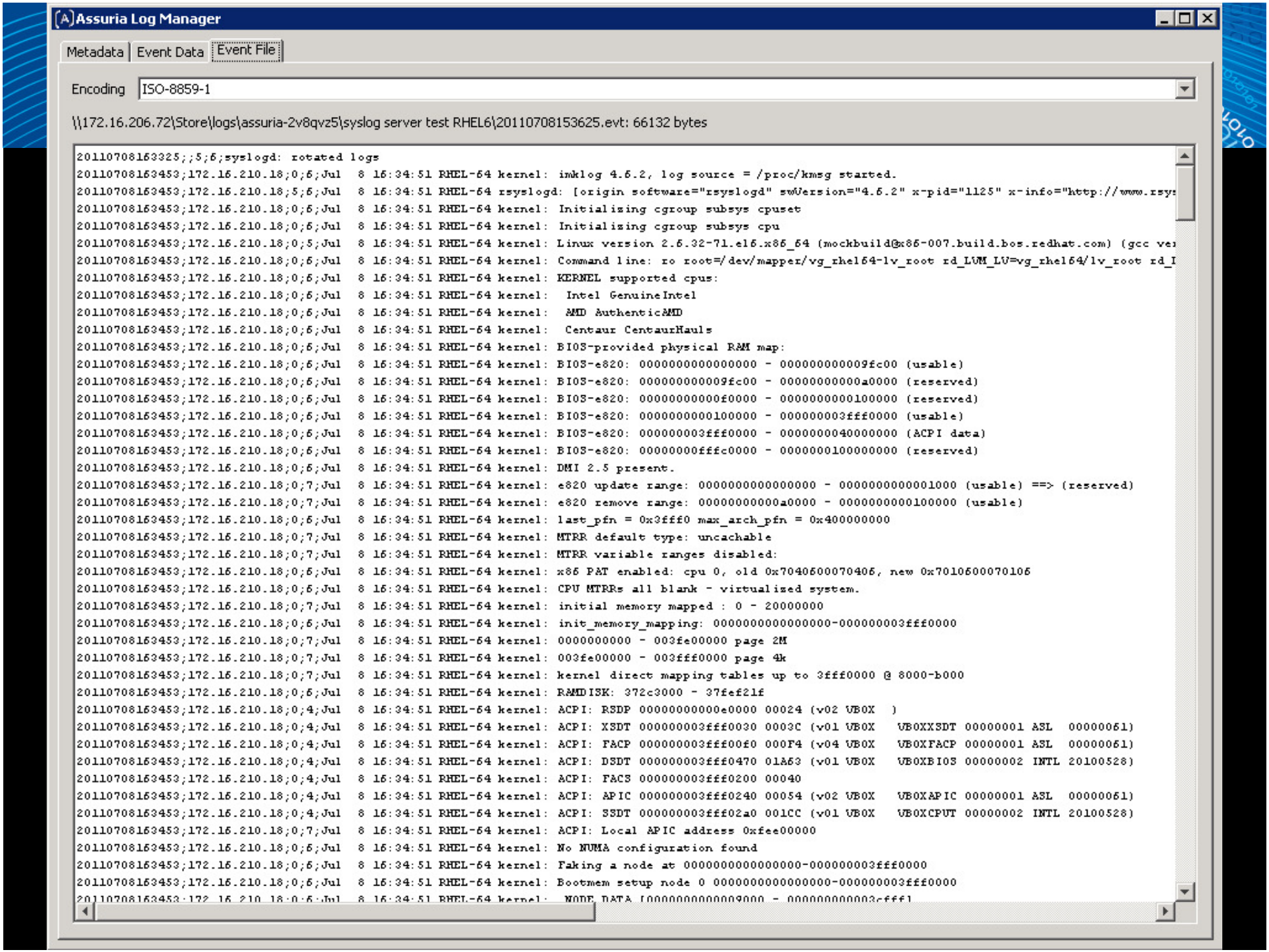
Log management and log analysis and iGRC

Nick Connor
Technology Group, iGRC Consortium

Co-Founder and Director
Assuria Limited

Audit / Event Logs?

