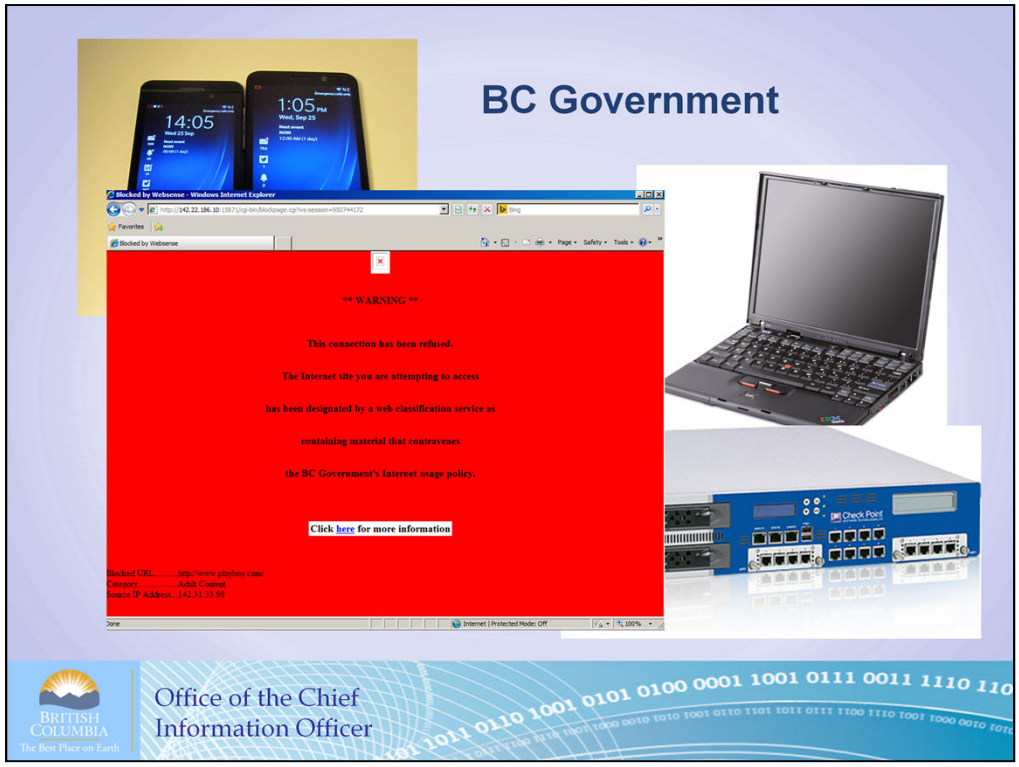
Security Logging and Monitoring

February 7th, 2014



Government's Technology Wing

Under the Office of the Chief Information Officer

Manage and Maintain the Government Desktops, Mobile Devices, Servers, Network and Security Infrastructure.

Within this environment our group looks after infrastructure security devices.

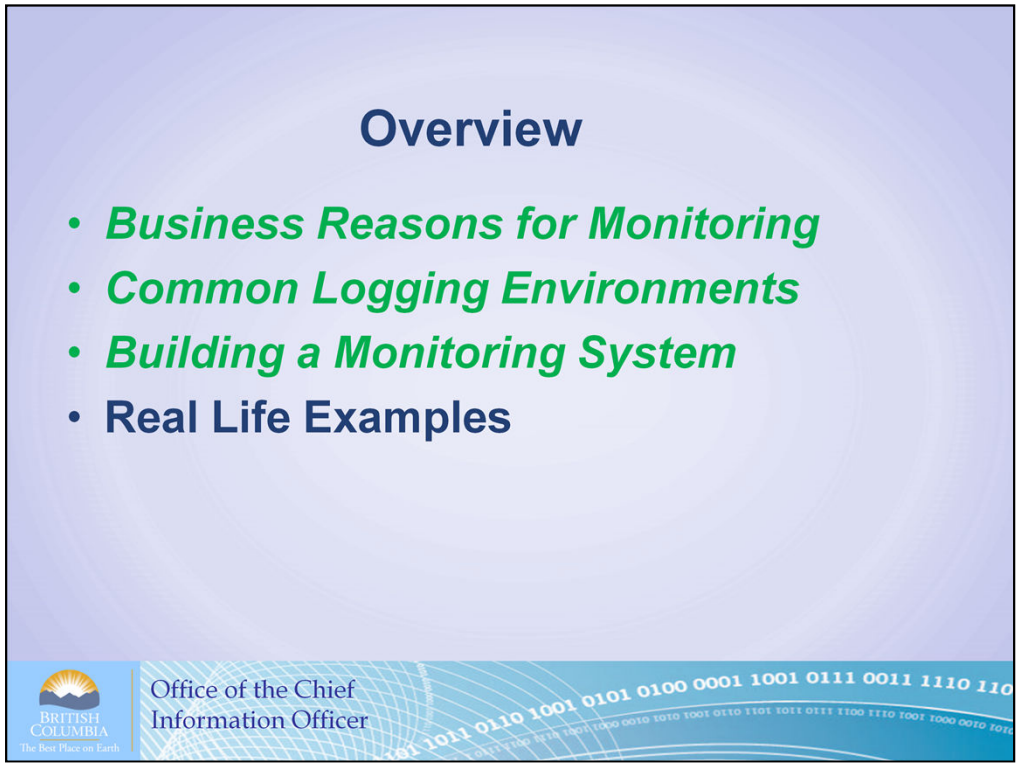
Scope and size of SPAN/BC

Clients : Ministries, Schools, Colleges, Communities, Pharmacies,

Users : 700,000 ++

All types of devices from SmartPhones, Desktops, routers, switches, firewalls, servers

Locations: Secure Data Centers, Restricted Office Buildings, Publicly accessible Government offices, Schools, School Boards, Community Centers,



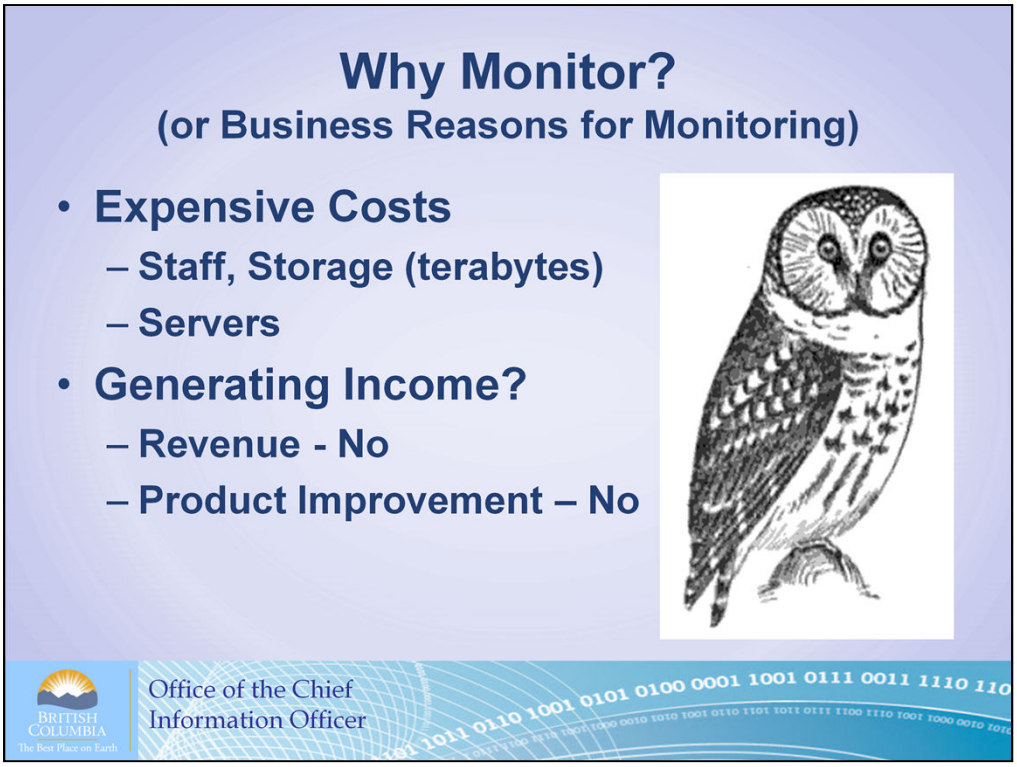
Introduction – Background of Government Monitoring

Why – Reasons for monitoring

What – are the Key IT Environments

How – to build a monitoring system.

Time permitting we'll take a look at some real life monitoring examples.



Why would you monitor – it takes up resources such as staff, terabytes of storage and dedicated monitoring servers? There had better be some good reasons. Most of this is overhead costs that don't contribute to revenue growth.

Drivers for building a monitor system :

Everything in IT , not just logging and monitoring, should have a business justification, a reason to be sponsored by Senior Executives. Sometimes this is to save money, sometimes it's to improve service and sometimes it's to enable a new way of doing something.

The "HAVE TO" Category - Legislation and Policy

or "WANT TO" Category - Manage Business Risk and Validate Existing Controls.

Psuedo Legislation – Industry Watchguard with teeth. Fines can run into the tens of millions of dollars for groups that don't pass the requirements – including logging and monitoring of network, database and server infrastructure.

Big one here is PCI standards which threaten to impose large financial penalties on non-compliance. This standards alone has been responsible for the huge growth in Security Monitoring companies over the past 5 years.

Corporate Policy – ISO 27001 is an International Best Practice.

BC Government policy is based on the ISO27001 framework

Most companies have Corporate Policy, but this alone is usually not a strong enough reason to implement a monitoring program. It's often used in conjunction with Auditor's who find that the Operations are not matching the Policy.

Logging and Monitoring wouldn't PREVENT a breach. There are lots of other controls for this at the Enterprise level – Anti-Virus, Intrusion Prevention, Firewalls.

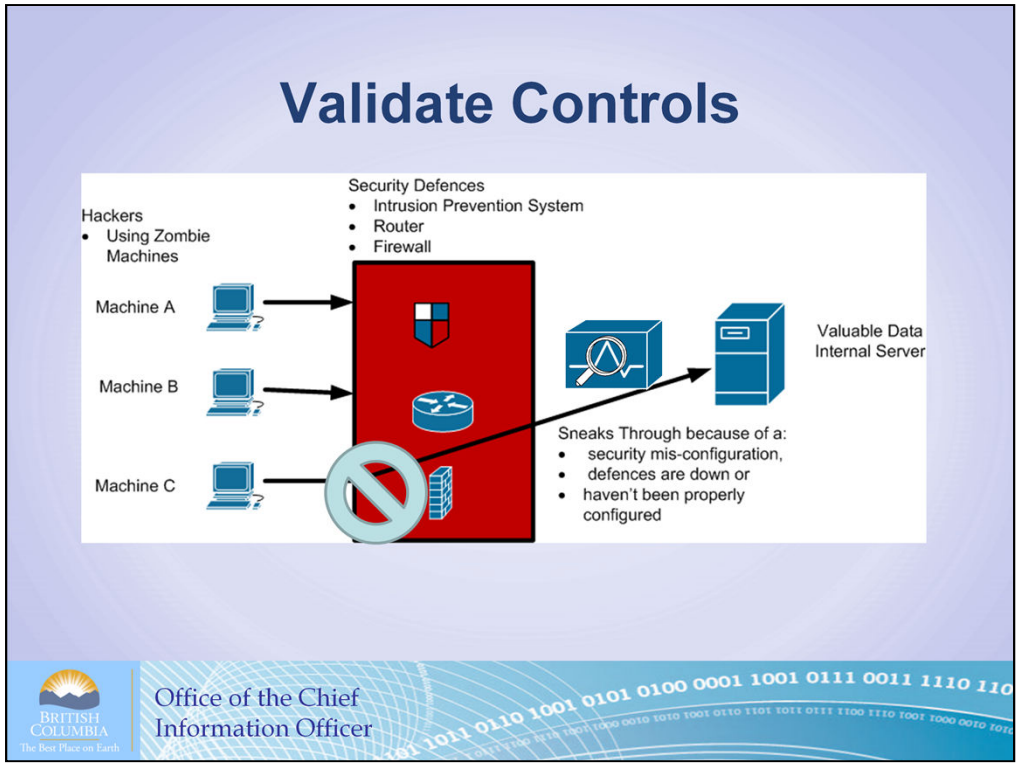
Invariable, there seems to be weaknesses either in the product, the implementation or the overall architecture. You must operate under the assumption that your organization either is or will be compromised and that logs are the key way in determining what has happened.

BC Government Newspaper incident – Commonly visited local newspaper web site was infected with an ad banner. AV didn't prevent it, three levels of network defenses didn't prevent the breach. The AV software did notify us that the system was infected – it then had to be re-imaged.

Financial Gain can be through selling BotNets or trying to break into bank accounts. Either way the malware is designed to be difficult to detect.

Nation States and the IOC in Montreal, didn't even know they were compromised. Shown the evidence and still didn't believe.

Insiders – may not how to circumvent security controls but not necessarily the monitoring systems.



Validate Controls – existing Security controls may not be working as expected for a variety of reasons. Perhaps the hardware malfunctioned and all traffic is bypassing the Security Device. We have seen this in the past where a security device “Fails Open”, if it stops working the device is configured to pass all traffic through rather than shut down the link.

Regular Security device configuration changes, either to the rule set or to the Operating System can result in traffic unexpectedly getting through. Maybe a rule was accidently deleted when making a change or a rule was put in place that negated another rule. Perhaps the rules where changed but the changes where never applied or made active.

Real life example from 10 years ago within the BC Government.

Someone brought down a key BC Government Internet router for regular maintenance, when it was brought on-line they forget to apply the Access Control List, which at the time was the Government basic line of defence against Internet attacks. Within a few days many internal devices where experiencing direct attacks from the Internet and internal logs where showing unusual connection attempts from the Internet. The problem was traced back to the Internet Gateway ACL and it was re-applied.

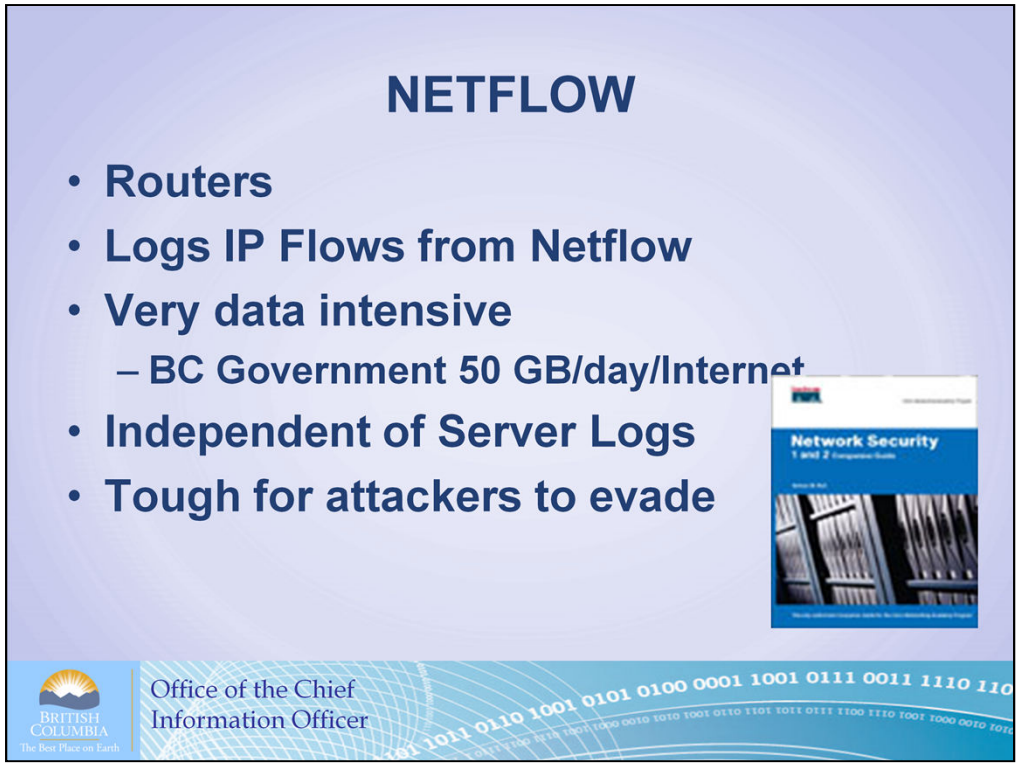
Monitoring = Logging plus Log Analysis

Big Three = Netflow for Networks, Syslog for UNIX system and Event Viewer for Windows.

The logging environment's all perform the same function, they provide a convenient program for log generating functions to use. These log generating function can be the Operating System and subroutines, applications and databases.

Our group also does Physical Security, we do not review the Application Logs as part of our regular duties.

Airborne Warning and Control Systems (AWACS)



Netflow is the standard router network traffic logging mechanism. It's been around since 1996. Cisco Product. Can contain up to 89 Fields of data.

Many monitoring programs take netflow data for analysis. Primary network accounting technology in the industry.

Provides a vast amount of data, usually the security aspect is 15 – 20 fields.

Q? Has anyone worked on Netflow data? When and what was experience?

Q? Who has heard of an IP Flow? Can you explain it to the class.

Monitoring IP Flows. An IP flow is all traffic associated with a connection. So there might be 25 packets with 50 000 bytes in a connection. This shows up as 1 flow with 25 packets and 50 000 bytes.

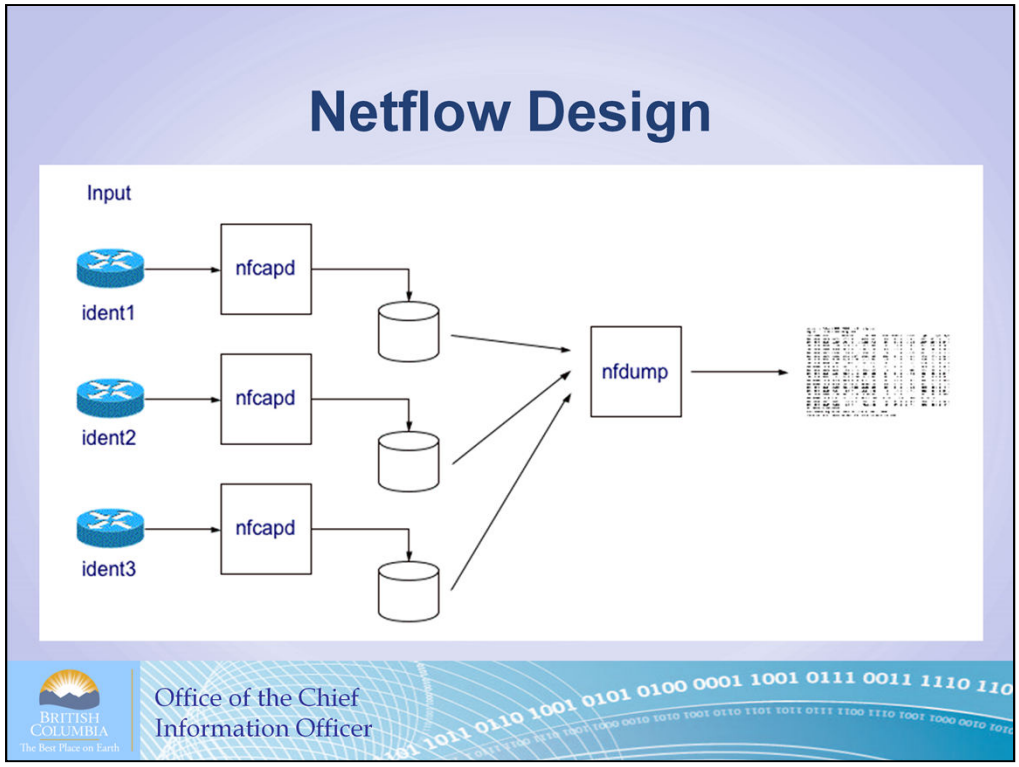
Bonus Fields:

Options (TOL, TTL, ID, ...)

