GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Network Monitoring and Threat Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

Successful SIEM and Log Management Strategies for Audit and Compliance

GIAC GCIA Gold Certification

Author: David Swift, dgswift@verizon.net

Advisor: Egan Hadsell

Accepted: November 4, 2010

Abstract

Organizations often spend a great deal of money on Log Management and Security Information and Event Management (SIEM), with disappointing results. Many organizations struggle with "use cases," and most SIEM vendors fail to provide effective out of the box correlations. Then too, many organizations fail in their vision and process, considering SIEM just another tool to be dropped onto the network. This paper covers common requirements and a process that has proven successful in multiple Log Management and SIEM, deployments in helping organizations meet both compliance needs, and improve their overall security strategy. A process including defining threats, documenting responses, and standard reporting to meet compliance regulations is detailed. Baseline correlations, reports, and compliance basics with reference links are provided in appendices.

© 2010 SANS Institute, Author retains full rights.

1. Introduction

While there are any number of compliance regulations (SOX, GLBA, PCI, FISMA, NERC, HIPAA…see Appendix E for and overview and links to regulations), and auditors follow various frameworks (COSO, COBIT, ITIL…see Appendix F for and overview and reference links), there are a few common core elements to success.

In a nutshell:

1. log all relevant events
2. define the scope of coverage
3. define what events constitute a threat
4. detail what should be done about them in what time frame
5. document when they occurred and what was done
6. document where both the events and follow up records can be found
7. document how long events and tickets are kept

By defining which events are of interest and what should be done about them, security and log analysis not only aids in compliance, but becomes proactive. Log analysis used in this manner can be used to detect emerging threats and trends, and even to tune and improve overall security.

It is easy to become overwhelmed by the millions of events generated by firewalls, authentication logs, intrusion logs, and other logs *ad nauseum,* however certain anomalous behavioral patterns, and repeat events are common relatively easy to detect signs of malware.

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

2. Discussion

First, with respect to auditors, regulators and the courts, they each have their own interpretation of the various regulations. A review of the regulations, and practical interpretation will show a series of common elements from which the process and strategy in this document were derived. To date these practices have been widely accepted for multiple customers subject to varying compliance requirements this author has been involved with.

Sarbanes Oxley (SOX) , though widely applicable to any publically traded company, can be a difficult document from which to infer IT requirements. However SOX provides language, which when interpreted in an IT context translates to "we must log events, and respond in a timely fashion. From *Sarbanes-Oxley Act of 2002* (H.R. 3763) 107th Congress (2001-2002) SEC. 103. AUDITING, QUALITY CONTROL, AND INDEPENDENCE STANDARDS AND RULES. (c)(2 "The Board shall respond in a timely fashion to requests from designated professional groups of accountants and advisory groups...."

While the focus of the bill is on auditors, and financial reporting, supporting logs and data to which the board is required to attest to often fall on the heads of IT professionals to provide.

Sarbanes Oxley, also provides a base timeline of one year for event retention. Again, though not technology directed, actors subject to the law are required to provide annual reports, and both annual and one year appear repeatedly in the law. From one related section of the law, *Sarbanes-Oxley Act of 2002* (H.R. 3763) 107th Congress (2001-2002) SEC. 102. REGISTRATION WITH THE BOARD. (e) PUBLIC AVAILABILITY. "Registration applications and annual reports required by this subsection, or such portions of such applications or reports as may be designated under rules of the Board, shall be made available for public inspection, subject to rules of the Board or the Commission"

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

PCI provides a clear mandate for logging and review in more specific terms, *PCI DSS Requirements and Security Assessment Procedures,* v1.2.1, Requirement 10, (2008).

"Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs."

From GLBA, one can derive a mandate to provide a written security plan, *Gramm-Leach-Bliley Act* , PUBLIC LAW 106–102, Subchapter I, Sec. 6801-6809 (1999)

"…each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards -

(1) to insure the security and confidentiality of customer records and information;
(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."