- What are audit logs?
  - A record of activity
    - Events
    - Transactions
    - Access attempts
- Why are audit logs relevant to GRC?
  - Verify working controls
  - Help identify failing controls
- Where do audit logs come from?
  - Almost anything with a processor and software


Assuria Log Manager
Metadata
Event Data
Event File
Encoding
ISO-8859-1
\\172.16.206.72\Store\logs\assuria-2v8qvz5\syslog server test RHEL6\20110708153625.evt: 66132 bytes
20110708163325;;5;6;syslogd: rotated logs
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: imklog 4.6.2, log source = /proc/kmsg started.
20110708163453;172.16.210.18;5;6;Jul 8 16:34:51 RHEL-64 rsyslogd: [origin software="rsyslogd" swVersion="4.6.2" x-pid="1125" x-info="http://www.rsys
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: Initializing cgroup subsys cpuset
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: Initializing cgroup subsys cpu
20110708163453;172.16.210.18;0;5;Jul 8 16:34:51 RHEL-64 kernel: Linux version 2.6.32-71.el6.x86_64 (mockbuild@x86-007.build.bos.redhat.com) (gcc ver
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: Command line: ro root=/dev/mapper/vg_rhel64-lv_root rd_LVM_LV=vg_rhel64/lv_root rd_I
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: KERNEL supported cpus:
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: Intel GenuineIntel
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: AMD AuthenticAMD
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: Centaur CentaurHauls
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: BIOS-provided physical RAM map:
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: BIOS-e820: 0000000000000000 - 000000000009fc00 (usable)
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: BIOS-e820: 000000000009fc00 - 00000000000a0000 (reserved)
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: BIOS-e820: 00000000000f0000 - 0000000000100000 (reserved)
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: BIOS-e820: 0000000000100000 - 000000003fff0000 (usable)
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: BIOS-e820: 000000003fff0000 - 0000000040000000 (ACPI data)
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: BIOS-e820: 00000000fffc0000 - 0000000100000000 (reserved)
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: DMI 2.5 present.
20110708163453;172.16.210.18;0;7;Jul 8 16:34:51 RHEL-64 kernel: e820 update range: 0000000000000000 - 0000000000001000 (usable) ==> (reserved)
20110708163453;172.16.210.18;0;7;Jul 8 16:34:51 RHEL-64 kernel: e820 remove range: 00000000000a0000 - 0000000000100000 (usable)
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: last_pfn = 0x3fff0 max_arch_pfn = 0x400000000
20110708163453;172.16.210.18;0;7;Jul 8 16:34:51 RHEL-64 kernel: MTRR default type: uncachable
20110708163453;172.16.210.18;0;7;Jul 8 16:34:51 RHEL-64 kernel: MTRR variable ranges disabled:
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: x86 PAT enabled: cpu 0, old 0x7040600070406, new 0x7010600070106
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: CPU MTRRs all blank - virtualized system.
20110708163453;172.16.210.18;0;7;Jul 8 16:34:51 RHEL-64 kernel: initial memory mapped : 0 - 20000000
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: init_memory_mapping: 0000000000000000-000000003fff0000
20110708163453;172.16.210.18;0;7;Jul 8 16:34:51 RHEL-64 kernel: 0000000000 - 003fe00000 page 2M
20110708163453;172.16.210.18;0;7;Jul 8 16:34:51 RHEL-64 kernel: 003fe00000 - 003fff0000 page 4k
20110708163453;172.16.210.18;0;7;Jul 8 16:34:51 RHEL-64 kernel: kernel direct mapping tables up to 3fff0000 @ 8000-b000
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: RAMDISK: 372c3000 - 37fef21f
20110708163453;172.16.210.18;0;4;Jul 8 16:34:51 RHEL-64 kernel: ACPI: RSDP 00000000000e0000 00024 (v02 VBOX)
20110708163453;172.16.210.18;0;4;Jul 8 16:34:51 RHEL-64 kernel: ACPI: XSDT 000000003fff0030 0003C (v01 VBOX VBOXXSDT 00000001 ASL 00000061)
20110708163453;172.16.210.18;0;4;Jul 8 16:34:51 RHEL-64 kernel: ACPI: FACP 000000003fff00f0 000F4 (v04 VBOX VBOXFACP 00000001 ASL 00000061)
20110708163453;172.16.210.18;0;4;Jul 8 16:34:51 RHEL-64 kernel: ACPI: DSDT 000000003fff0470 01A63 (v01 VBOX VBOXBIOS 00000002 INTL 20100528)
20110708163453;172.16.210.18;0;4;Jul 8 16:34:51 RHEL-64 kernel: ACPI: FACS 000000003fff0200 00040
20110708163453;172.16.210.18;0;4;Jul 8 16:34:51 RHEL-64 kernel: ACPI: APIC 000000003fff0240 00054 (v02 VBOX VBOXAPIC 00000001 ASL 00000061)
20110708163453;172.16.210.18;0;4;Jul 8 16:34:51 RHEL-64 kernel: ACPI: SSDT 000000003fff02a0 001CC (v01 VBOX VBOXCPUT 00000002 INTL 20100528)
20110708163453;172.16.210.18;0;7;Jul 8 16:34:51 RHEL-64 kernel: ACPI: Local APIC address 0xfee00000
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: No NUMA configuration found
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: Faking a node at 0000000000000000-000000003fff0000
20110708163453;172.16.210.18;0;6;Jul 8 16:34:51 RHEL-64 kernel: Bootmem setup node 0 0000000000000000-000000003fff0000