Flags (SYN, ACK, PSH ....)

Interface (S0, Eth1, HME2...)

Excellent independent source for what happened, Netflow logs present a central view that attackers have a difficult time evading.



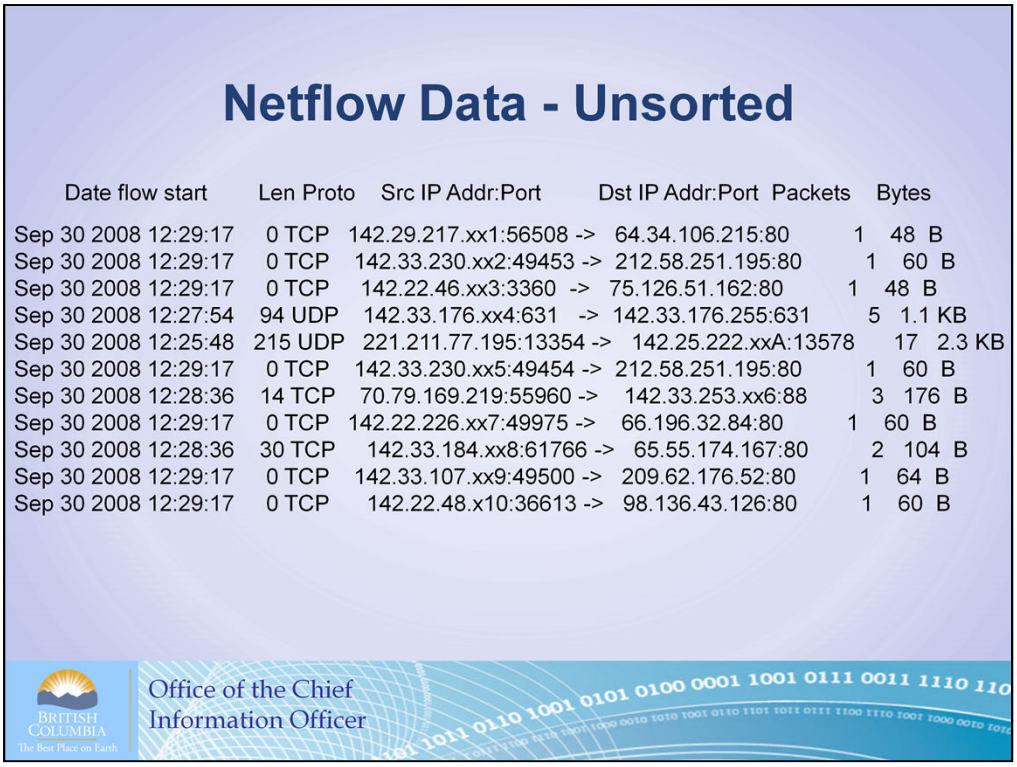
Captures the logs, very specific, doesn't log information on Operating System, authentication and a variety of applications. It only logs from one application, the netflow application which is an advanced application used to speed up packet processing.

Nfcapd ➔ Netflow Capture Daemon, captures all the netflow network traffic, stored on disk in binary format.

Nfdump ➔ Query Tool - Reads data (binary) from files stored by the netflow capture daemon.

Inbound traffic from the Internet can represent hackers

Outbound traffic from Servers to the Internet can represent compromised systems.



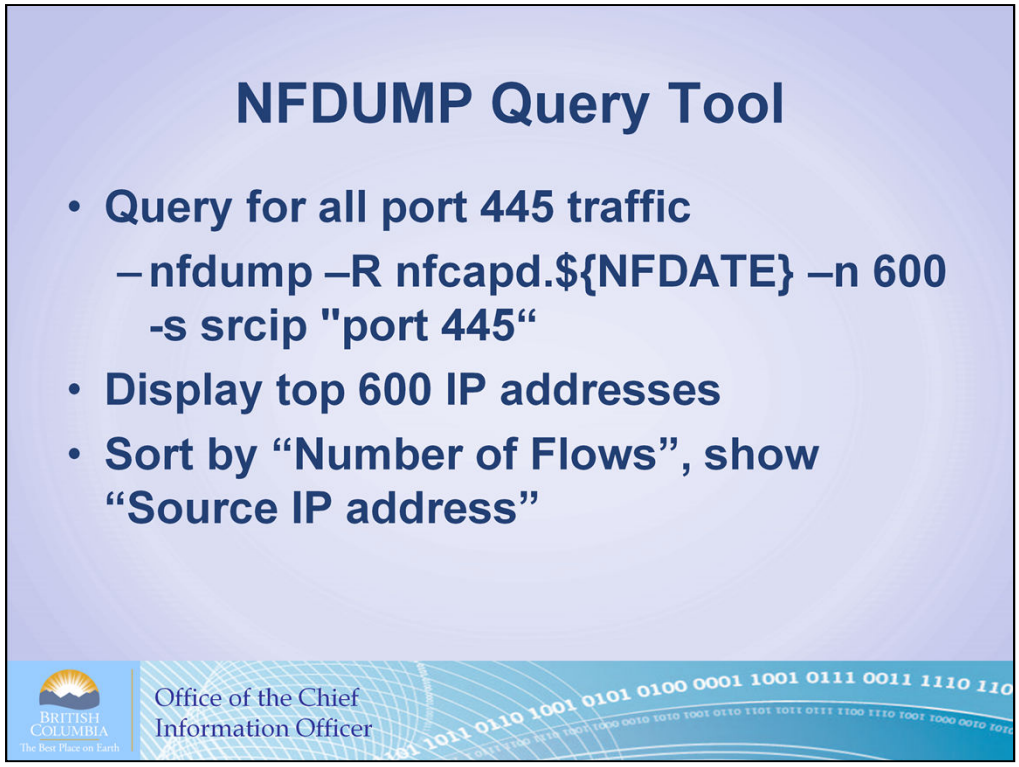
10 Fields here

Examples of other fields include

SRC_MASK, DST_MASK,, IPV4_Next_Hop, SRC_AS, DST_AS, BGP_IPV4_Next_Hop, FLOW_ACTIVE_TIMEOUT, FLOW_INACTIVE_TIMEOUT

This is raw netflow data taken from a nfdump query with no parameters for sorting or matching. It is virtually meaningless on it's own.

Investigator's will take the raw data and perform selected queries for IP addresses to get an idea of what a particular workstation was doing.



NFDump is the query tool for reading the Binary NetFlow data and converting it into useful Text.

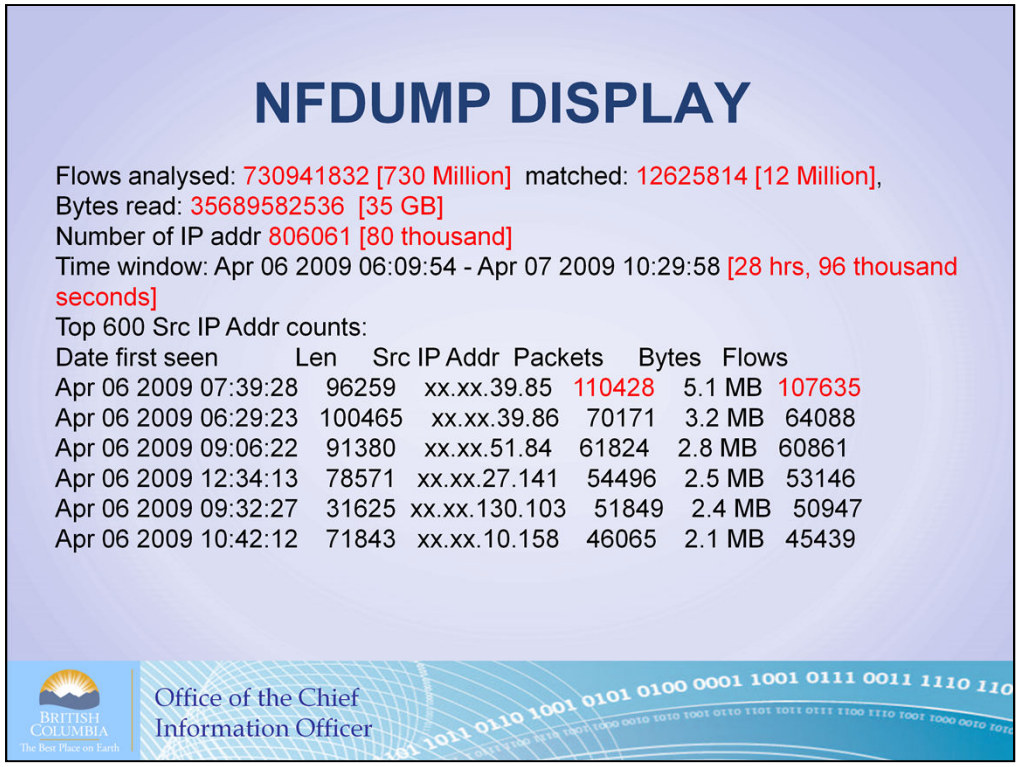
This search is for all traffic to port 445.

Could also search for a particular IP address, a subnet, multiple IP's or subnets and Ports

What kind of data do you think is stored by Netflow??

Answer :

- **Src / Dst IP**
- **Src / Dst Port**
- **Protocol (ICMP, UDP, TCP)**
- **Packets**
- **Bytes**
- **Start Time**
- **Length (in seconds) of flows**
- **Number of flows**
- **Autonomous System**
- **Next Hop**
- **Flags**



This is a real Netflow log parsed by NFDUMP for the BC Government's Internet gateway connection several years ago.

How to read the log: It shows that 730 Million records where analysed and there was 12 ½ Million matches. The number of overall bytes read was 35 GB.

The number of unique source IP addresses was 806,000.

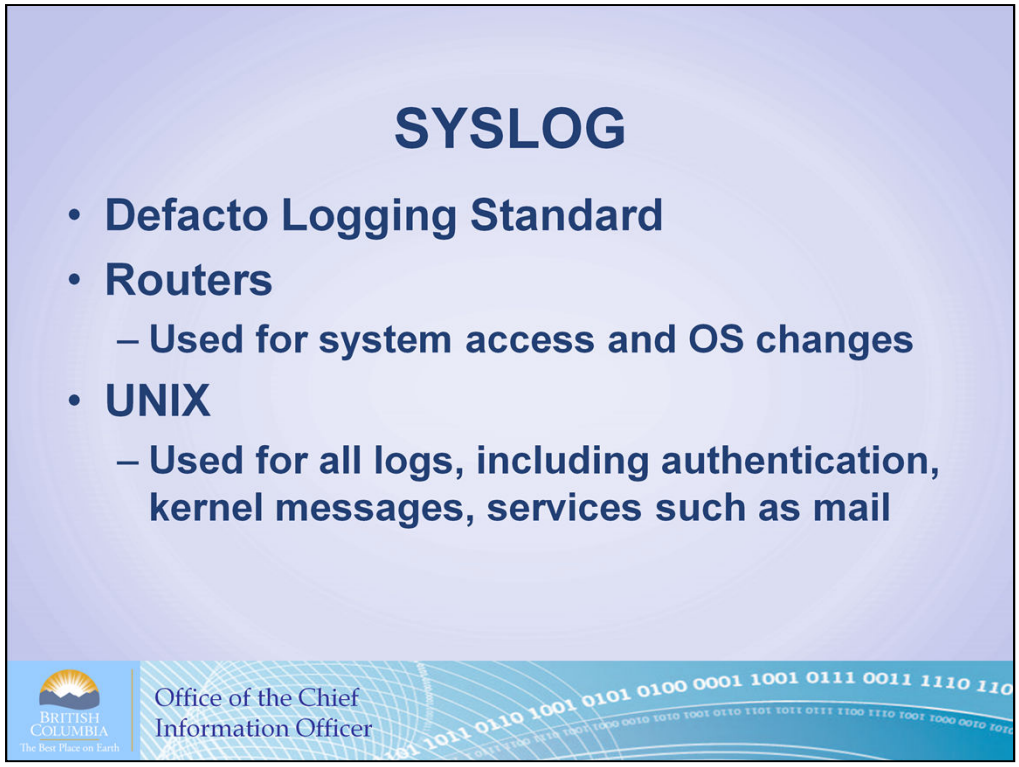
This data represented a 28 hour time span from Aprl 6 at 6AM to April 7 at 10 AM.

The top 600 SRC IP addresses are listed.

The first record reads that over a 96,259 second period during which this system produced IP Flow records, over 100,000 distinct FLOWS where detected on port 445. That is going out to a different system on the Internet every second for 26.7 hours straight. This does not indicate if there was a break at night . This system is clearly infected as are all the others listed here.

This is the Netflow signature for Conficker.

Netflow logs offer lots of information about network traffic but don't tell you much about the content of the traffic. Did the connections to a server result in a successful login? Was the user accessing restricted files or changing files on the server? Can't make this determination from Netflow.. Netflow logs are broad and shallow; Server logs are narrow and offer lots of detail for activity on a particular system.



Syslog developed in the 1980s by Eric Allman as part of the Sendmail project. Proved so valuable that other applications started using it. Syslog has since become the standard logging solution on UNIX and Linux systems.

Standard for forwarding log messages in an IP network

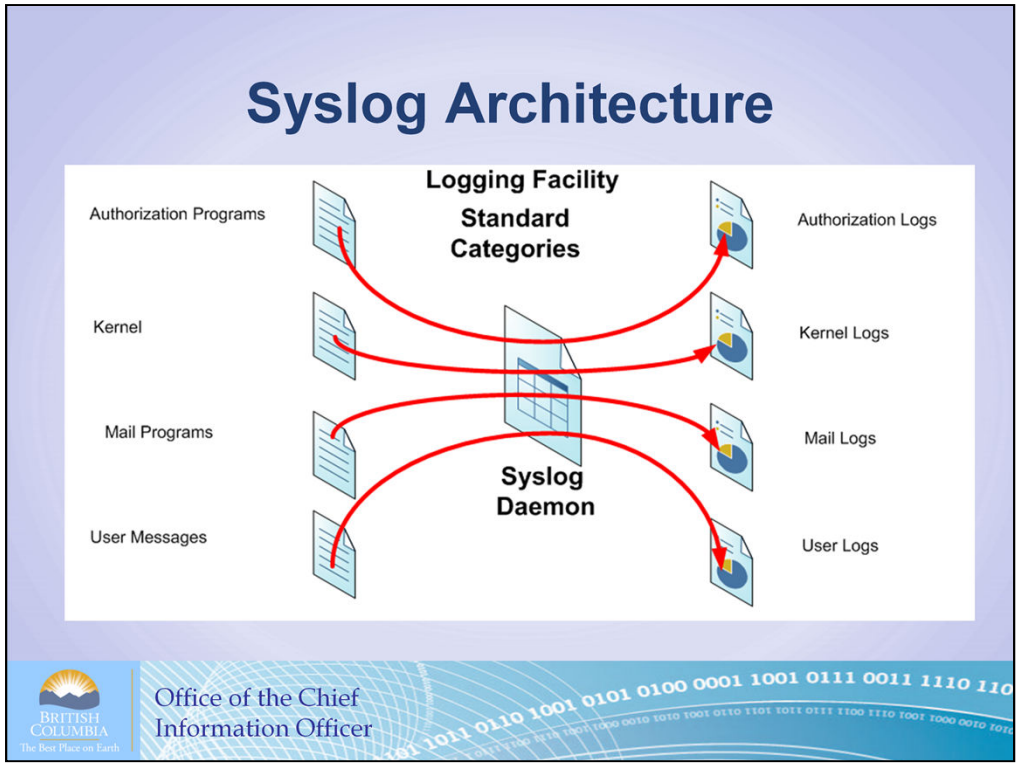
Syslog name is usually used for TWO meanings, A) as the network syslog protocol and B) as the application or library sending the messages

Syslog provides a true logging environment used by different Operating Systems, subsystems, common applications and services and specialized applications

Open Source, Comman Line Driven

REFERENCE ARTICLE:

http://www.sans.org/reading_room/whitepapers/casestudies/case_study_implementing_a_centralized_logging_facility_1205



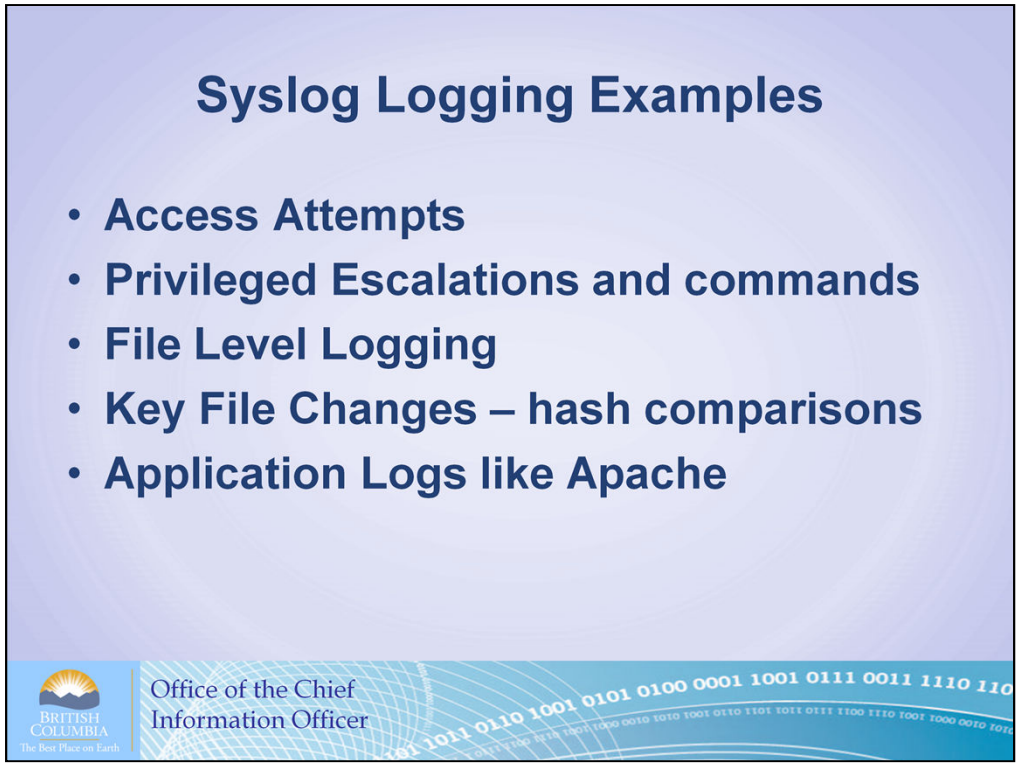
.

Syslog is like a traffic conductor, routing traffic from Log Generating processes to their proper destination, which could be a file, an E-mail, a console or a named pipe to another application.

Log Generating Processe => Kernel, SMTP, User Messages, Authorization Programs

Syslog is the conductor and relies primarily on the syslog.conf file to determine destinations.

Destination => Authorization Logs, Kernel Logs, Mail Logs, User Logs, Console, Remote Destination, E-mail.



You can tell if someone had a successful login, who was logging in, when and for how long.

Tell if someone elevated their privilege and what commands where performed (useful for audits).