Within FISMA is the nucleus of a charter to monitor for threats, *Federal Information Security Management Act of 2002*, H. R. 2458—48, § 3544 (2002)

" (a) IN GENERAL.—The head of each agency shall—
(1) be responsible for (A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;"

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Contained in HIPAA, are mandates for anti-malware controls, *HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996*, 164.308(a)(5)(ii)(B),(1996) (B) *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

From NERC, we can derive a requirement to document the scope for which we will be responsible and at least annual reviews, *Standard CIP–002–3,* Cyber Security, Critical Cyber Asset Identification, B. R2 (2009) "Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary."

While you may not be subject to all, or even one of these regulations, it is best to assume at some future date you could be required to be compliant with one or more of them and design any comprehensive security solution to meet the common criteria. Also consider that most public policies include the catch all phrase "best practices" subjecting us to not just those most directly linked regulations, but compliance best practices from every regulation.

A single common denominator for all regulations requires that one log all events, and review them. The intent and implication is that we are reviewing logs for threats, and following up on them to resolve any issues discovered, and can document that we have done so.

In an effort to identify what would constitute a threat, a common set of events in logs that would rise to the level of a threat are defined in Appendix A – Events of Interest. During audits, providing an unambiguous definition of what constitutes a threat can quickly reduce much of the noise of common logs and provide a common basis for discussion.

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

In most SIEM products today, log review (threat detection), can be automated by creating correlation content matching the Events of Interest in Appendix A to automatically notify, or even create automated trouble tickets for threats as they are detected in real time. Auditors time and time again have expressed a strong preference for automated ticketing, and are much more likely to accept one's documentation for threat tracking and follow up if we can show the process is automated.

In addition to threat identification, auditors and regulators expect "timely" review of logs, which can be documented through regular reports. A common set of reports to meet the review process are defined in Appendix B – Common Reports. Both regularly reviewed and operational detail reports are outlined.

A minimal set of monthly summary reports for system review is provided in Appendix C – Sample Summary Reports. Summary reports have proven useful in providing oversight for security devices, helping to identify when a device is not detecting or blocking to the extent one would expect. A simple top ten list of what was detected and blocked, with a count by severity can help prioritize security responses. Operational reports detailing the source hosts for any given malware can then direct remediation responses (see Appendix B – On Demand Operational Reports). Finally, summary reports can identify key outliers and spikes that may be first signs of malware even when specific signatures are not triggered.

Reports that may require review, including user activity reports and reports on configuration changes are documented in Appendix B (User Activity Reports, Configuration Change Reports and Access Reports). It is a common best practice to have reports requiring review, to require sign off by the system or data owner (explicit attestation), and to store the signed report for a length of time matching your record of authority documentation (See Appendix D – Record of Authority and Retention). Alternatively, one may send reports for review via email, noting in the body of the email that unless otherwise noted and reported, the data or system owner acknowledges and attests that the access or changes noted in the attached reports are normal and permitted (assumptive affirmation). Caution is advised with assumptive affirmation. While this

© 2010 The SANS Institute Author retains full rights.

may relieve the security group for responsibility, it is not usually accepted as proof the organization as a whole has met its requirements for review.

Additional industry best practices and reference organizations are listed in Appendix G – Best Practices and Compliance Links. The National Institute of Standards and Technology (NIST), 800 series documents can provide additional system and function specific guidelines. The International Standards Organization (ISO) 17799 Code of Practice for Information Security Management is one of the most widely used audit frameworks and a basic summary and link is provided in Appendix G – Best Practices and Compliance Links.

© 2010 SANS Institute, Author retains full rights.