Audit / Event Logs?

- What are audit logs?
  - A record of activity
    - Events
    - Transactions
    - Access attempts
- Why are audit logs relevant to GRC?
  - Verify working controls
  - Help identify failing controls
- Where do audit logs come from?
  - Almost anything with a processor and software

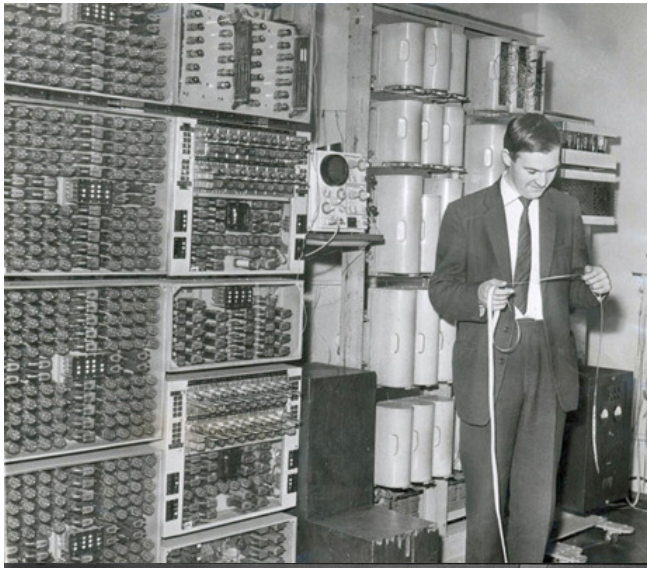
What gets logged?

- System or software startup, shutdown, restart, and abnormal termination (crash)
- Thresholds being exceeded or reaching dangerous levels: Disc space, Memory, Processor load,…….
- Hardware health that the system can detect and record.
- User access to a system. Remote login (RDP, telnet, ssh), Local login, network access (FTP, SFTP), VPN access,
- User access privilege changes; an ‘su’ command on Unix/Linux.
- Object access: read, write,
- Audit policy change
- User credentials and access right changes.
- Account updates, creation, and deletion.
- System configuration changes and software updates.
- Access to system logs. Modification, deletion, reading!