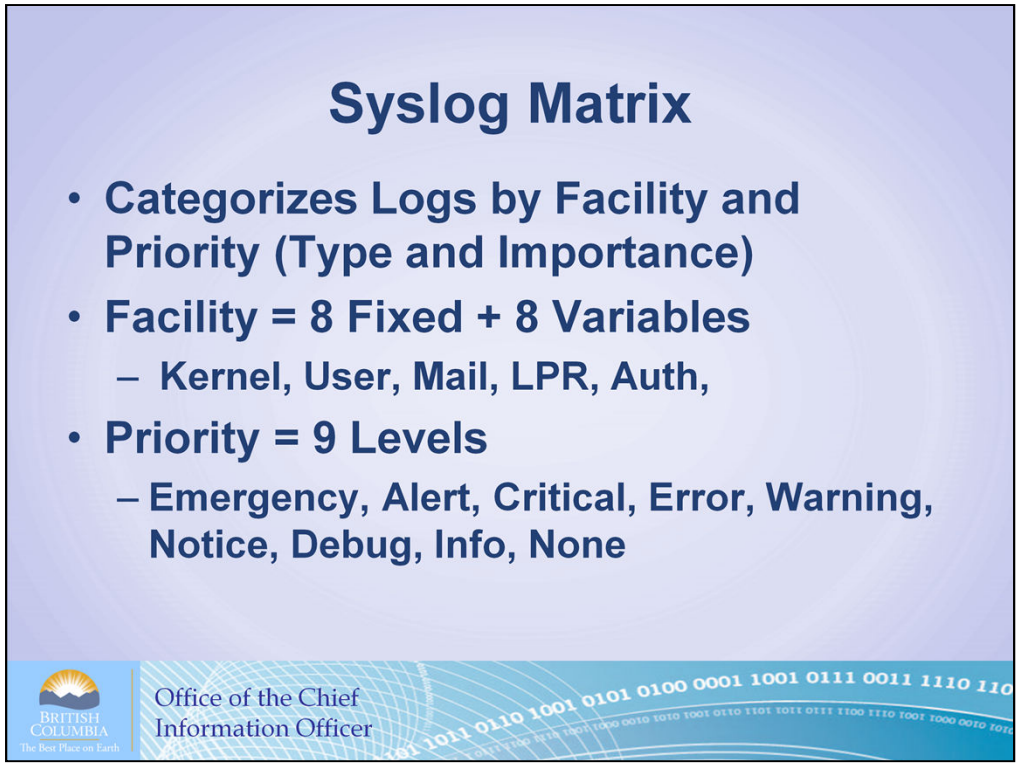
Tell if a particular file was read or altered

Are you familiar with "Hashing" and what it means?

Hint: Usually used as a One Way Hash for integrity purposes.

Netflow logs will tell you the quantity of traffic to the server, not the quality. System logs tell more of a story about the quality of the traffic.

Syslog is more Server or Host based. Netflow simple reports on one Application - Netflow



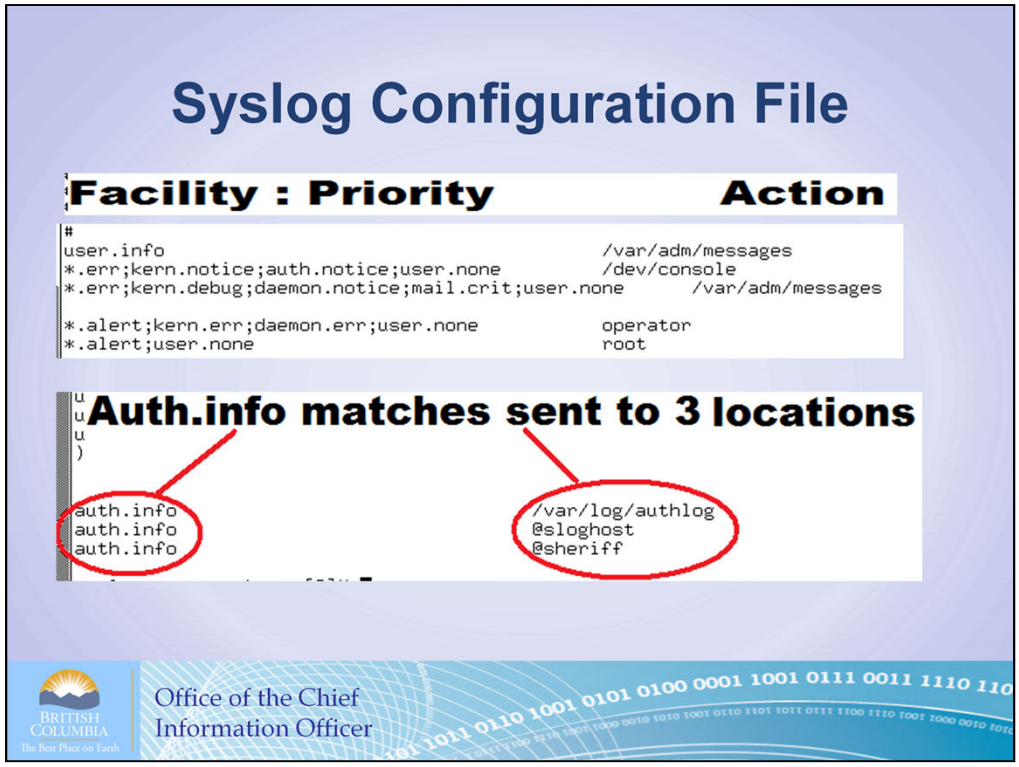
Two levels for categorization.

Originally 16 Facility Categories, RFC 3164 added an additional 8 Fixed Categories for a total of 24 of which 8 are still reserved for local use.

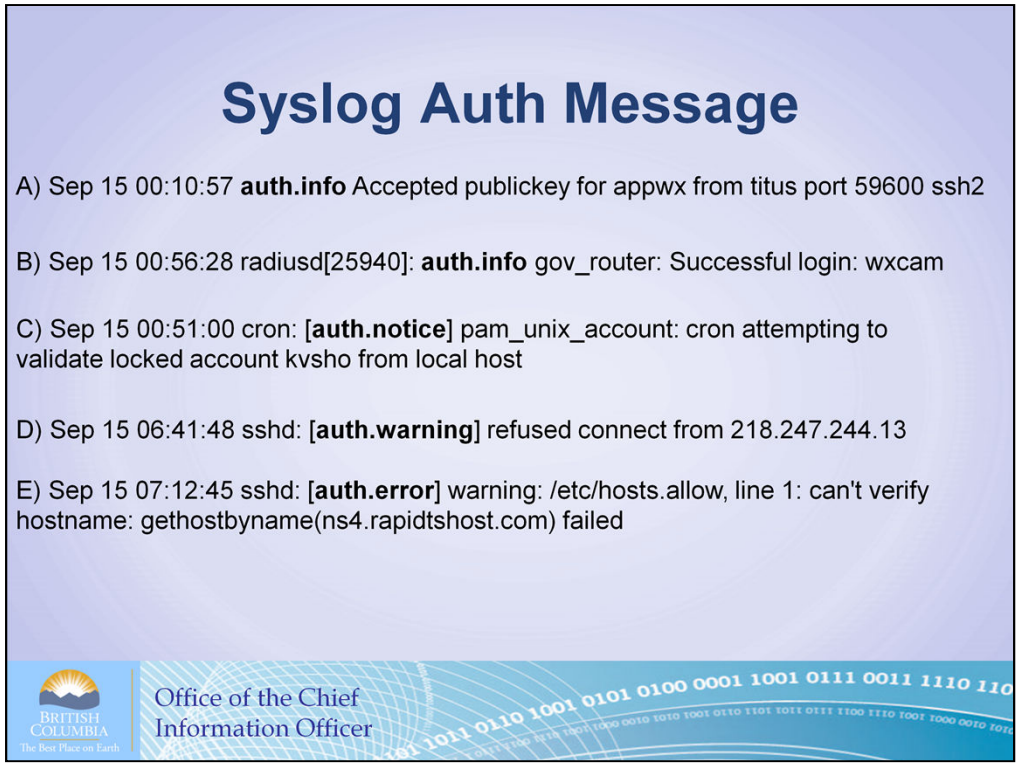
Like having a list of 24 categories to choose from along with nine subcategories (Priorities) to assign.

24 (Facility) x 9 (Priority) Matrix for a total of 216 different possible combinations.

The Priority defines the level of the importance and can range from a simple notification that everything is proceeding smoothly (successful logins) to more important messages all the way up to the EMERG message that the system is about to shut down. Usually security related messages are within the Warning, Notice and Info levels.



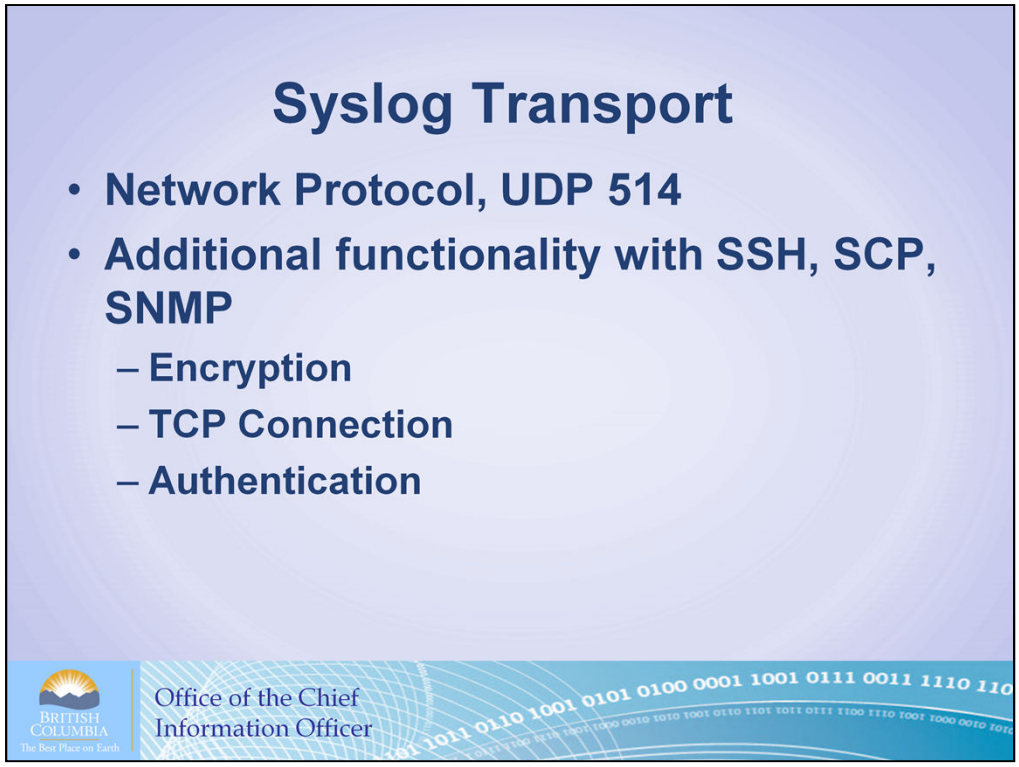
Syslog configuration file determines matches log types to files, or other output forms.



First Thing you'll notice is that the messages are readable, they are in plain TEXT and not binary or some compressed format.

Priority gradually increasing.

One of the things I like about syslog messages is that it can print the service which issued the syslog message. Examples above include radius, cron and ssh. This makes it easier to sort and group messages.



Designed to move logs over the network to Syslog Servers

Designed for use over a Secure Network, a network in which you control and administer. UDP – connectionless and clear text.

Easy to impersonate, can pretend to be another system and send logs to the central system.

Syslog is the defacto standard, widely available; most systems can export using Syslog transport and accept using Syslog format

Windows Event Log Service Re-written for VISTA / Server 2008

EVTX files are for WIN7, Vista and Server 2008, called Windows Event Log format, which is an XML format.

EVT files where for NT 4.0 and XP, very little change since NT 4.0, called Event Logging.

Like Syslog has a Severity Field called the Level Property (Information, Warning, Error, Critical, Success Audit, Failure Audit).

The Facility (Syslog – categories) is call the Windows Log File Stream and the Application and Service Logs Stream.

Two channels for logging

Channel Group **Windows Logs** (Application, Security, System) and Setup, Forwarded Events (Microsoft Logs)

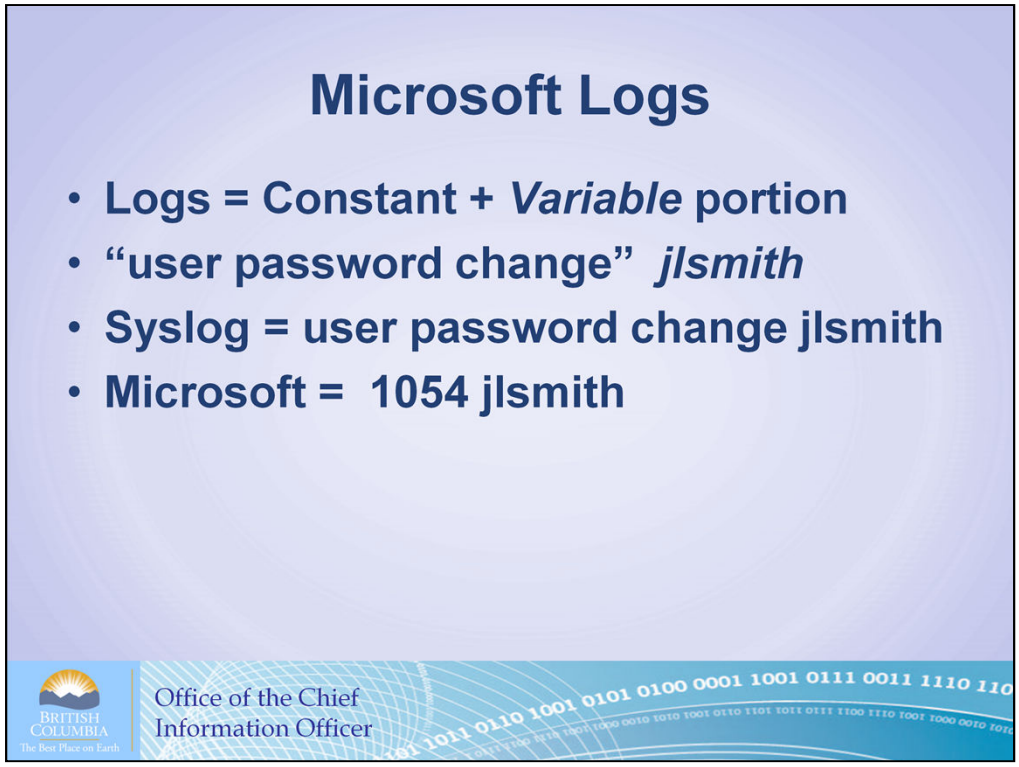
Channel Group **Application and Services Logs** (Many [Publisher Defined]) (Other vendors)

Channel Types ➔ **Serviced** (Admin, Operational) and **Direct** (Analytic, Debug).

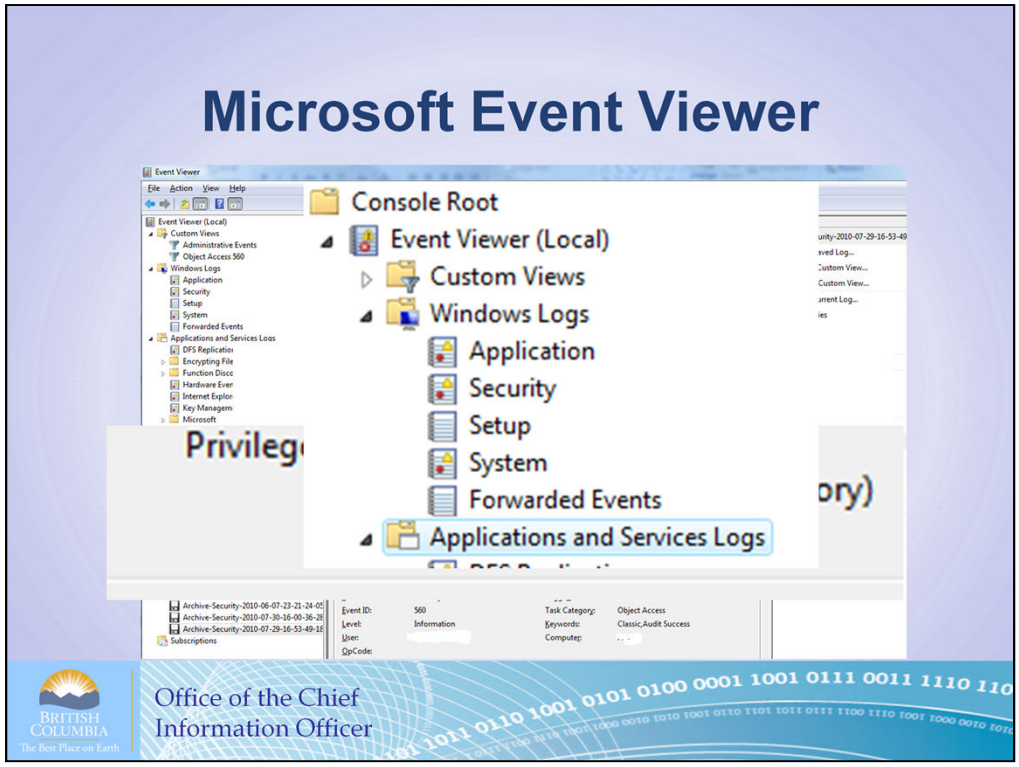
Serviced Channels can be forwarded and/or collected remotely.

Direct Channel is local only.

Can use Vista / Server 2008 Event Viewer to view EVT and EVTX logs. XP and Server 2003 Event Viewer can't read EVTX files.



This is key to understanding Microsoft Logs and why it has additional challenges not posed by Syslog.



Microsoft Event Viewer.

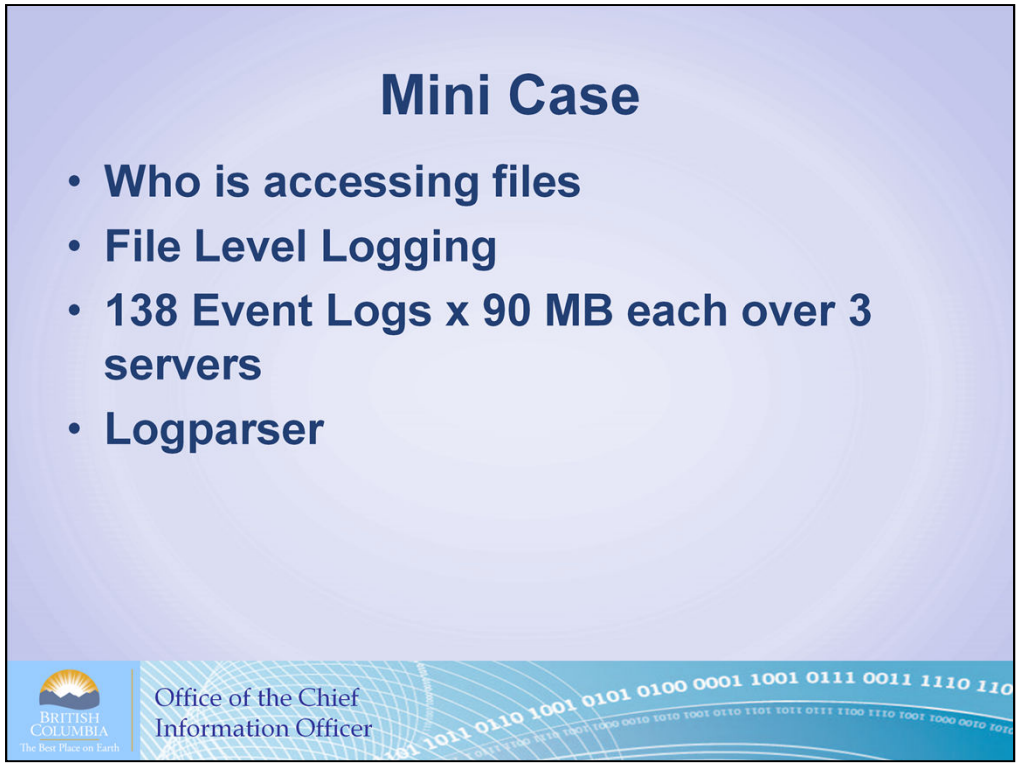
OK for searching a single file, not very good at searching multiple files.

OK for searching a structured data field (Userid, time), Unable to search unstructured Strings.