David Swift, dgswift@verizon.net

3. Log Management Strategy

A successful security program that passes the scrutiny of audit and compliance will need to provide for the following:

1) Centrally log all relevant events.
   a) Events may be filtered, aggregated, and/or normalized[1]
   b) Only events from devices in scope need to be collected.
2) Define and document the scope of coverage.
   a) Document which assets are in scope for each compliance regulation you're organization is subject to.
   b) Define which networks and assets are internal and part of the protected network.
   c) Create a Record of Authority (ROA), document defining where logs will be stored, and the retention period for each log. (See Appendix D – Record of Authority and Retention)
3) Review logs in a timely fashion.
   a) Define and watch for Events of Interest (EOI), that could constitute a threat.
   b) Of the millions of events per day an organization collects, less than 1% will represent a threat.
   c) Define and document Service Level Agreements (SLAs), and Standard Operating Procedures (SOPs).
      i) Per event of interest, define the time frame for follow up.
      ii) Define and document a minimum process for follow up to standardize response for each event of interest.
   d) Schedule regular reports for review of key events and oversight of security devices.
4) Create an audit trail for reviewed events.
   a) We must maintain an auditable trail to prove events of interest were followed up on and resolved.
   b) Document that each EOI in scope was followed up on using SOPs and in compliance with stated SLAs.

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Second, the choice of log management tools is individual, and may include a centralized syslog server, or a distributed collection approach. The current market leaders in Log Management solutions are ArcSight (Logger),LogLogic, LogRythm, Syslog NG and Splunk (see *Appendix H – SIEM & Log Management Vendors*).

In most cases sizing these devices to retain events for one year will meet most compliance regulations.

You will also want to make sure the device can pull logs from databases, Windows hosts, and other systems that do not by default forward events via syslog.

Consider placement carefully, as syslog is by default UDP based and does not guarantee delivery, nor encrypt the traffic. In many cases syslog can be configured to use TCP. Secure tunnels or VPNs may also be required to ensure logging does not expose sensitive data.

Centralized logging alone is not enough. The spirit, and in some cases the specifics, of the various compliance rules require that logs be reviewed in a timely manner. In most cases this is physically impossible with limited staff, and millions of events per day. It is common to have 100 Million or more raw security events per day or more in a large enterprise.

A common best practice is to use a correlation engine to automate threat detection and log analysis. ArcSight ESM, Q1 QRadar, RSA EnVision are top SIEM vendors providing correlation capabilities. SIEM is a significant undertaking and can be quite expensive. See *Appendix H – SIEM & Log Management Vendors* for a more complete list and reference links. While SIEM tools can provide a good framework, many find the default content, or "use cases" very limited, or non-functional in a production environment.

This is where it becomes important to define events of interest (EOI). The correlation rules to create the EOI alerts are outlined in *Appendix A – Events of Interest*. The syntax for the rules varies by product, but the essential capabilities should exist in any mature SIEM.

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

A general principal of compliance is to have a written policy. Auditors then check to confirm that the written policy is followed. By defining and documenting our events of interest (EOI), and providing a written copy to auditors, we improve our overall compliance, and meet our requirement for a written policy. Then, instead of being held to someone else's interpretation of the regulation, provided of course that we have a legitimate supportable set of EOI definitions, we will be measured to an agreed upon standard.

A clear definition of EOI is our starting point, next we must define standard operating procedures (SOPs), and service level agreements (SLAs), that state what is done when an EOI has been detected, and in what time frame.

SOPs will vary widely based on the severity of the EOI, and the staff and tools one has to follow up on them. Drawing on the experience of one's best and brightest, capture their process into an SOP. Doing so then allows transference of that knowledge to the institution and aids in training new security staff.

SLAs will also vary widely, and should be dependent on the severity of the EOI, and the available staff. Critical events with a high chance for contagion or corruption of data should have very narrow windows for follow up. Events with higher false positive rates that may be leading indicators of malware, or system misconfiguration should be followed up on a "best effort basis."

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

4. Reporting and Review

To be in compliance, auditors require that key system access, and changes are reviewed on a regular schedule. Much of the focus is on "who" and can be covered by tracking, reporting, and reviewing periodically key reports (See Appendix B – Common Reports).

A common and successful strategy is to track by system access both who, when, from where, and against which authentication device each user accessed a protected resource.

Providing these reports as summary, including only who, and which system type was accessed to the system owners for each authentication log collected for monthly (or quarterly in less critical networks).

