account Activity
- Monitor account creation, update, deletion
- Validate defined authorization and access rights for users and groups
- Ensure password expiration periods are set for users
- Ensure defined passwords meet security requirements

Critical Dataset Monitoring
- Ensure only authorized users and groups are accessing critical datasets
- Monitor unauthorized access attempts

File Transfer (FTP) Activity
- Ensure only authenticated users are sending or receiving files
- Monitor FTP file activity including file modification, download, creation, deletion
- Track inbound and outbound files along with who is initiating the transfer

Intrusion Detection
- Monitor port scans (fast and slow)
- Monitor flood attacks (interface floods, SYN attacks,
- Denial of Service - DoS)
- Perform malformed packet detection

IP Traffic Analysis
- Monitor IP component usage (TCP, UDP, Stack, tn3270 etc.)
- Monitor network infrastructure events

Mainframe Security Critical Data Sources

TSO Logon Activity: SMF Type 30

Subtype 1 - Logon activity for TSO users is captured via SMF Type 30, Subtype 1 which records all job and session start activity

TSO Account Activity: SMF Type 80

Creation, updates, deletion and lockout activity for TSO accounts are captured. For RACF the following commands are recorded:

- **ADDUSER - creating a new TSO user account**
- **ALTUSER- changing an existing TSO user account**
- **DELUSER - deletion of an existing TSO user account**

SMF Type 80 Event Code Qualifier (7) is used for LOCKOUT detection:

- When SMF80EVQ = 7 TSO user account lockout due to excessive password attempts

Critical Dataset Access Monitoring: SMF Record Types 14, 15, 17, 30, and 80

Critical dataset access monitoring requires utilizing 5 different SMF record types.

- **SMF Type 14 for input datasets**
- **SMF Type 15 for output datasets**
- **SMF Type 17 for scratch (temporary) datasets**
- **SMF Type 30 records job activity including datasets allocated for use by a job or workload**
- **SMF Type 80 captures dataset access authorization requests from RACF, ACF2, and Top Secret**

Mainframe Security Critical Data Sources

File Transfer Protocol (FTP) Session Activity: syslogd Messages EZYFS5nI

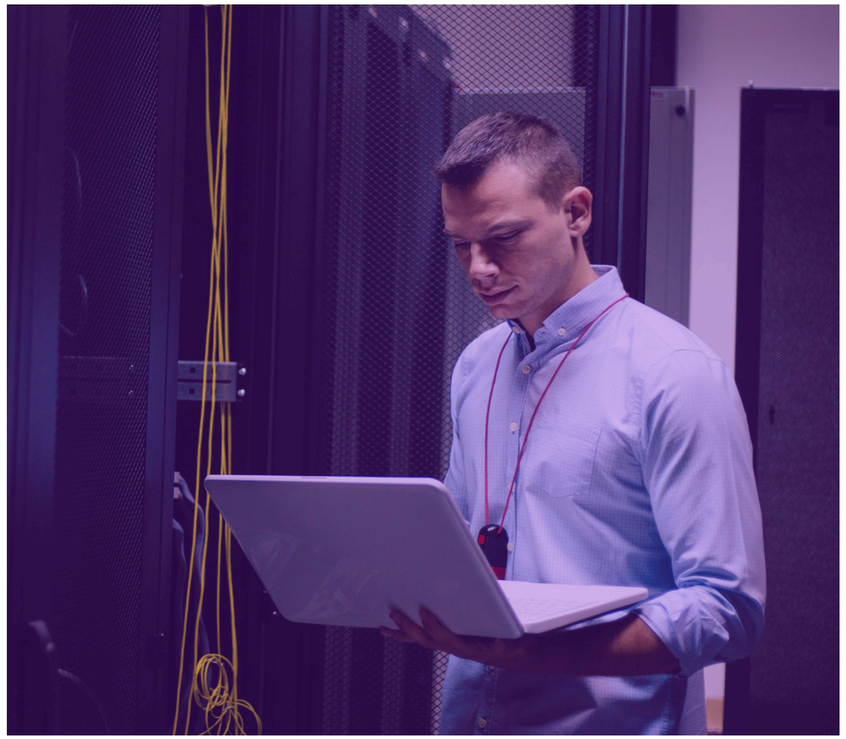
FTP session activity is recorded via the following syslogd messages:

- **EZYFS51I - CONN fails**
- **EZYFS52I - CONN ends**
- **EZYFS56I - ACCESS OK**
- **EZYFS57I - ACCESS fails**

File Transfer Protocol (FTP) File Change Activity: SMF Type 119

File modification, download, creation and deletion activity is captured in SMF Type 119 records. The following record sub-types are critical:

- **Subtype 3 - records z/OS acting as an FTP client (data potentially leaving the mainframe).**
- **Subtype 70 - records z/OS acting as an FTP server (data potentially arriving on the mainframe).**



Mainframe Security Critical Data Sources

Intrusion Detection: Traffic Regulation Management Daemon (TRMD) and SYSLOGD

z/OS implements Intrusion Detection Services (IDS) via the Traffic Regulation Management Daemon (TRMD) which is part of the z/OS Communications Server. TRMD is required to detect and collect intrusion events. The daemon must be configured to collect the following message types, which are recorded to syslogd:

- **EZZ8643I - TRMD SCAN threshold exceeded**
- **EZZ8650I - TRMD ATTACK SYN flood**
- **EZZ8654I - TRMD ATTACK Interface flood start: date**
- **EZZ8648I - TRMD ATTACK packet was discarded**
- **EZZ8649I - TRMD ATTACK packet would have been discarded (packet kept)**

File Transfer Protocol (FTP) File Change Activity: SMF Type 119

Various IP traffic types (IP, UDP, FTP, Stack activity etc.) are tracked via SMF Type 119 in a variety of record subtypes. Traffic analysis is captured when network connections are terminated. Most critical is:

- **Subtype 2- Connection termination**

Network Management/ User-Defined Notifications: Requires a Network Management Component