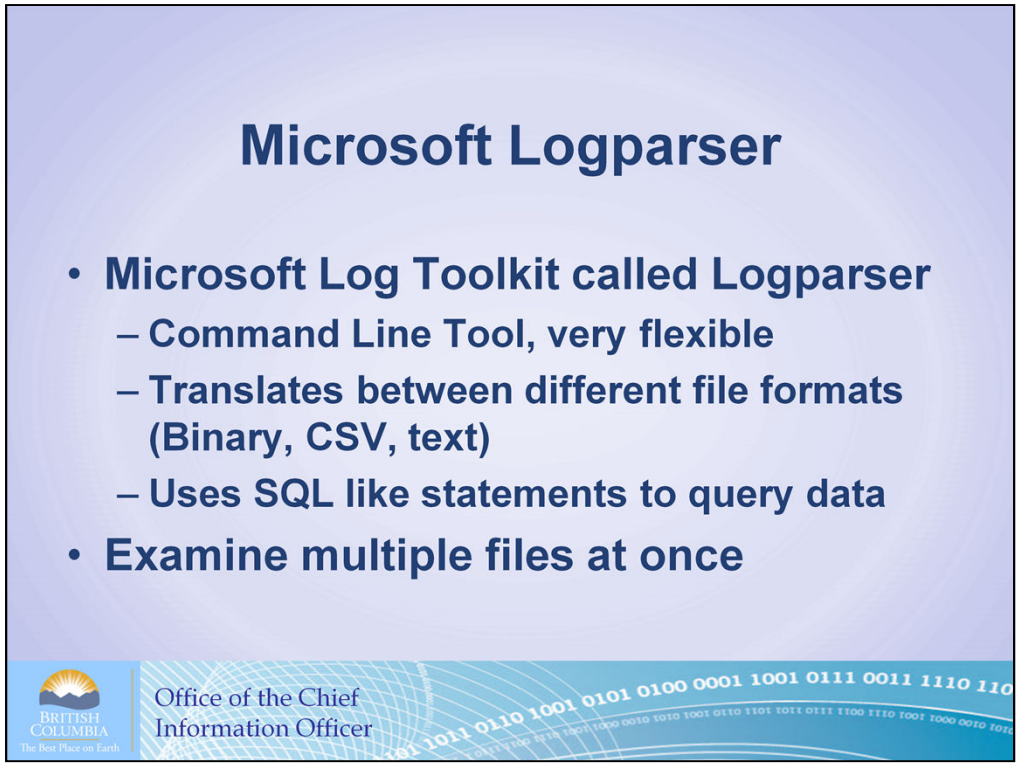
Event Logs are Binary Format and translated on the fly by Event Viewer. Error codes are translated to English.

Example, the User Privileges are DELETE and READAttributes for this directory.

If possible don't use Event Viewer. Back in 2005 MSFT produced one of the best pieces of software ever to come out of Redmend, WA. It was small (1.4 MB) command line and very quick. It's called logparser and if you do any work with MSFT logs this is the tool to learn.


Mini Case
• Who is accessing files
• File Level Logging
• 138 Event Logs x 90 MB each over 3 servers
• Logparser
BRITISH COLUMBIA
The Best Place on Earth
Office of the Chief Information Officer

Back in 2010.



Customer requested 2 months of Detailed File Level logging (Audit Object) across 3 Shared Servers.

Produced 144 Files with 13GB+ of data.

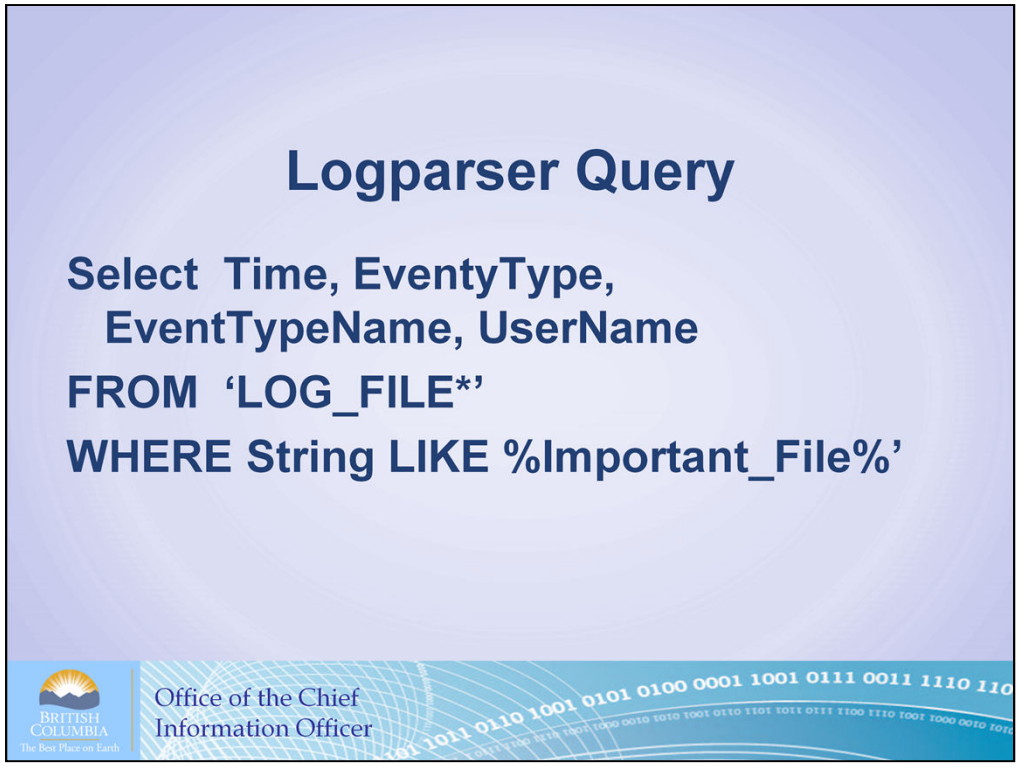
Determine who the users where that accessed selected Directories.

Event Viewer of no use here.

Microsoft Logparser much better, able to handle the job.

Designed with NT / XP environment; can only read EVT files, not the newer XML EVTX files; must convert these first with “wevtutil” program.

CSV ➔ Comma deliminated files



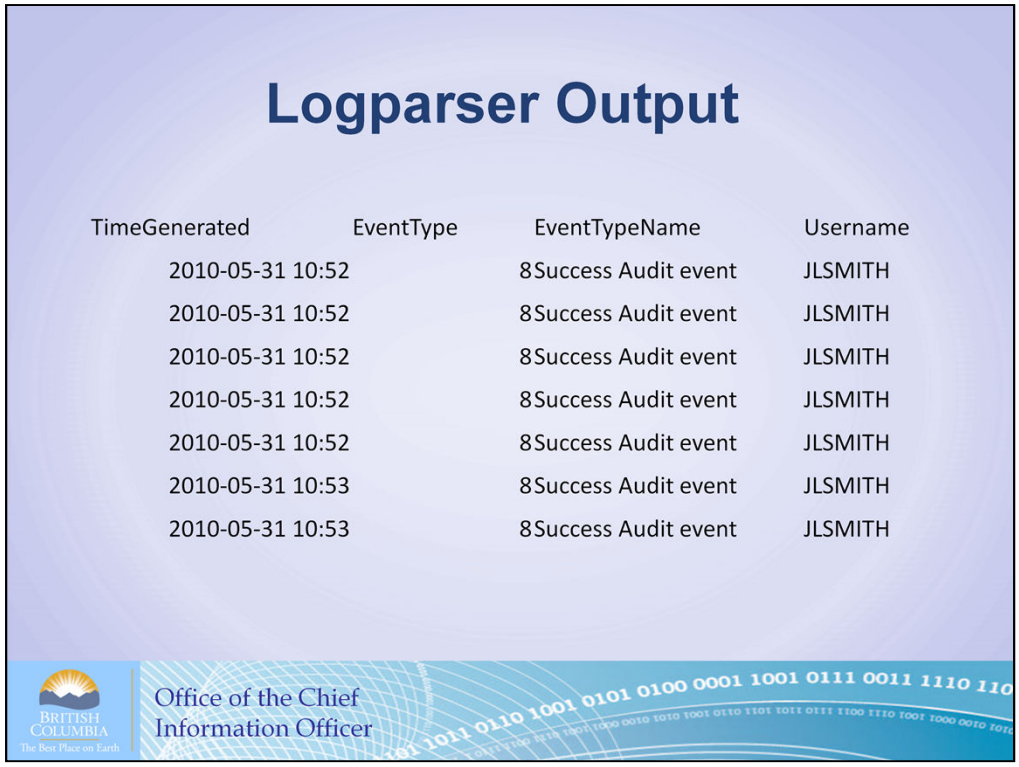
Logparser was created in 2005 and continues to be a popular download at the Microsoft site, averaging over 15,000 / day.

This is a powerful tool and a must have for anyone involved with Microsoft logs. It can even search REGISTRY entries.

Unfortunately it hasn't been kept up to date by Microsoft, so must translate the log files back to XP EVT file format. Can also use it to examine and change Registry Files.

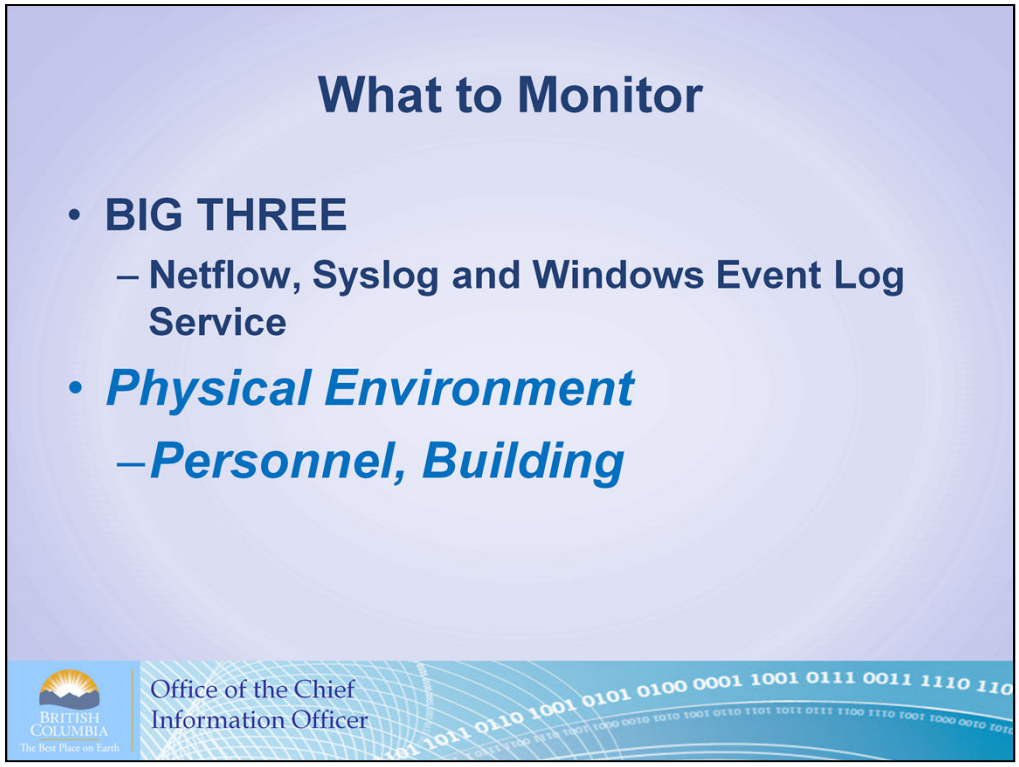
This example shows the SQL like query format.

Select some fields from a Log File and match the line under the following conditions.

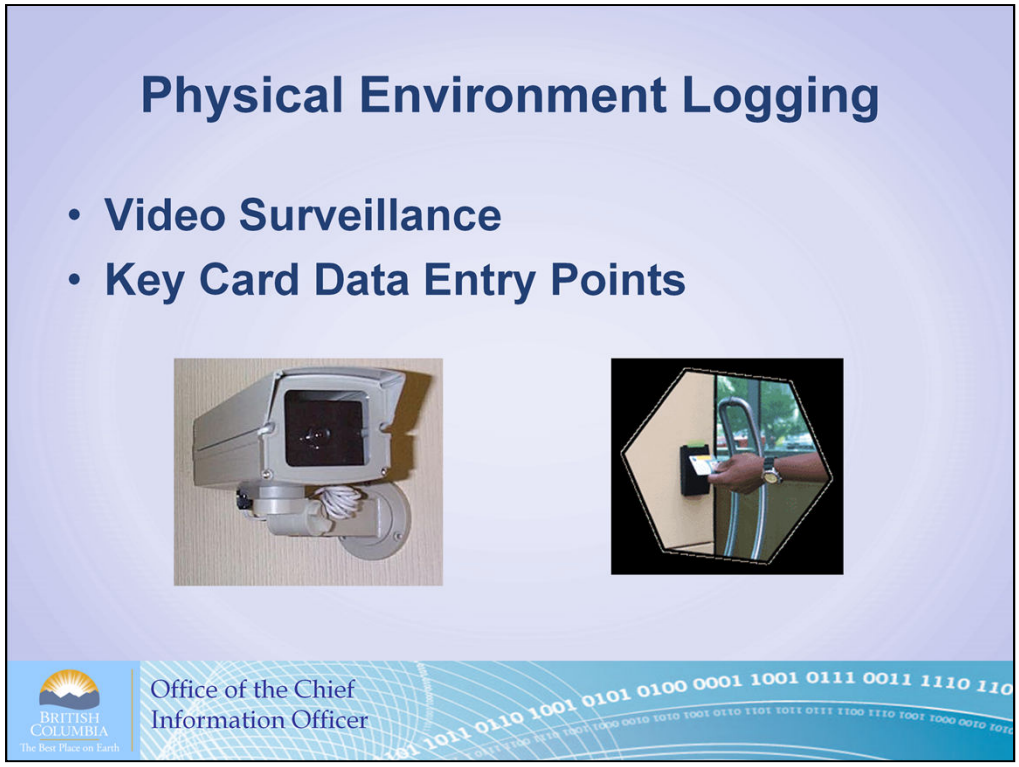


Results of the prior query.

Query from a 10GB database of multiple EVT files. Couldn't hope to do this with Event Viewer. The full query showed the actual file which was being access.



Usually Physical Security is done by a separate group from IT Security. Frequently, ex-Military or ex-Policy make up the ranks.

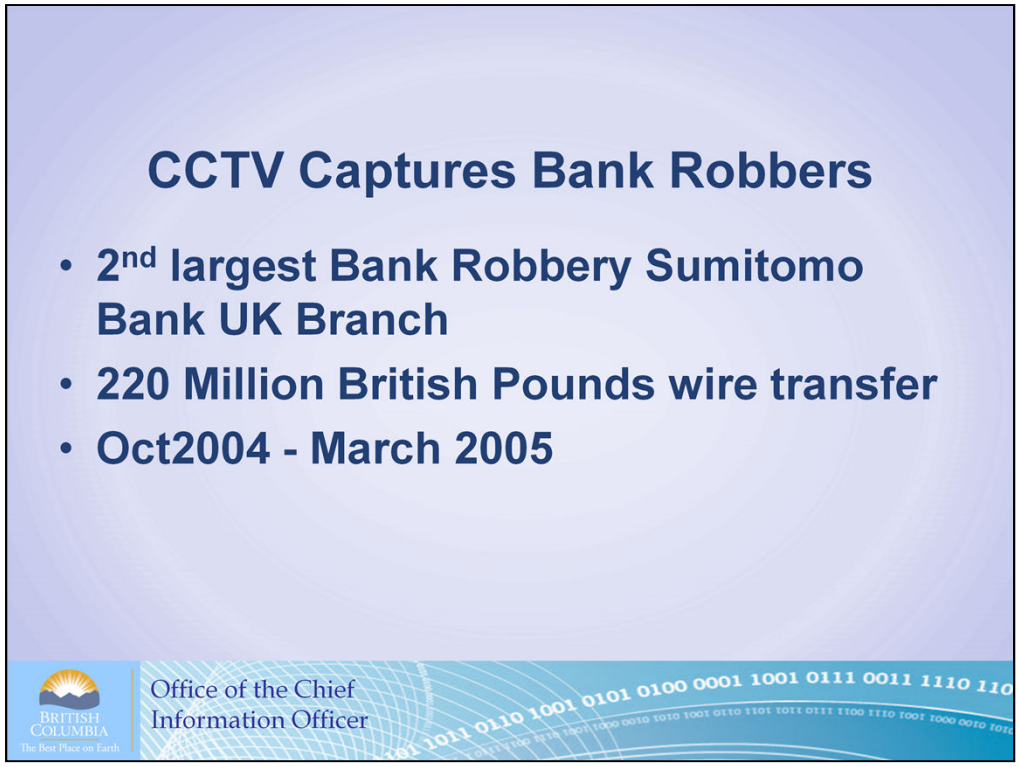


Camera characteristics – zoom, pan, night vision, resolution, sensitivity to movement. Good for outside, perimeter viewing or server rooms.

Lighting is important.

Key Cards – good for server rooms and areas with low to moderate traffic.

Not designed for busy areas or public areas.



Sophisticated operation involving computer hackers, insider who was key, planners and money transport and laundering.

Banks CCTV camera's triggered by motion sensors, but the sensitivity was turned down on all. The Security supervisor missed 2 or 3 which caught the individuals on tape.

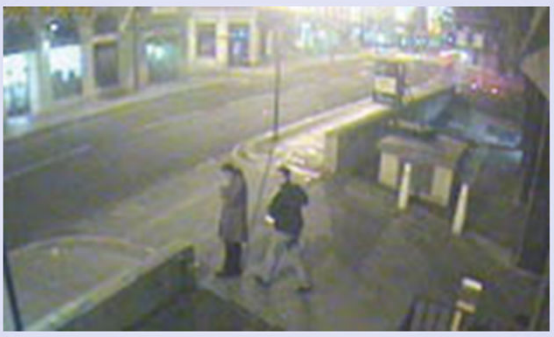
Phone call records further linked the Security supervisor to the Belgian hackers.

Keylogger application called Iopus Starr placed onto bank systems.

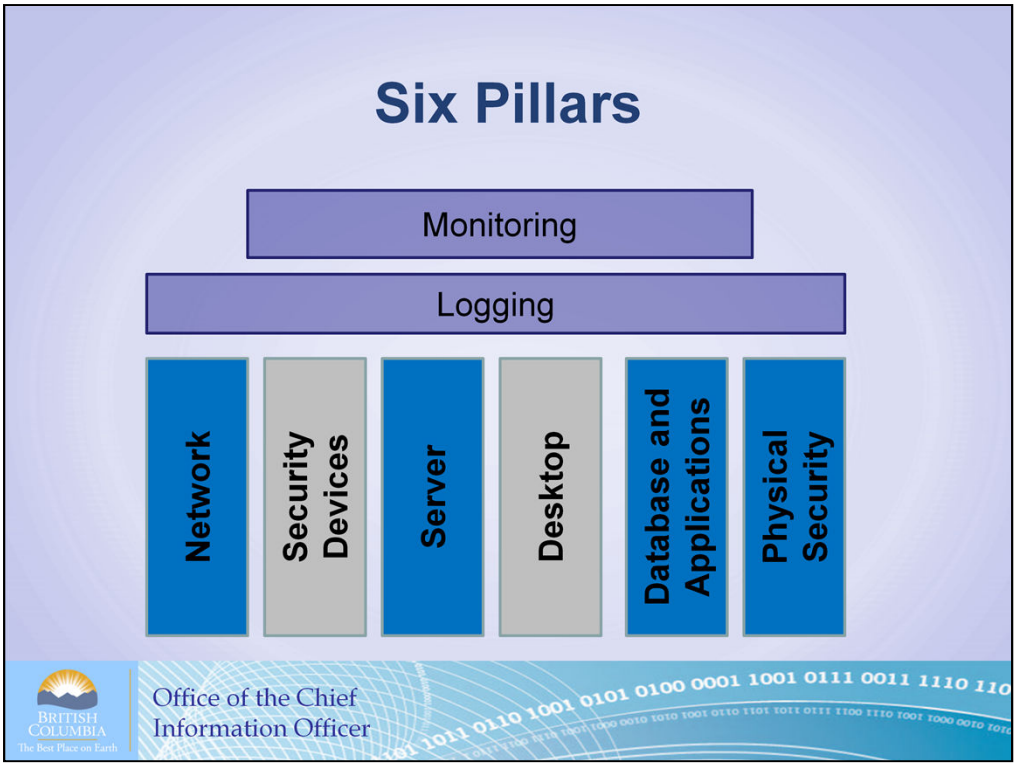
Stored the screenshots and recorded keystrokes onto a file on the PC. Sophisticated enough to avoid the Anti Virus software. No transfer across the network, so network monitoring didn't detect anything.