In query terms this is a simple select where user = * and event name contains login, group by user and authentication device.

Variations of the same report can be used to produce other common reports, by simply limiting the user name to the key accounts. A common use is for default accounts (root, administrator, guest). Another common use is for all administrative access (user name contains $, admin, or root).

Additionally, reports for any rights or user additions or permission modifications will need to be reviewed. These reports are similar, but are grouped by the specific event types to be monitored (where contains user deleted, or object modified, or rights assigned…). Here again, a good strategy is to provide these reports to the application owners (by authentication type), each month or quarter for review and acceptance. The signed accepted reviews should then be filed for audit purposes.

Last, we need to provide executive level review and oversight. Top 10 reports for each device feeding your log management or SIEM solution will often suffice.

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Best practice is to review each log source for variety in signature, and number of occurrences. For devices that detect malware, simply group by malware or name or ID, severity, and by unique source address.

If the number of events is low, perhaps the device can be tuned to more effectively detect additional attacks, or the network may be in fact clean.

If the number of unique sources is high, the malware signature may be a false positive.

Outbreaks of malware can be spotted as the number of unique source addresses for any given signature rise. These reports can also be used for operational benefit, allowing prioritization and cleaning of systems with detected infections, and prophylactics to be applied to the broader protected network for active threats preventing spread.

5. Ticketing and Tracking

For each of the identified threats in reports, or real time via Events of Interest, based on the Service Level Agreement applicable, trouble tickets with a description of the problem and the resolution efforts will need to be kept.

Key metrics and a common audit review process is to check:

1. Are tickets being created (preferably automatically) and tracked for protected assets?
2. Are tickets being closed?
3. Are tickets being closed within the SLA? Mean Time to Resolution

Though often not a part of compliance and audit, a key operational need is:

4. Are threats being detected (preferably thorough automated intelligence, not after the fact end user notification)?

Spot checks by auditors that can confirm 1, 2, and 3, are often all that's needed from ticket systems to confirm compliance.

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

6. Conclusion

If one follows several basic steps, and documenting both scope and process it is possible to achieve nearly any IT audit requirement.

1. Define your Events of Interest (EOI) – and create appropriate reports and alerts to monitor for them (See Appendix A – Events of Interest)
2. Define an Incident Handling Policy (IH) and process to follow for each EOI
3. Define Service Level Agreements (SLAs), for each EOI and follow up IH process – Standard Operating Procedures for Security Analysts (SOP)
4. Create and Maintain an Audit trail showing both EOI's and IH responses, tracking the mean time to detect (MTD) and mean time to remediate (MTR) – frequently this is done in an external ticketing system.
5. Define the Record of Authority (RoA) for each device in scope for an audit
    a. Document the source IP's for which the log management/SIEM will be the RoA
    b. Document the retention period, and the document destruction/deletion policy followed.
    (See Appendix D – Record of Authority and Retention)

It is possible to prepare for an audit while building a stronger security program by preparing unambiguous well documented scope, record of authority, events of interest, and incident handling policies. Provided these written policies are shared with auditors, and can be confirmed by spot checks showing both an event was logged, and that it was remediated in accordance with standard operating procedures within the define service level agreement, audits can be made quick and relatively painless.

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

7. References

Kerr, Orin S, *Computer Records and the Federal Rules of Evidence* retrieved from October 18, 2010 from U.S. Department of Justice, http://www.justice.gov/criminal/cybercrime/usamarch2001_4.htm

NERC CIPs and Standard, Retrieved October 18, 2010 from the North American Electric Reliability Corporation http://www.nerc.com/page.php?cid=2|20

Payment Card Industry Data Security Standard v1.2.1 (2008), Retrieved October 19, 2010 from the PCI Security Standards Council https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html

Sarbanes-Oxley Act of 2002 (H.R. 3763) 107th Congress (2001-2002) Retrieved October 18, 2010 from the Library of Congress http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03763:

The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, *et seq.*), Retrieved October 18, 2010, from the National Institute of Standards and Technology http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

The Gramm–Leach–Bliley Act (GLB), also known as the Financial Services Modernization Act of 1999, (Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999), Retrieved October 18, 2010 from the Federal Trade Commission, http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191) Retrieved October 18, 2010 from the U.S. Department of Health and Human Services http://aspe.hhs.gov/admnsimp/pl104191.htm

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

8. Acknowledgements

General credit and thanks to Mike Poor @ SANS for the process and analytical training needed to develop specific correlation rules.