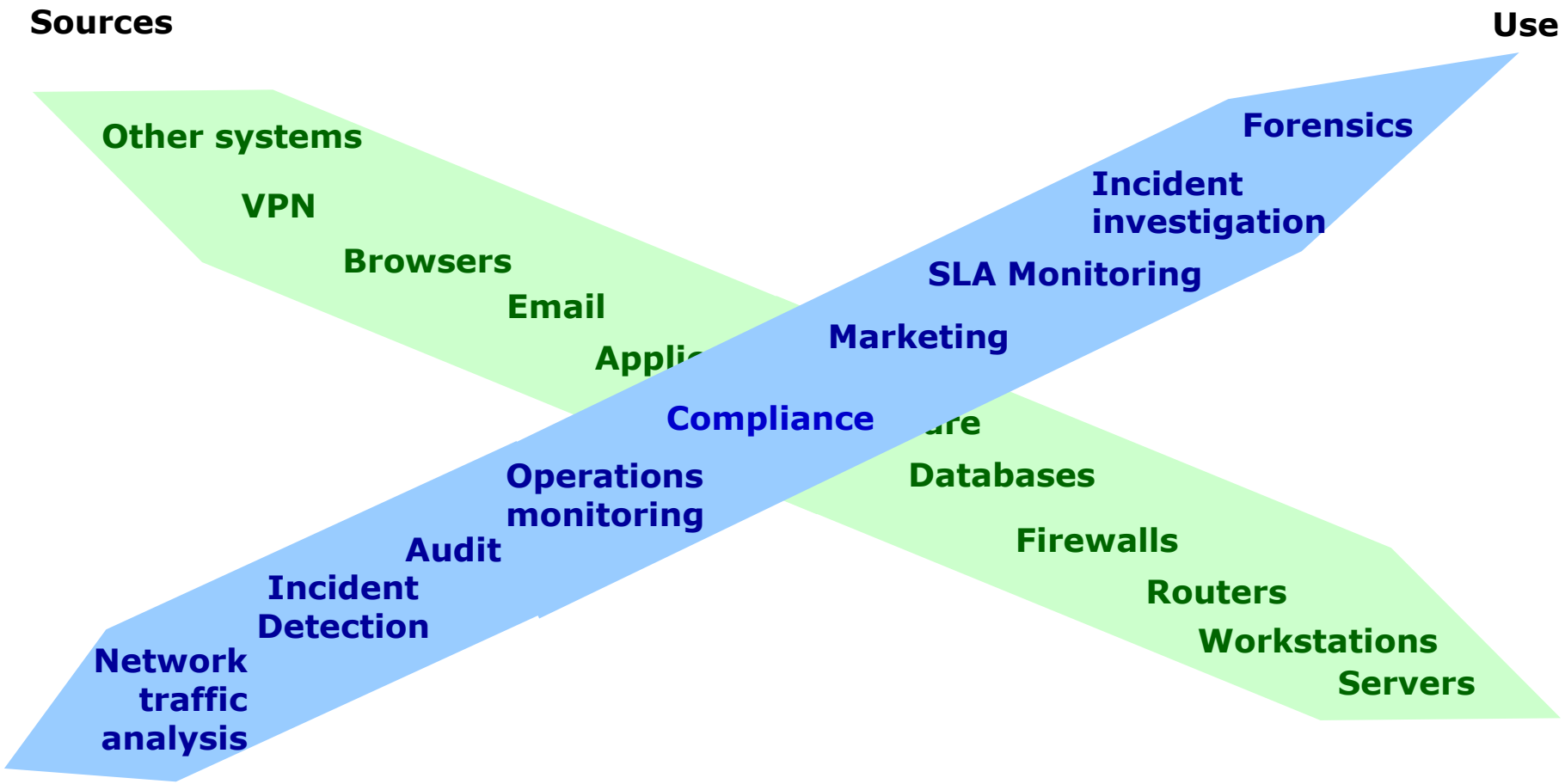
Not a complete list

Use of log data

- Not new, multiple uses
- Used for incident investigation / debugging of systems for many years.
- Typically in specific areas – network, database, system.
- Requirements now for an enterprise view of logs – SIM, SIEM products.
- Mainly driven by compliance requirements.



Logs – sources and uses



Logs can provide

Key information relating to events / incidents:

- What?
- When?
- Where?
- Who?
- What to?
- Where from?

Good or bad?

- ✓ A failed logon event is good as it shows that a control is working.
- ✗ Multiple failed logon events may indicate that someone is trying to break in to the system.
- ✗ Multiple failed logon event in rapid succession may indicate that an automated attempt to break in is underway.

Good or bad?

- ✓ A successful logon event provides a record of an access to a system.
- ✘ A successful logon out of normal hours may indicate a break-in to the system.

Risk events

Risk events can be identified from log data:

- Secure collection of audit / event logs from servers, workstations, network devices, applications, databases, security tools across the organisation
- Through the analysis, aggregation, enri and correlation of events from audit / event logs Risk Events can be identified.

Value of log analysis

The simple analysis of logs can reveal:

- Policy failure or compliance.
- Misuse - Login by a former employee.
- Insider activity - Access to sensitive data.
- Compliance:
  - Confirmation that controls are working.
  - Alert if controls not working.

Value of log analysis

More sophisticated analysis can detect:

- Sequence of correlated and or aggregated events.
- Anomalous events.
- Policy failure.

ALL are potential RISK events

Value of logs

In addition to identifying Risk Events collected audit and event logs can be used to:

- Demonstrate compliance to auditors
- Support a forensic readiness requirements.
- Provide data for forensic analysis.
- Provide audit trail for possible evidential use.

Summary

- Log data can enhance the understanding of activity on IT systems.
- Help identify issues either:
  - Preventative

  or

  - Reactive
- Risk events can be identified and fed to GRC platforms via the iGRC interface.

Thank you

nickc@assuria.com
www.assuria.com