Foiled due to a coding error placed in the SWIFT banking system. The remote banks asked for confirmation due to the coding error, but the crooks had already cut the computer cables and disabled the desktop systems. They never saw the request.

The Hackers



The Two Belgium Hackers caught
On CCTV outside the Sumitomo Branch



Review of the different environments that can be monitored.

Good data (logs) will improve the monitoring.

Poor data or no data will result in poor monitoring or no monitoring.

Building Monitoring Systems

BRITISH COLUMBIA
The Best Place on Earth

Office of the Chief
Information Officer

Similar to Making Whiskey

This is the slide to see who's awake!

My neighbour makes a lot of wine, 30 tons of California Grapes every year.

Another neighbour makes whiskey at a store.

I've got a nephew who's taking Viticulture (Winemaking) course at college.

Last week I was thinking "what would a 20 something year old relate to" and right away wine, beer and spirits came to mind. The more I thought about Logging and Monitoring system the more similarities came to mind with distilling spirits, wines and even natural health drinks such as Kombucha which undergo a fermentation.

Six main checklist components are required to design a well though out monitoring system and keep it running.

You will need to know the legal ramifications of monitoring, a systems architecture for successful monitoring, storage requirements, time issues and a standard time framework, data analysis techniques and structuring reports to match different audiences.

Corporate Policy of Monitoring for Virus's, Worms, Hackers, Network Operational traffic

Employees know that their traffic and usage patterns are being collected as part of normal operational processes.

Telecommunications Act of1993 replaced the Railway Act of 1906 which governed Telecommunications prior to 1993

Bill C-176 Protection of Privacy Act

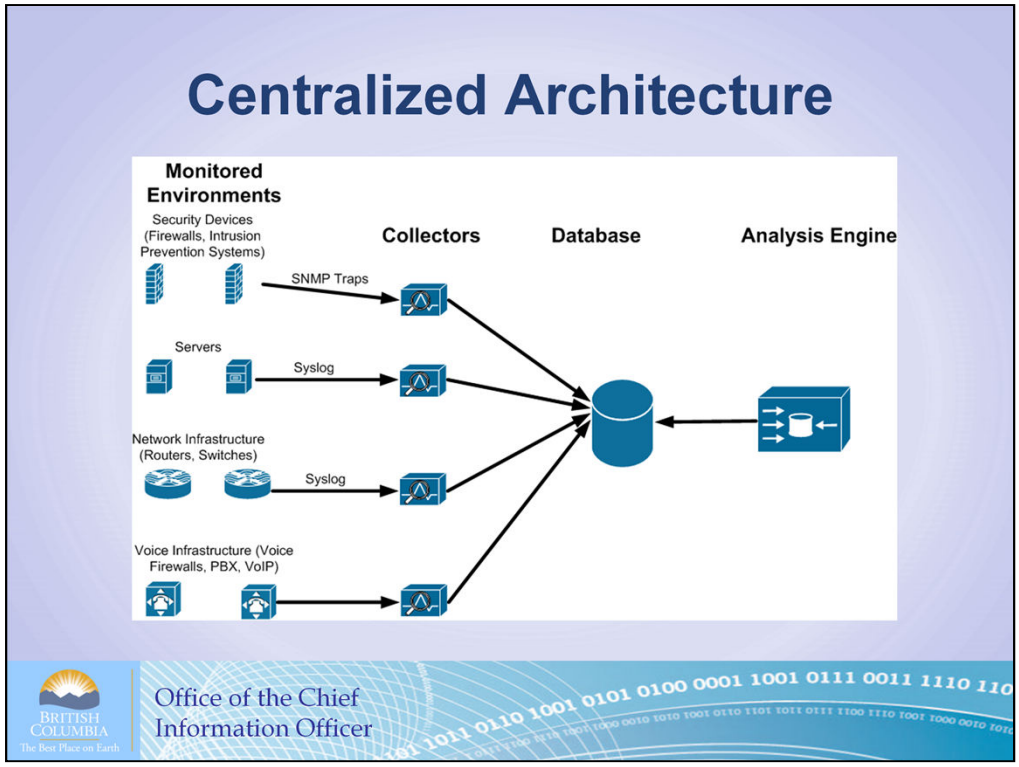
Bill C-46 Criminal Code of Canada; Section 342 deals with theft, forgery or credit cards and unauthorized use of computer

Keep notes if investigating an employee.

Should be aware of the following two Bills

Bill C-46 - Gives Police the legal framework to get Search Warrants for electronic evidence, Production Orders (similiar to Search Warrants).

Bill C-47 – Telecommunications organizations must be able to monitor (Wiretap) calls on lots of different environments (Cellular, LandLine, VoIP).



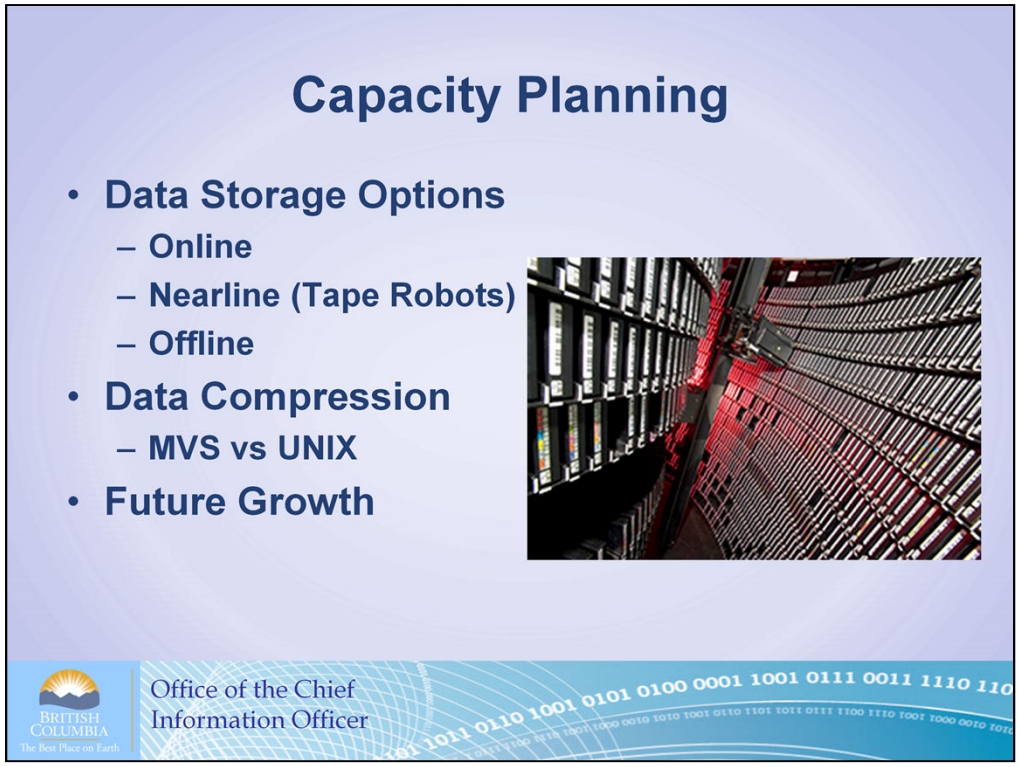
Three Tier centralized monitoring system with Collectors, Database and Analysis engine.

Data is supplied by the Monitored Environments to the Collectors, which are tuned to accept, parse and normalize the data prior to sending it to the Database. Collectors receive the data real time, the database can be updated at intervals. Analysis can be performed either real time or Reports are run daily, weekly or monthly.

The environments being monitored are based on IT categories security devices; Servers; Network Infrastructure and Voice.

Just as easily it could be based on Geographic region such as monitoring Victoria, Sook, Langford, Colwood and Sydney.

Or by Business Type --- PCI Monitoring;



Often logs are determined for you and everything comes your way.

Logs – real time or archived, determines the processor requirements.

Logs can be long term archiving to satisfy auditors or compliance folks.

Logs can be reviewed to assist with current investigations and determine scope of incidents.

Data can be stored Online (HD), Nearline (Tape Robots) or offline (manual intervention).

Data Form – data can be kept in raw format, compressed, aggregated

Future Growth - Our Internet rates have been doubling every 3 – 4 years. However the system is built it should be built with the expectation that storage requirements will go up 10 fold in 10 years.

BC Government ➔ 1 TB holds 7 days of Netflow Logs

Central Log Server must be secure, depending on the organization this can be:

•Minimal access and services running on the Central Log Server

•Located in a secure zone

•Data is encrypted

•Hash value is taken of the log files

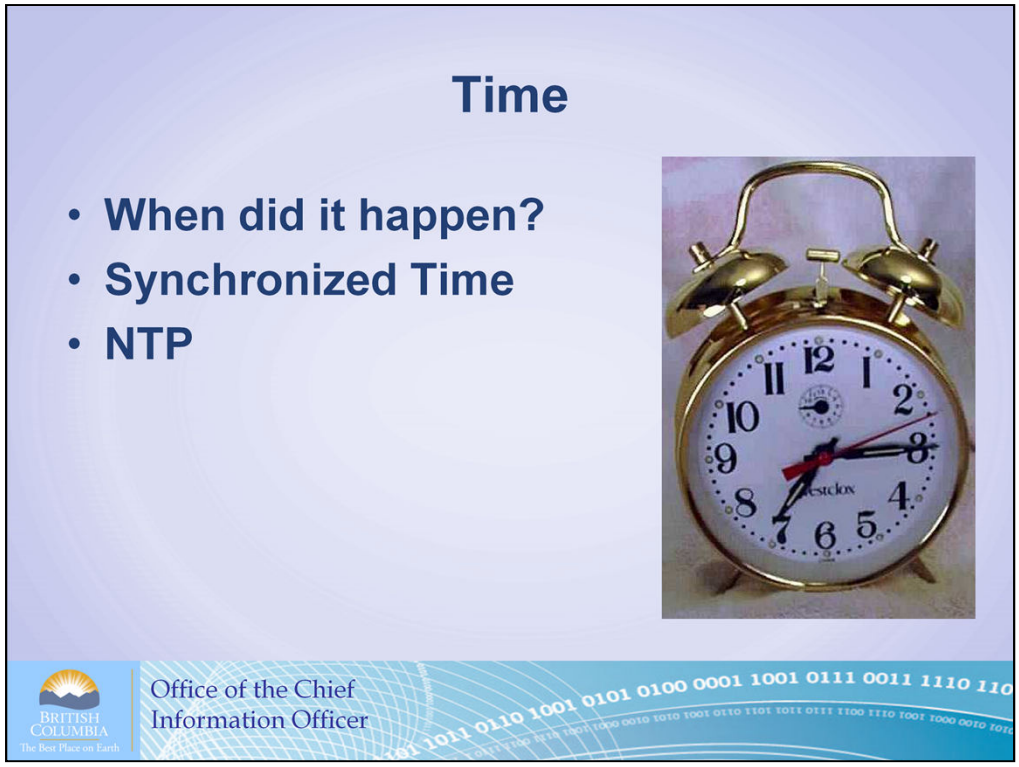
Local logs are kept for regular operational purposes and for comparison to see if any logs changed on the local system or if all the logs sent to the central system.

Know the retention period for both the local logs and the Central Log server,

How long do you need to keep the records (Company Policy); 1 week, 1 month, 1 year, 5 years;

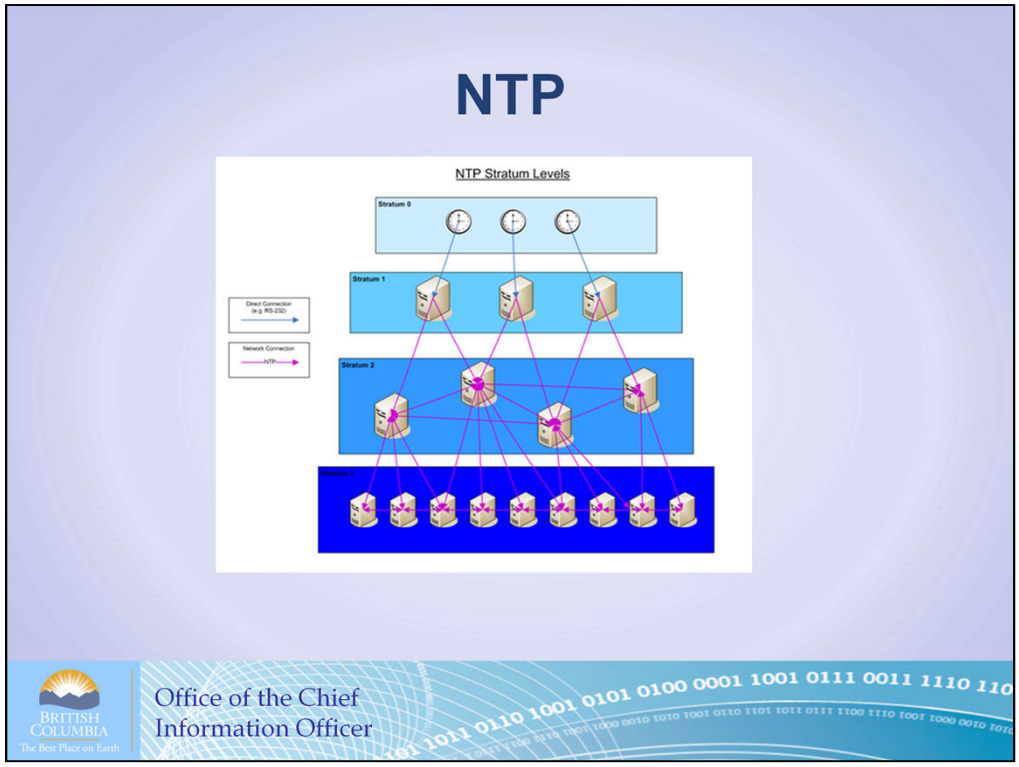
Which records need to be available real time, which can be archived? Usually based on a time (under 6 months real time, over 6 months Archive)

Can older data be aggregated instead of keeping single records?



The important thing is not the actual time but the fact that all systems are synced to a common time source. This way a sequence of events can be determined.

The most common source of time today on the Internet is through the Network Time Protocol (NTP).



Based on ATOMIC CLOCK time.

Stratum 1 servers are attached to Atomic Clocks (Ceasium), public ones are the US Military, Canada's National Research Center.

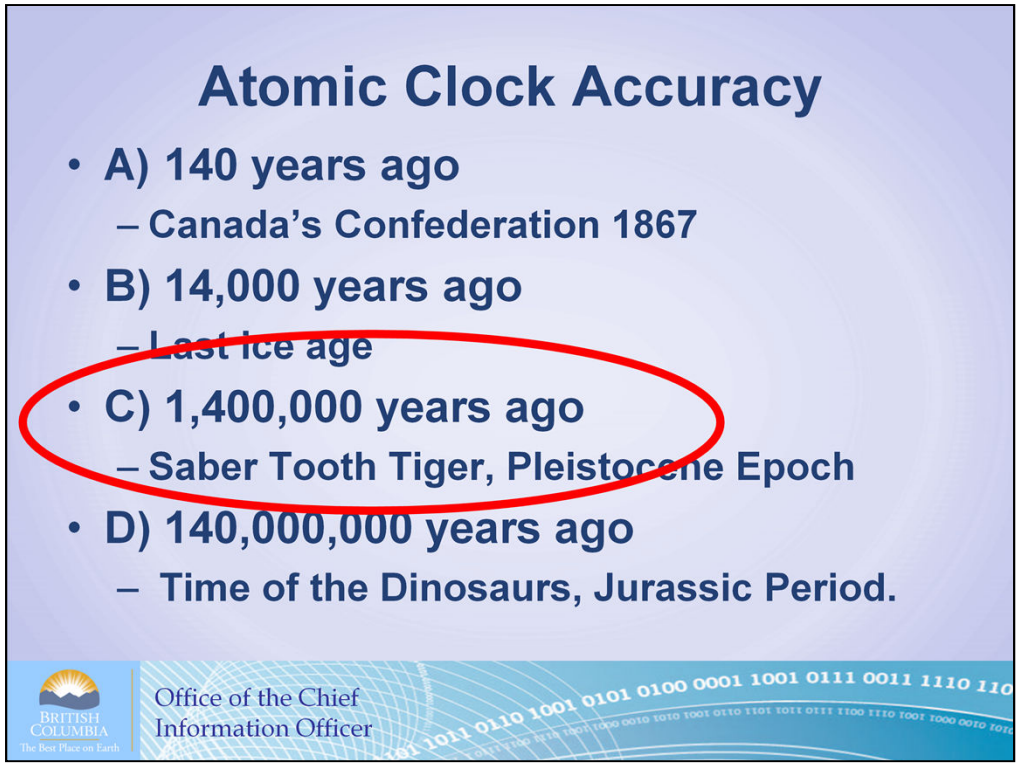
What is the accuracy of Atomic Clocks? Ceasium has an oscillation frequency of 9 192 631 770 Hz, which defines 1 second. Accuracy is 1 second different every 1,400,000 years.

Large Centers like University's act as Stratum 2 servers and serve information regionally.

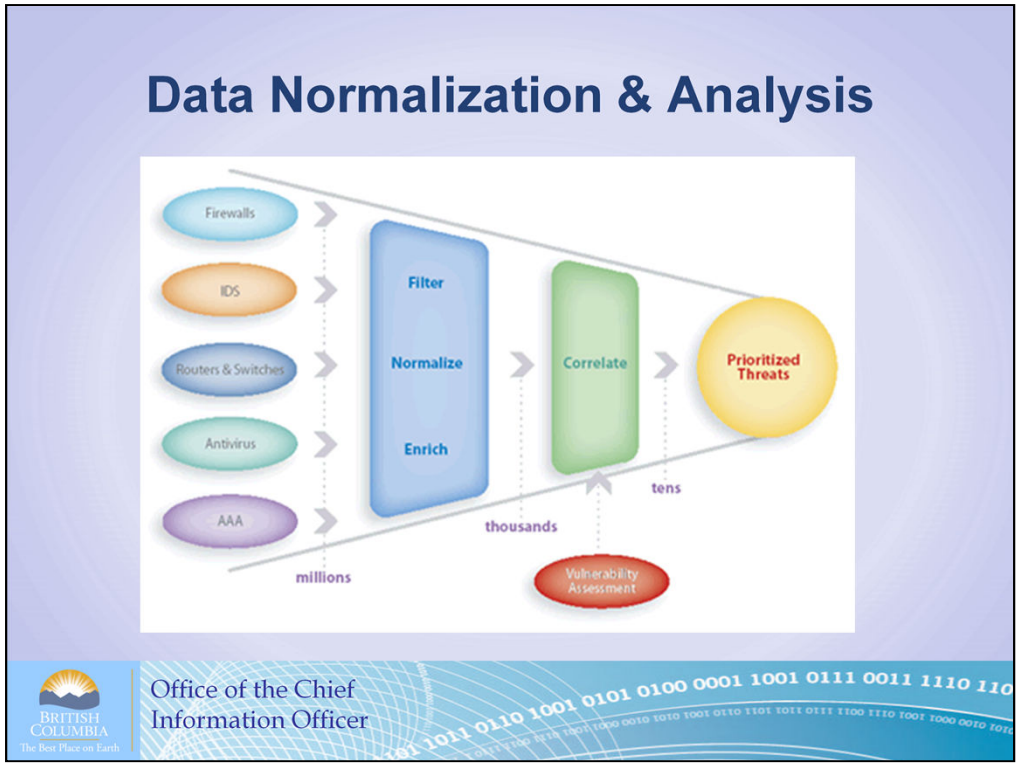
Many Level 2 and Level 3 servers will propogate downwards to other servers within their organization.