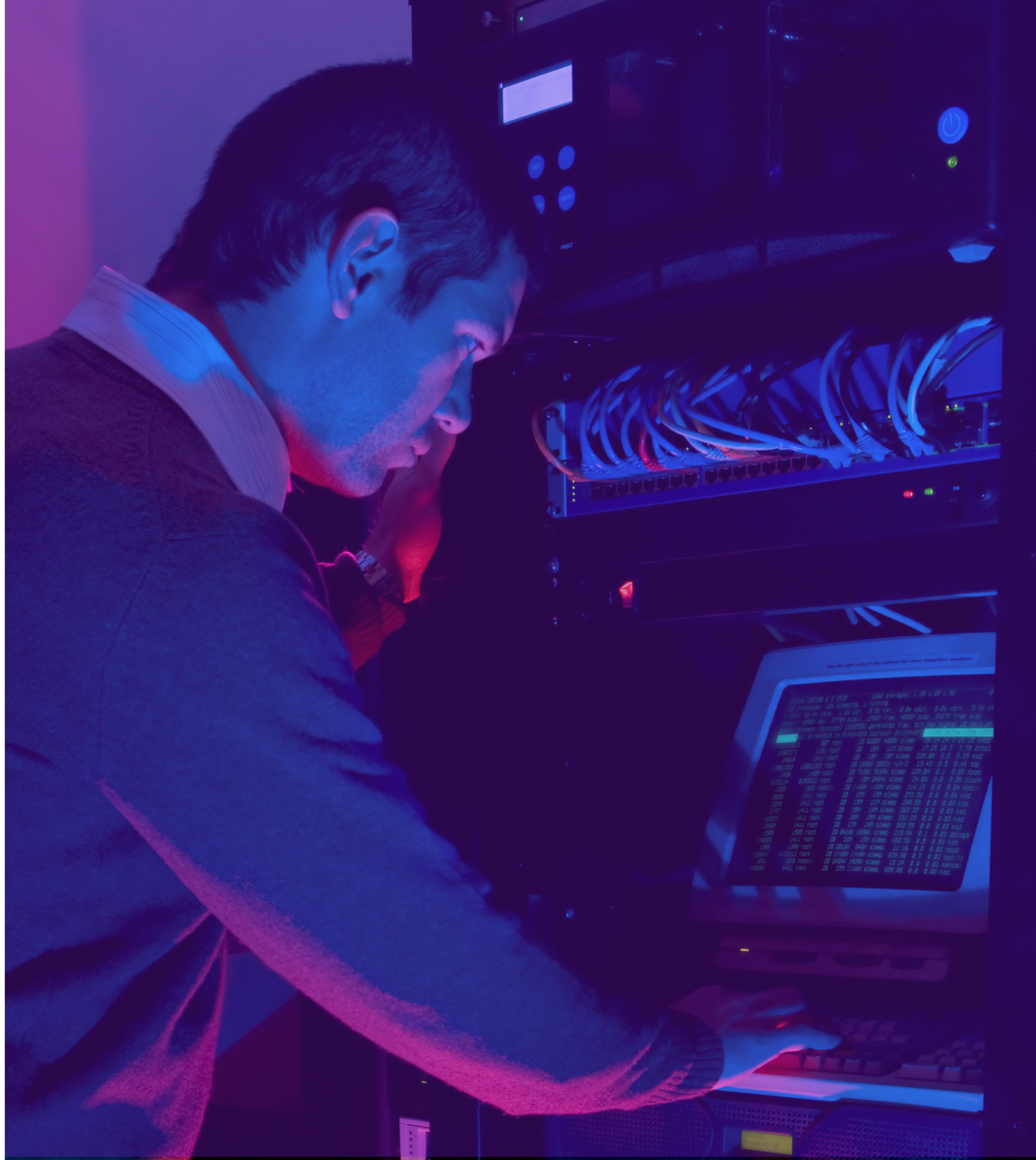
Alerts and notifications detected by a network manager can be critical in understanding potential threats and intrusions. These can include events such as broken connections, threshold breaches, or low activity anomalies. User-defined alerts might also be created within the network manager for installation specific condition tracking. An example of a network management component providing these type of capabilities would be Precisely Syncsort.

Conclusion

The IBM mainframe platform is undeniably one of the most secure server platforms in the world. As an isolated system it is virtually impenetrable from outside attacks. However, in today's modern IT infrastructures the mainframe resides as a critical processor within the network making it susceptible to external threats and attacks. Furthermore, defined user accounts within the system can always be leveraged to access and compromise secured resources. These types of attacks can occur when account information is maliciously compromised or it simply can occur when employees are disgruntled or careless.

Fortunately, security systems and components within the IBM z/OS mainframe enable critical resources to be protected and provide excellent event recording and logging that can be leveraged to determine potential threats and security risks. In addition to this, many system functions utilize SMF recording to provide an abundance of information related to logons, account changes, and FTP activity to help provide a complete picture of security on the mainframe. Finally, Intrusion Detection Services (IDS) via the Traffic Regulation Management Daemon (TRMD) which is part of the z/OS Communications Server, and alerts/notifications detected by a network manager can be critical in understanding potential threats and intrusions occurring from the outside world.

The information is available as outlined in this eBook – an IT security team simply has to leverage the data sources to effectively monitor for threats and prevent risks to their mainframes.



precisely

About Precisely

As a global leader in data integrity, Precisely ensures that your data is accurate, consistent, and contextual. Our portfolio, including the Precisely Data Integrity Suite, helps integrate your data, improve data quality, govern data usage, geocode and analyze location data, and enrich it with complementary datasets for confident business decisions. Over 12,000 organizations in more than 100 countries, including 93 of the Fortune 100, trust Precisely software, data, and strategy services to power AI, automation, and analytics initiatives. Learn more at www.precisely.com

www.precisely.com