Thanks to Egan Hadsell @ SANS for editorial and formatting advice and guidance.

Thank you to Accuvant (my employer), for allowing me to share the included content, having developed and/or refined much of it "on the job" at numerous client installations.

I owe general credit to SANS courses for information and processes that have become part of my standard way of thinking, if not specifically quoted in the paper.

SANS Audit 507, *Auditing Networks, Perimeters and Systems*, 2006

SANS Security 504, *Hacker Techniques, Exploits and Incident Handling*, 2009

SANS Security 503, *Intrusion Detection In-Depth*, 2006

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Appendix A – Events of Interest

Provided below is a common set of perimeter defense correlation rules. In vendor terms these are often referred to as "use cases." These are meant to provide a good base starting point, and should not be considered comprehensive for all situations.

User Authentication Rules and Alerts

1. Repeat Attack-Login Source

Goal: Early warning for brute force attacks, password guessing, and misconfigured applications.

Trigger: Alert on 3 or more failed logins in 1 minute from a single host.

Event Sources: Active Directory, Syslog (Unix Hosts, Switches, Routers, VPN), RADIUS, TACACS, Monitored Applications

2. Repeat Attack-Login Target

Goal: Early warning for brute force attacks, password guessing, and misconfigured applications.

Trigger: Alert on 3 or more failed logins in 1 minute on a single user ID

Event Sources: Active Directory, Syslog (Unix Hosts, Switches, Routers, VPN), RADIUS, TACACS, Monitored Applications

Note: The actual number of events required to trigger a correlation will vary over time and will need to be tuned to each system as the frequent threats are removed, and the rules are optimized. Separate similar rules may be required for log sources with higher or lower sensitivity (i.e. one rule triggers on 5 or more failures for Windows, one rule triggers on 3 or more failures for Unix).

David Swift, dgswift@verizon.net

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute Author retains full rights.

Attacks Detected on the Network

3. Repeat Attack-Firewall

Goal: Early warning for scans, worm propagation, etc…

Trigger: Alert on 15 or more Firewall Drop/Reject/Deny Events from a single IP Address in one minute.

Event Sources: Firewalls, Routers and Switches

4. Repeat Attack-Network Intrusion Prevention System

Goal: Early warning for scans, worm propagation, etc…

Trigger: Alert on 7 or more IDS Alerts from a single IP Address in one minute.

Event Sources: Network Intrusion Detection and Prevention Devices

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute Author retains full rights.

Attacks and Infections Detected at the Host Level

5. Repeat Attack-Host Intrusion Prevention System

Goal: Find hosts that may be infected or compromised (exhibiting infection behaviors).

Trigger: Alert on 3 or more events from a single IP Address in 10 minutes

Event Sources: Host Intrusion Prevention System Alerts

Virus Detection/Removal

6. Virus or Spyware Detected

Goal: Alert when a virus, spyware or other malware is detected on a host.

Trigger: Alert when a single host sees an identifiable piece of malware

Event Sources: Anti-Virus, HIPS, Network/System Behavioral Anomaly Detectors

7. Virus or Spyware Removed

Goal: Reduce alerts and warnings, if after detection, anti-virus tools are able to remove a known piece of malware.

Trigger: Alert when a single host successfully removes a piece of malware

Event Sources: Anti-Virus, HIPS, Network/System Behavioral Anomaly Detectors

8. Virus or Spyware Detected but Failed to Clean Critical EOI

Goal: Alert when >1 Hour has passed since malware was detected, on a source, with no corresponding virus successfully removed.