SPAN/BC has 2 Stratum Level 2 servers which serve the rest of the network routers (Stratum 3) that in turn serve the main UNIX / Microsoft Time servers (Stratum 4) that other PC's and UNIX devices rely on (Stratum 5)

.


Atomic Clock Accuracy
• A) 140 years ago
– Canada's Confederation 1867
• B) 14,000 years ago
– Last Ice age
• C) 1,400,000 years ago
– Saber Tooth Tiger, Pleistocene Epoch
• D) 140,000,000 years ago
– Time of the Dinosaurs, Jurassic Period.
BRITISH COLUMBIA
The Best Place on Earth
Office of the Chief Information Officer

Pop Quiz



Variety of different log sources that must be reduced. Mostly log systems are single focused – just firewall logs, just router logs, just server logs.

Some of the more complex monitoring systems take logs from many different sources and require the data to be normalized – or changed into a common format where analysis can be done.

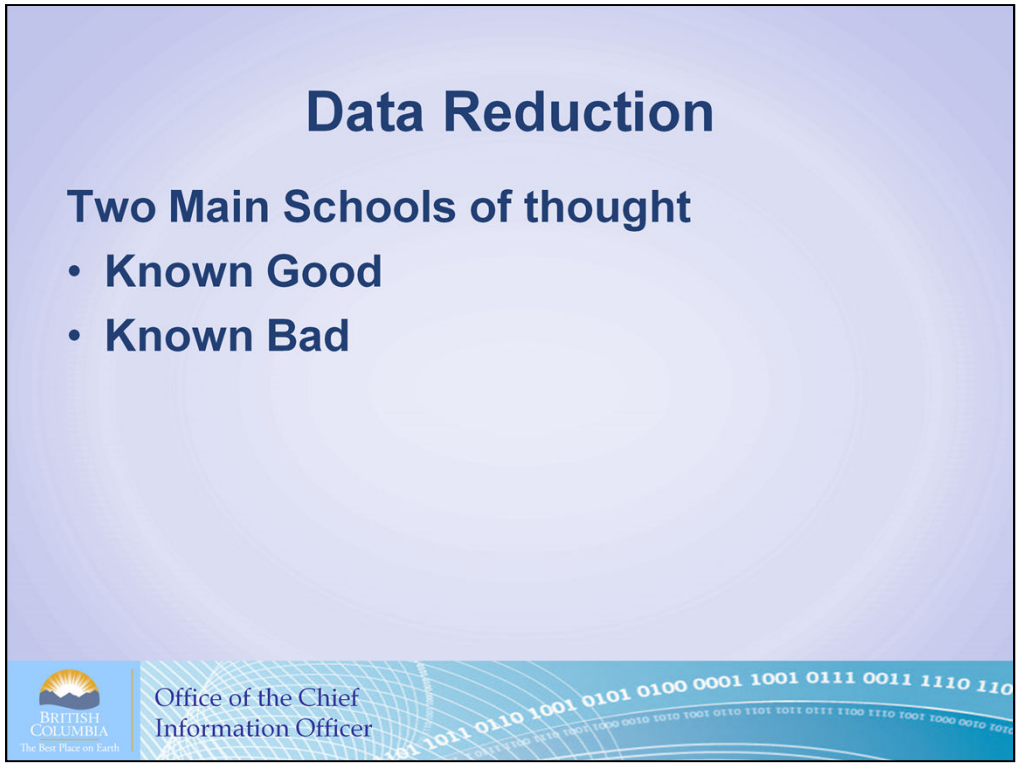
Millions of events need to be reduced to a manageable amount that can be acted upon.

Reduce Events and Correlate

•Filter - Remove Non Security Events

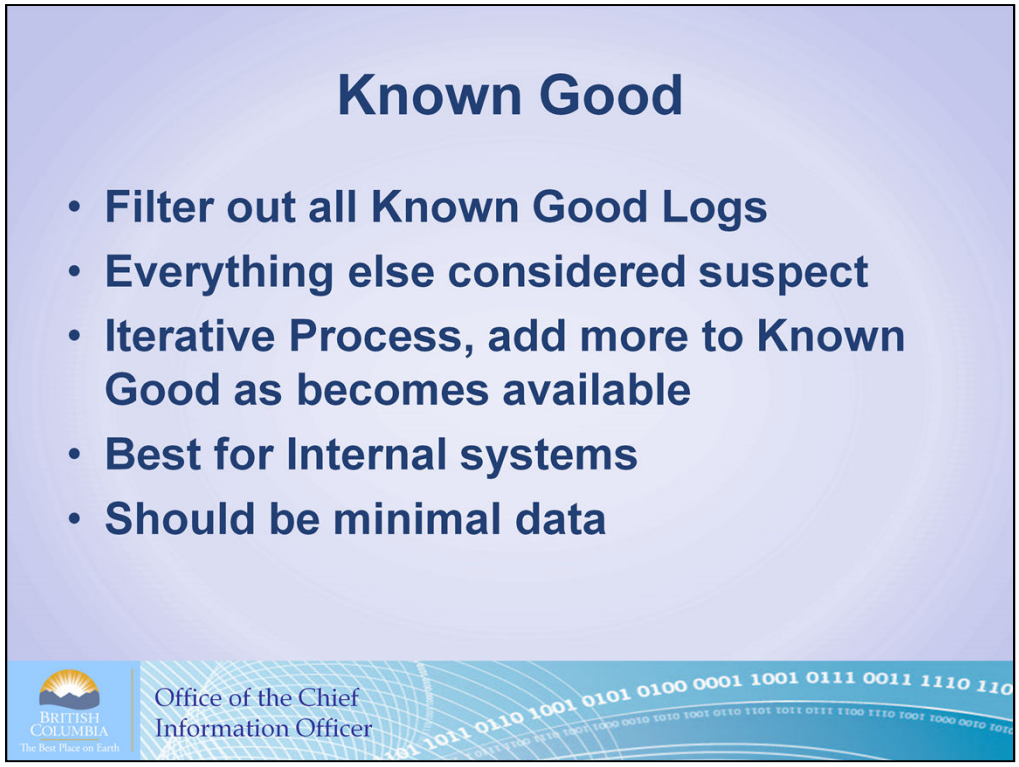
•Enrich – add data where it is missing, such as date timestamps (including year), host system.

•Correlate – determine common patterns across different systems (servers) or between different platforms (routers, servers, security devices).



To me this is the interesting part of Monitoring – writing queries to determine what are suspicious events.

This is the KEY ASPECT for MONITORING as opposed to LOG COLLECTION. Monitoring is really about DATA ANALYSIS for Security staff or administrators.



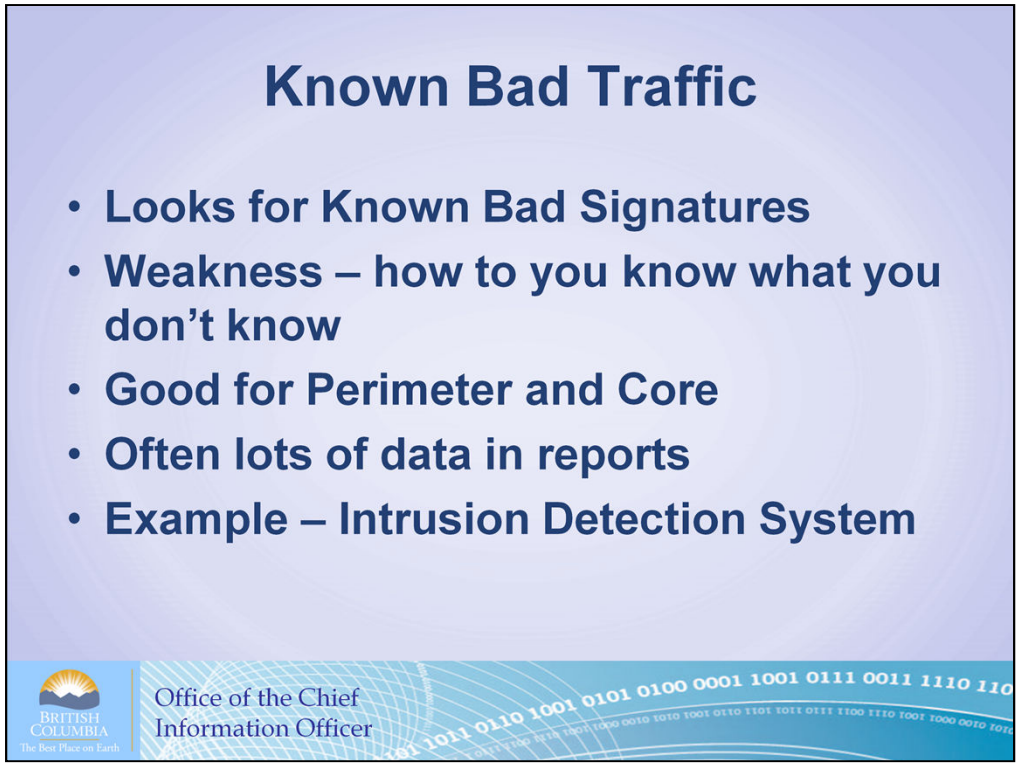
Filter out all Known Good Traffic, everything else is considered suspect.

Add additional log information to known good traffic as it becomes known. Malformed logs, new systems coming on line, staff changes.

Best used for Internal system

Examples – Firewall logs, Firewalls allow in known good traffic and block everything else.

Should be minimal data at the end as most logs are legitimate.



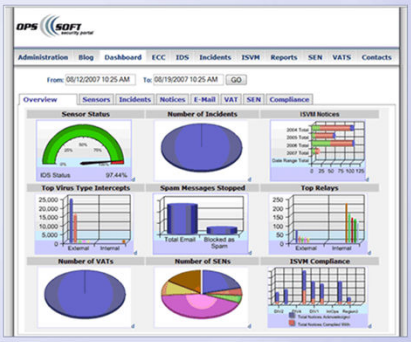
Examples include Intrusion Prevention Systems (IPS) blocks known BAD Signatures and lets everything else through.

Best used at the Perimeters and within the Network Core.

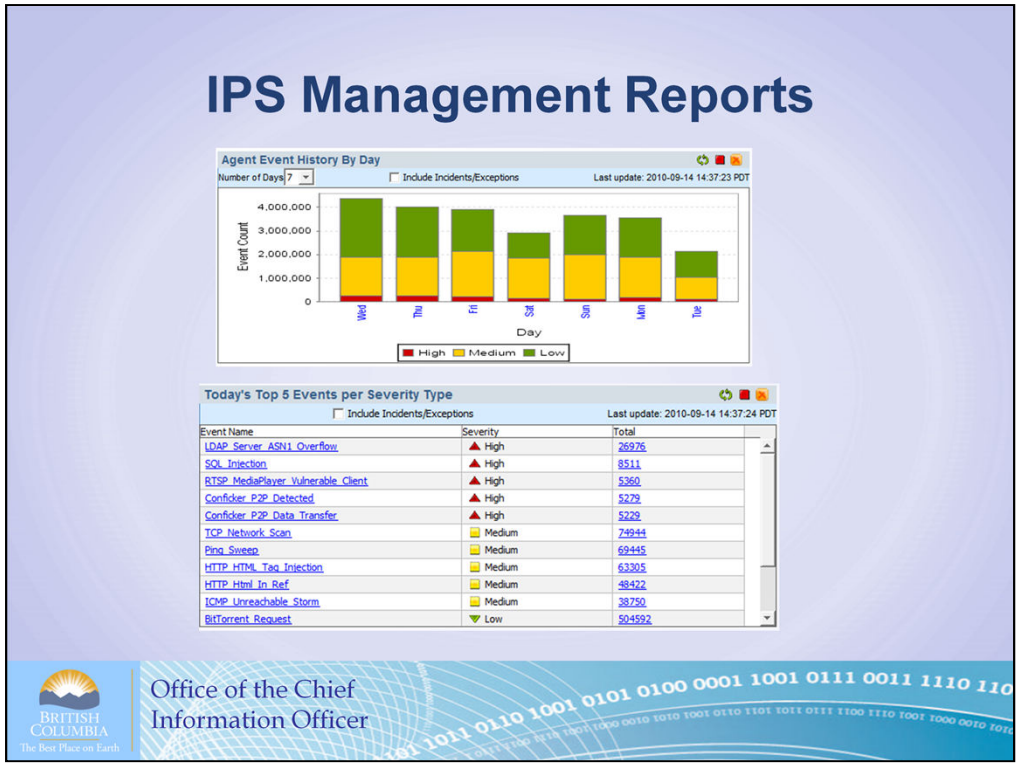
Should be lots of logs, often these systems are filtering out high volume traffic or attacks.

Reporting and People

- **Reports**
  - Tailored to the audience
- **Process**
  - Dedicate resources

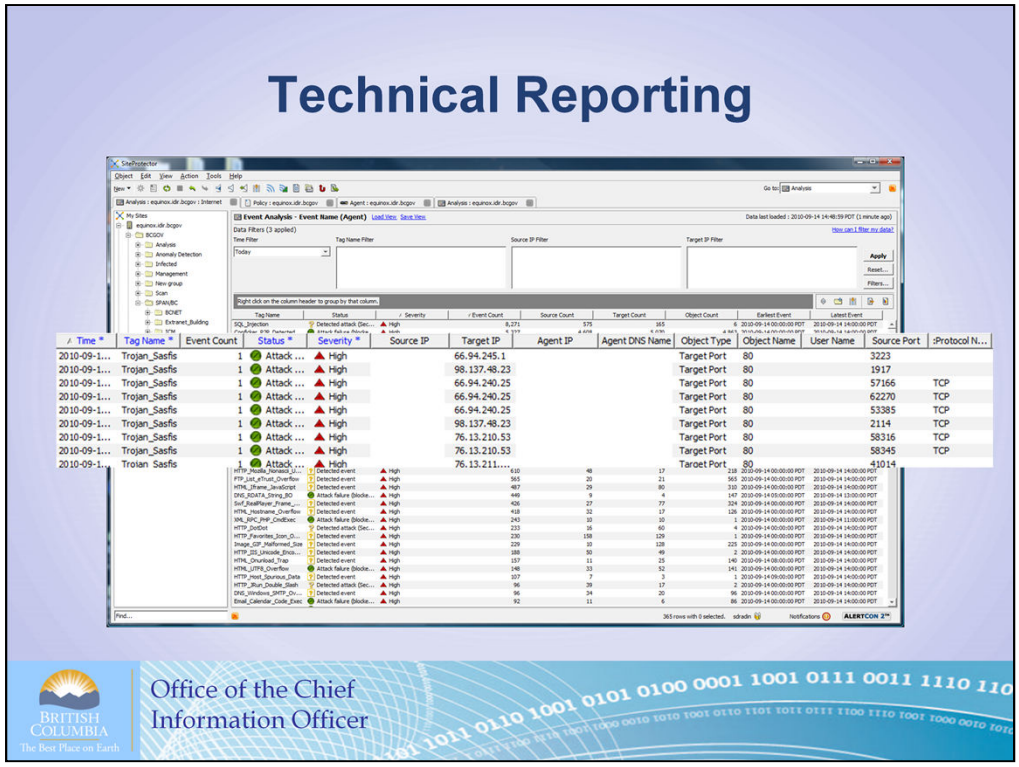


Matching the reports to the audience.



Management wants to have a high level overview, not because they like pretty pictures or colours. Not because of limited math capabilities.

Graphs and charts are useful for persuasive purposes to gain either more money, resources or staff. It can also be used to show that something is working smoothly or as expected.

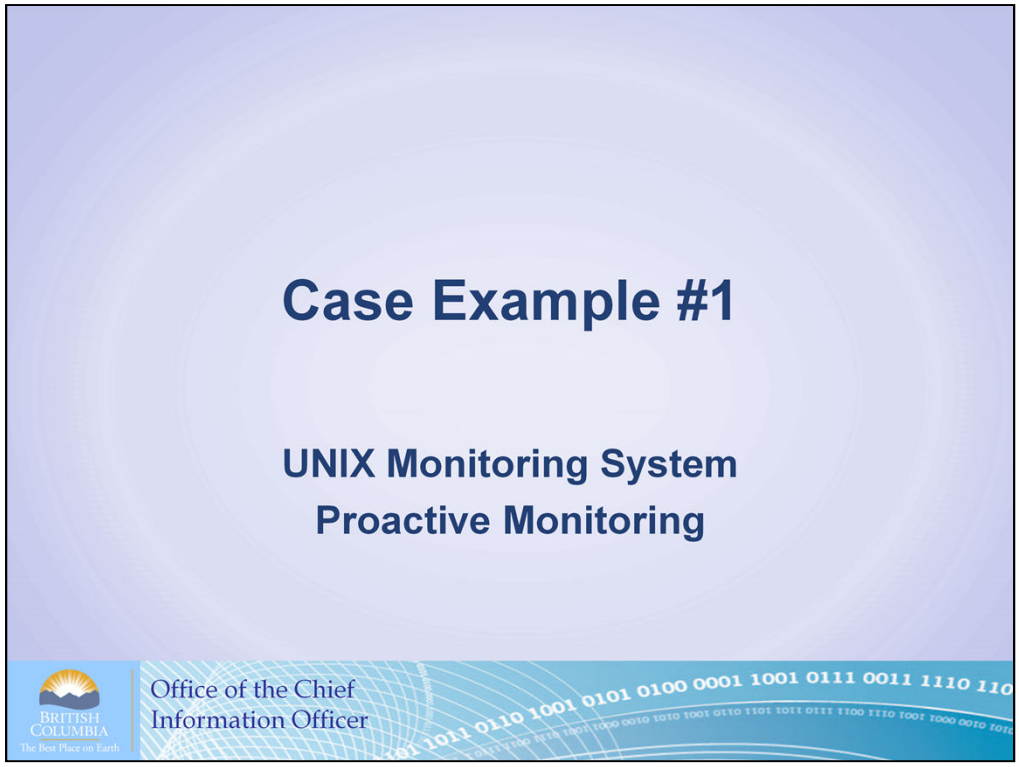


Daily Reporting

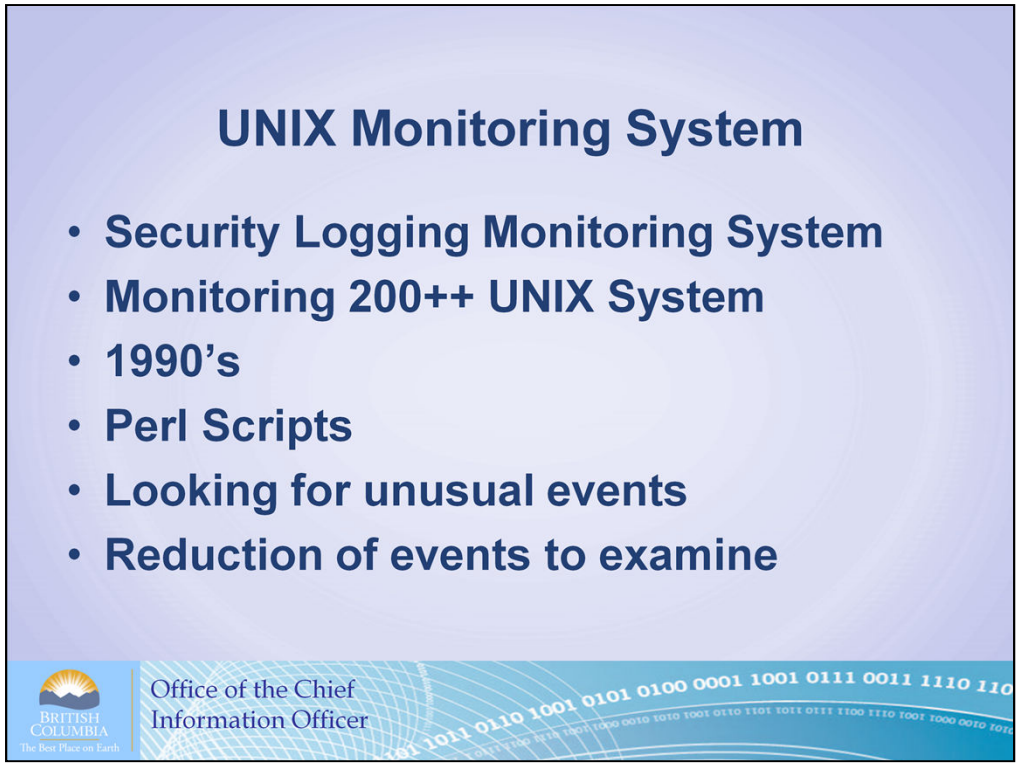
Really a very limited reporting capability. This is doing little more than sorting log files by attack type. It is not something which would generate a list of interesting traffic for further investigation on its own. Rather, it would be used to assist or find additional data for a current investigation.

Staff can be either dedicated Organizational Wide Staff and or administrator level staff.

Documentation – one person leaves, don't want to rebuild the wheel.

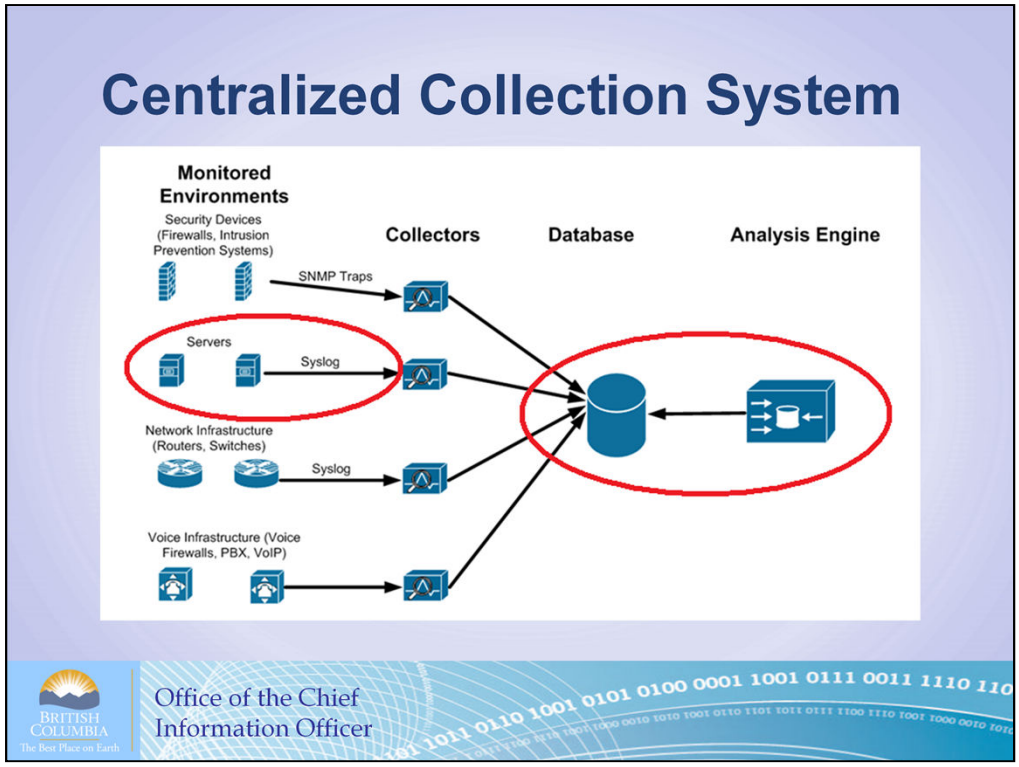


Firefighting – Unplanned Monitoring system, get it up and running quickly.



Planned Monitoring System - this system was written in response to an Audit which identified a weakness within the UNIX logging environment.

I wrote it in the 1990's a few years after graduating from UVIC. It has approx 3,000 lines of code using Perl.

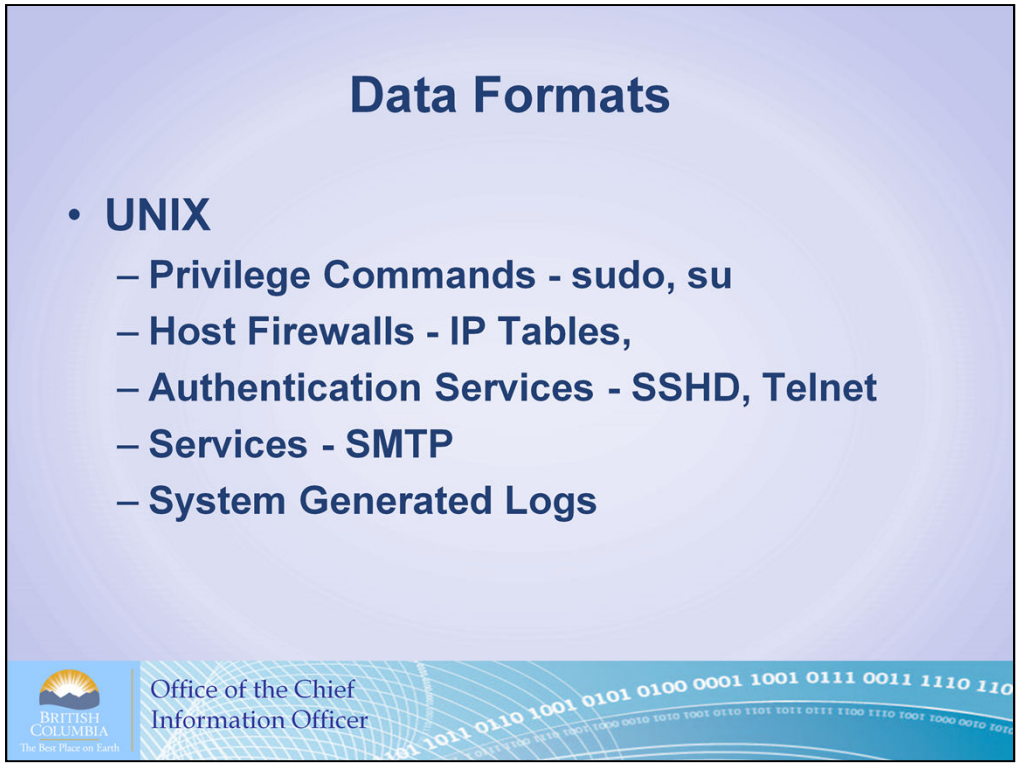


Based on the Syslog format. It was a single platform system – UNIX Servers – with no integration with Network Security Devices, desktops or routers.

There was another identical system written for the UNIX desktops at the time.

The syslog entries where sent to a central server, which can be thought of as a collector holding the raw logs. Then these logs where parsed and normalized by the Perl Programs and placed in a file with standardized fields. Reports where then run off this database.

Where possible data was aggregated. So if a single event occurred 10,000 in a day it would be rolled up as 1 line indicating the event and the number of occurrences.



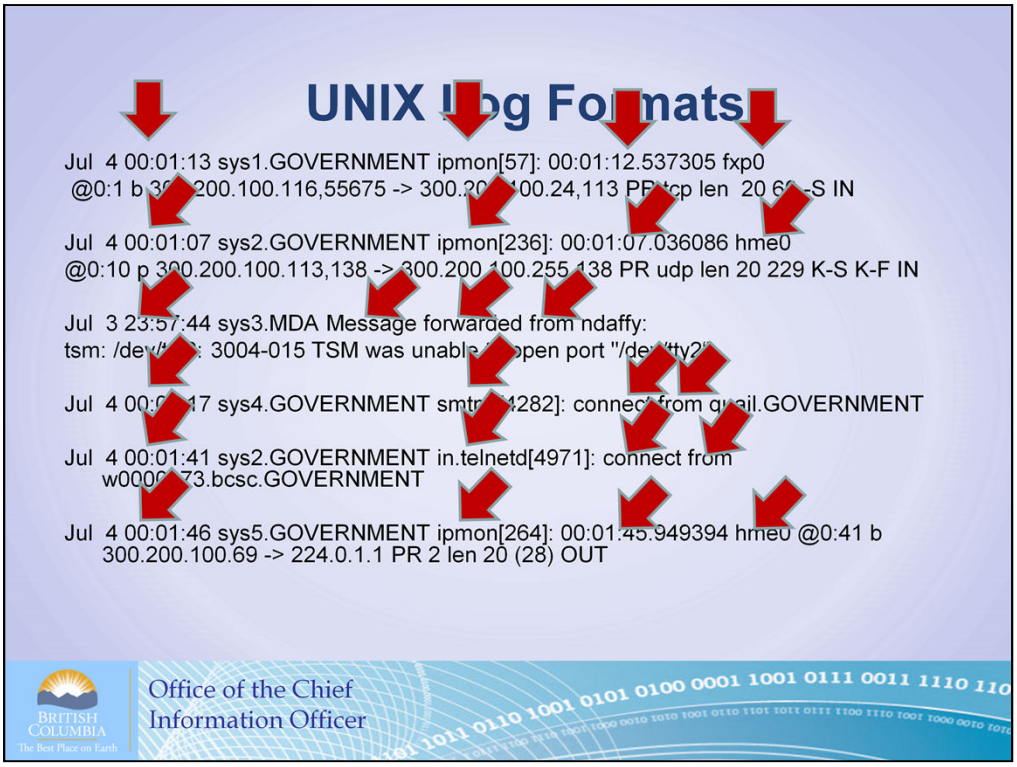
Many types of server logs – 17 different formats in all, this required normalizing.

Privledge escalation commands – su, sudo

Server Firewall Logs – IP Tables

Authentication - SSH, Telnet
Services - E-mail SMTP

System Generated Logs



Fields 1, 2, 3 all pertain to Date and Time

Field 4 is the system

Field 5 is the service (mostly)

Field 6 is TIME for IPMON,

"connect" for smtpd and telentd,

"forwarded" for tsm,

Field 7 is the network Interface for IPMON,

"from" for smtp and telnetd

"from" for tsm

IPMON has lots of fields (20), telnet has few fields (8),

IPMON has some fields which need to be split into two fields "300.200.100.24,113". The 113 is really the port number or service.

This is only for 4 different formats. Most heterogenous environments will have 20+ different logging formats; notice that the first 4 or 5 fields are consistent thanks to Syslog formatting.

Are you familiar with the IP address 224.0.1.1

FL = Field

Normalized the events into 8 Fields

Field 1 ➔ Repeat counts for that day, all other fields being equal

Field 2 ➔ Status Report (Success or Failure)

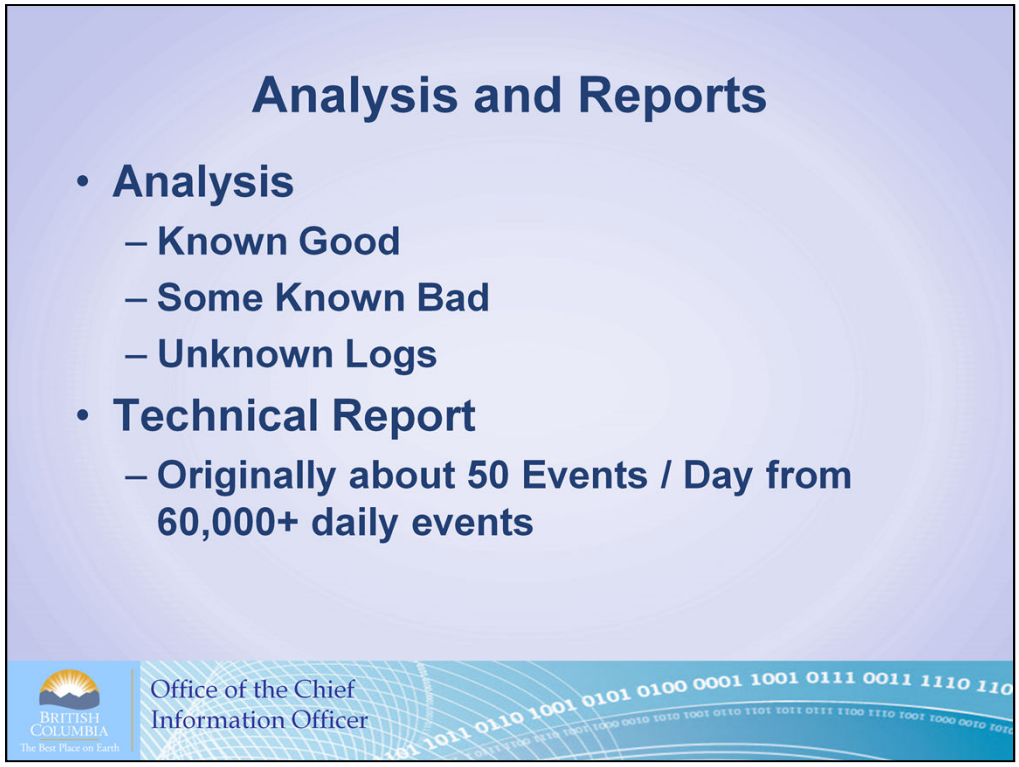
Field 3 ➔ Service or application producing the report (DialNet Application, TCP_Wrapper, Klogind, login – maybe just done for root logins).

Field 4 , 5, 6 ➔ Date and Time

Field 7 ➔ System producing the log or pertaining to the log

Field 8 ➔ Event captured by Service or Application (login, ftpd, telnetd)

Field 9 ➔ Source Address for remote connection



The servers where predominantly internal ones so there was a lot of filtering using Known Good Filter.

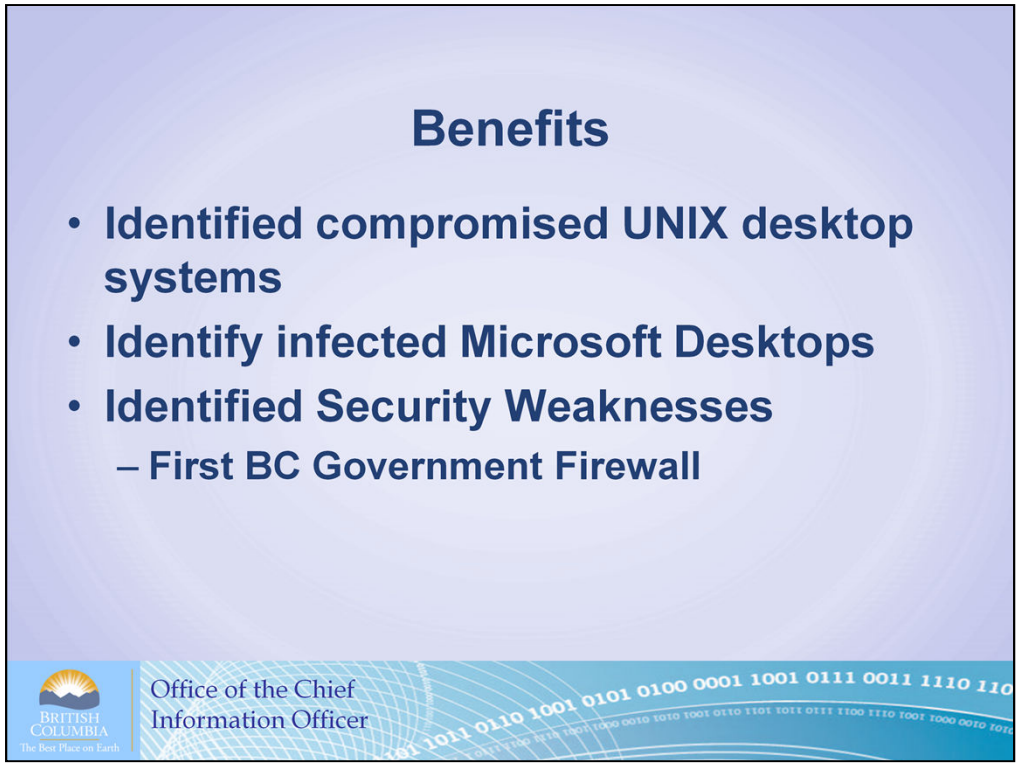
Some known Bad – especially any connections that occurred from outside of the secure network.

Broke data down into different reports :

Authentication – Telnet / FTP / Kerberos / SSH

Privilege Access – SU / SUDO

Remote Access – Radius / VPN

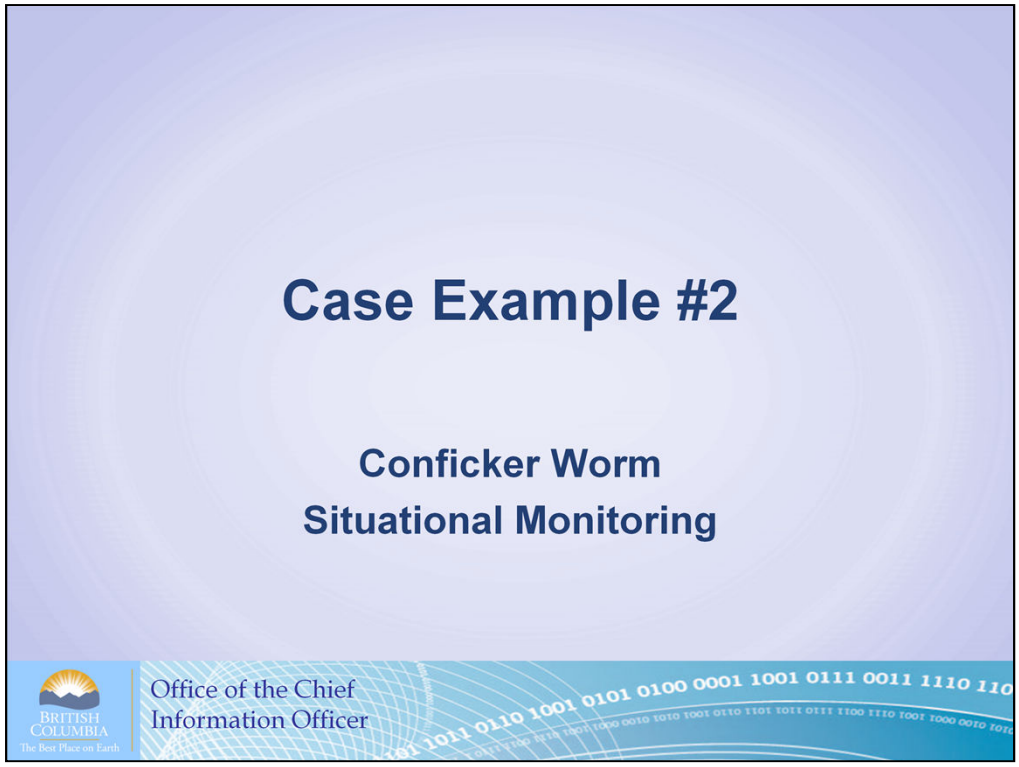


One of the cases involved a desktop that had been compromised back in the 1990's. Most of the desktops and servers had a trust relationship, so they could be RLOGIN. The local logs where all on individual systems and it would have been very difficult to log into each system and parse the logs for suspicious activity. The start date of the attack was unknown and the local logs where usually rolled over every month.

Using the centralized log database it was easy to query all the logs quickly and determine suspicious logins from the site in Italy. It was also easy to identify when the first occurrence happened and what the compromised machines did afterwards – which connections they made and who made those connections.

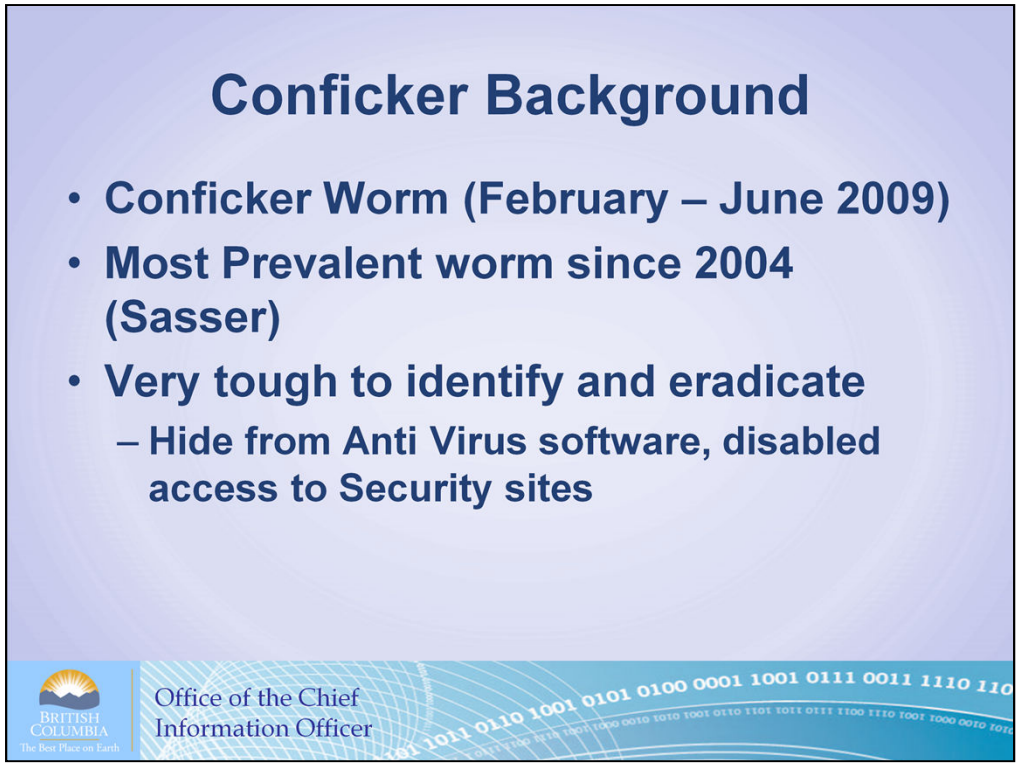
The system also easily picked off infected Microsoft Desktops – signature was systems connecting on port 135 – 137 to UNIX servers or desktops.

Identified Security weaknesses – connections from the Internet hitting what was supposed to be internal only systems. This lead to the Government's first Firewall which was a breakthrough at the time. Moving from an open network (ISP) model to an Enterprise model. It's a debate that Universities must constantly wrestle with – freedom vs safety.



Firefighting – Unplanned Monitoring system, get it up and running quickly.

Looking for very specific patterns instead of general data reduction and looking for unusual events. Looking for Known Bad.



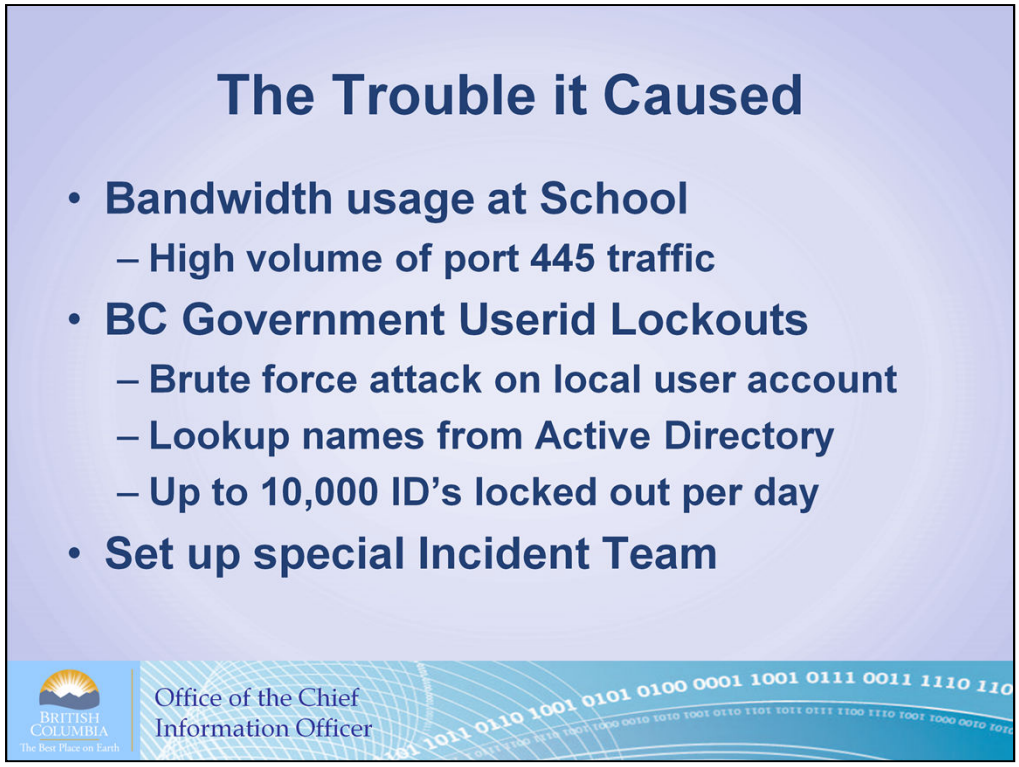
This was the predecessor to most of today's more sophisticated trojans. It displayed many advanced features – including the ability to stealthily hide from AV technologies, to disable AV and to try many different vulnerabilities instead of relying on just one exploit. It was also a noisy virus – unlike today's trojan's which tend to be quite.

The best way of detecting this worm was through Network traffic monitoring.

Government Network is expansive. Covers entire province. What was happening is that Userid's where getting locked out by the Conficker worm due to our lockout period after xx number of unsuccessful logins. We had domain controllers located throughout the Province and the worm was hitting them with password guesses for the userid's. The DC's themselves where never compromised, but the result of the worms activity was that lots of ID's where temporarily locked out.

Government took this worm very seriously, we had lots of network protection in place but somehow it got into the network. Initially with the schools / colleges but later it spread into some Government systems.

Most PC's had to be completely re-imaged to ensure they where clean.



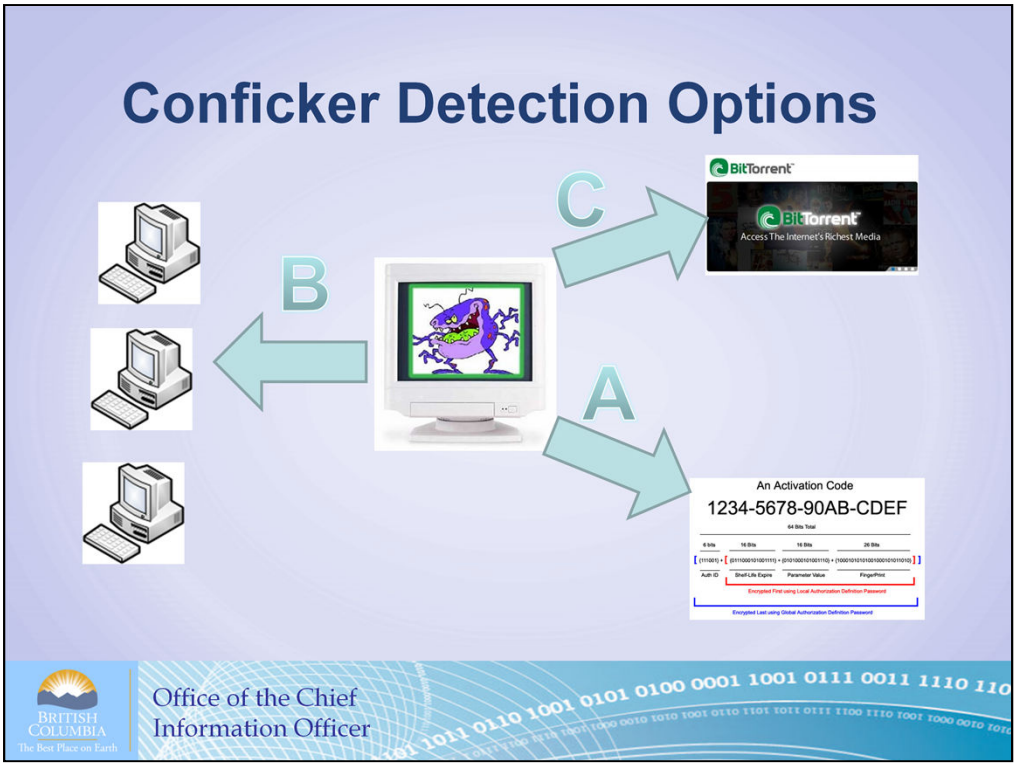
This was the predecessor to most of today's more sophisticated trojans. It displayed many advanced features – including the ability to stealthily hide from AV technologies, to disable AV and to try many different vulnerabilities instead of relying on just one exploit. It was also a noisy virus – unlike today's trojan's which tend to be quite.

The best way of detecting this worm was through Network traffic monitoring.

Government Network is expansive. Covers entire province. What was happening is that Userid's where getting locked out by the Conficker worm due to our lockout period after xx number of unsuccessful logins. We had domain controllers located throughout the Province and the worm was hitting them with password guesses for the userid's. The DC's themselves where never compromised, but the result of the worms activity was that lots of ID's where temporarily locked out.

Government took this worm very seriously, we had lots of network protection in place but somehow it got into the network. Initially with the schools / colleges but later it spread into some Government systems.

Most PC's had to be completely re-imaged to ensure they where clean.

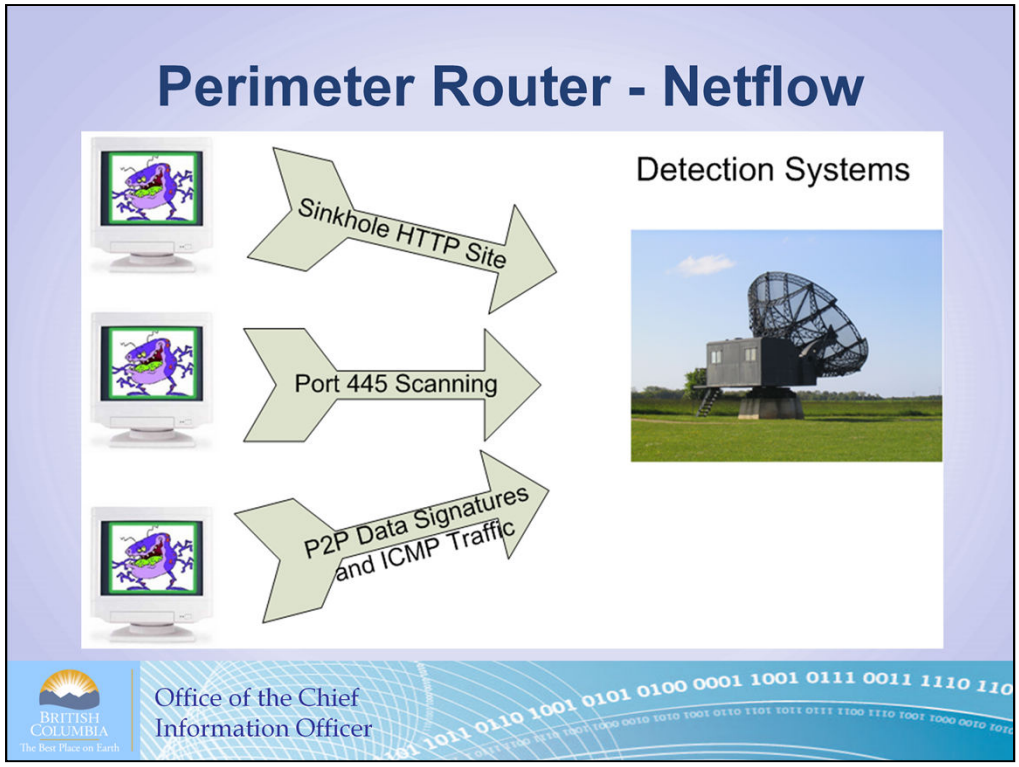


To catch Conficker infected machines, the old addage applies – Know thy Enemy. In this case the enemy was Conficker. In order to catch it you had to know how it functioned. There were three main areas when it communicated over the network.

A ➔ Worm becomes Activated by checking for Internet connection, time, IP address and Downloading Rest of Code. It used internally encrypted data files with algorithms based on the day to determine who to communicate with on the Internet. This was not very friendly to monitoring.

B ➔ Worm Starts infecting other machines by scanning port 445, looking for the Server Service, looking for unpatched vulnerability and guessing passwords. This left a big fingerprint in network logs.

C ➔ Variant “C” uses P2P looking for other infected machines. With all the P2P traffic on the Internet at the time, this was a very difficult way to search. Music and movie downloads both used P2P networks and P2P networks tended to be very noisy even when files weren’t being downloaded.



Sinkhole Sites ➔ Pre Programmed sites the worm expects will return Activation Code (Netflow) [40% overlap with port 445 scanning]

Port 445 Scanning ➔ Large amounts of port 445 traffic, stands out like a sore thumb at the Internet Gateway, high volumes (Netflow) [average around 250 sites]. Since port 445 is an Internal Microsoft port it should never be traversing over the Internet.

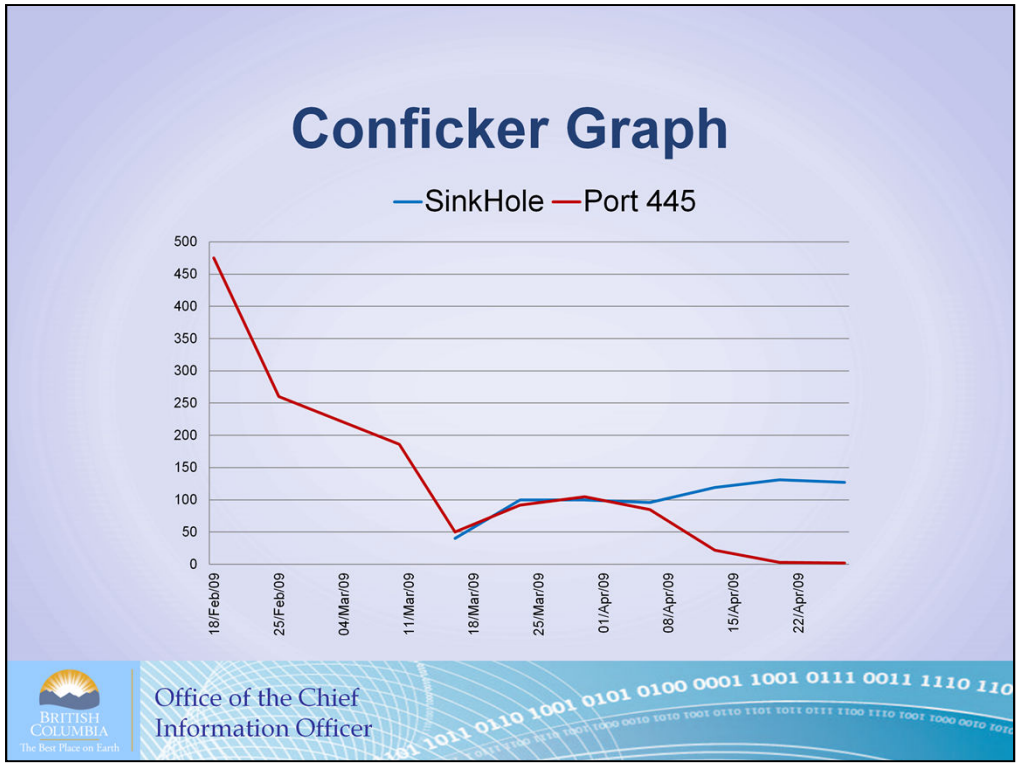
ICMP Signatures ➔ 30% Overlap with the Sinkhole Sites; 0% overlap with the 445 port scanning

P2P Data Signatures ➔ Worm Signature matches using IPS; large volumes of return ICMP traffic for P2P traffic [average around 15 sites, 20% overlap with other detection systems]

Other theories tried was Flows with 2 or less TCP packets and port > 444 (came up empty)

ICMP Signatures → No corallation with Worm; theory was that Variant “C” produces lots of random P2P traffic and this would result in large amounts of ICMP traffic.

Scanners used to confirm and identify infected machines.

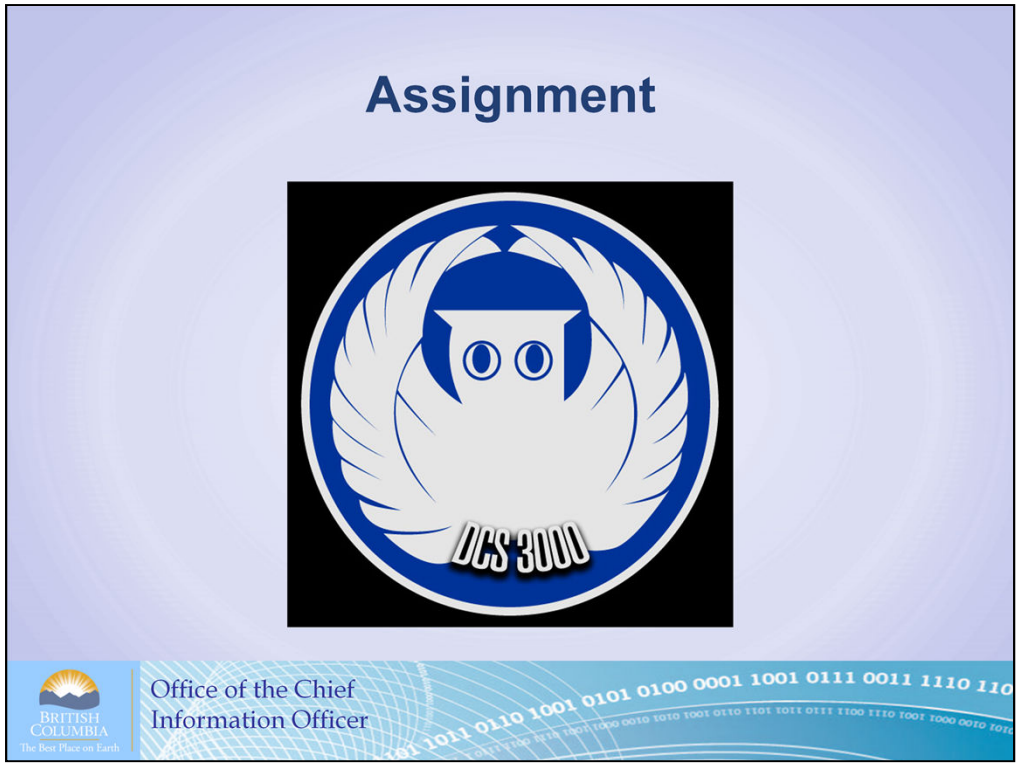


Noisy Worm – easy to detect at a central Network point

Mostly Schools and Colleges on the network

The data displayed is from the Sinkhole and Port 445 Monitoring. Notice the steep drop off at the start as remediation efforts take effect. About ½ way through the Sinkhole monitoring started, port 445 dropped off till nil as this traffic was dropped due to performance issues prior to hitting the monitoring system in April

QUESTIONS?



DCS Logo

An owl, an animal known for its exceptional vision dominates the logo of the Telecommunications Intercept and Collection Technology Unit, or TICTU, which developed the DCS-3000. This enhanced image is based on black-and-white FBI documents

The FBI monitors for content using their private DCSNet – lawbreaking citizens, terrorist, spies

The surveillance system, called DCSNet, for Digital Collection System Network, connects FBI wiretapping rooms to switches controlled by traditional land-line operators, internet-telephony providers and cellular companies. It is far more intricately woven into the nation's telecom infrastructure than observers suspected