Trigger: Alert when a single host fails to auto-clean malware within 1 hour of detection.

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Event Sources: Anti-Virus, HIPS, Network/System Behavioral Anomaly Detectors

Attacks from Unknown/Untrusted Sources

The use of periodic automatically updated lists (RBL, DShield…), of known attackers and malware sources applied to these correlations is highly preferred.

9. Repeat Attack-Foreign

Goal: Identify remote attackers before they make it into the network. Identify "back scatter" pointing to attacks that may have not been detected by other sources.

Secondary Goal: This rule also identifies new networks with active hosts that have been added to the internal network, but not reported or configured within the SIEM and/or other security tools.

Trigger: Alert on 10 or more failed events from a single IP Address that is not part of the known internal network.

Event Sources: Firewall, NIPS, Anti-Virus, HIPS, Failed Login Events

10. Known Attacker Allowed in Network Critical EOI

Goal: Identify allowed traffic from known "black listed" sources. If the source is known to be a source of malware or an attack, identify and alert if that source is every allowed into the network, while conversely filtering out/ignoring "drop/reject/deny" events from these sources when our defenses properly block the traffic.

Trigger: Alert on ANY Allowed (i.e. Firewall Accept, Allowed Login), events from an IP Address that is not part of the known network and is known to have/use malware.

Event Sources: Firewall, NIPS, Anti-Virus, HIPS, Failed Login Events

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

11. Traffic to Known Attacker — Critical EOI

Goal: Identify traffic from an internal address to known "black listed" destinations. If the destination is known to be a source of malware or an attack, identify and alert if traffic is ever allowed to that destination, or if repeat attempts (>5) are detected even when the traffic is blocked. This may indicate an infected host trying to call home.

Trigger: Alert on ANY Allowed (i.e. Firewall Accept, Allowed Login), event to an IP Address that is not part of the known network and is known to have/use malware.

Alternate Trigger: Alert on 5 or more drops from an internal source to any known attacker, or 1 Accept/Allow.

Event Sources: Firewall, NIPS, Anti-Virus, HIPS, Failed Login Events

High Threats

12. High Threat Targeting Vulnerable Asset — Critical EOI

Goal: Identify threats in real time that are likely to compromise a host. Vulnerability data has shown the host to be vulnerable to the inbound attack being detected by NIPS.

Trigger: Any event from a single IP Address targeting a host known to be vulnerable to the attack that's inbound.

Event Sources: NIPS events, Vulnerability Assessment data

13. Repeat Attack-Multiple Detection Sources — Critical EOI

Goal: Find hosts that may be infected or compromised detected by multiple sources (high probability of true threat).

Trigger: Alert on ANY second threat type detected from a single IP Address by a second source after seeing a repeat attack. (i.e. Repeat Firewall Drop, followed by Virus Detected)

Event Sources: Firewall, NIPS, Anti-Virus, HIPS, Failed Login Events

David Swift, dgswift@verizon.net

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute Author retains full rights.

14. Possible Outbreak – Excessive Connections Critical EOI

Goal: Find hosts that may be infected or compromised by watching for a host to connect to a large number of destinations.

Trigger: Alert when a single host connects to 100 or more unique targets in 1 minute (must apply white lists for known servers to avoid false positives, and destination port !=80).

Event Sources: Firewall, NIPS, Flow Data, and Web Content Filters

15. Possible Outbreak – Multiple Infected Hosts Detected on the Same Subnet Critical EOI

Goal: Alert on the detection of malware before it spreads beyond a limited number of hosts.

Trigger: Alert when 5 or more hosts on the same subnet trigger the same Malware Signature (AV or IDS) within a 1 hour interval.

Event Sources: Anti-Virus, HIPS, NIPS

Web Servers (IIS, Apache)

16. Suspicious Post from Untrusted Source

Goal: Alert when dangerous content (executable code) is posted to a web server.

Trigger: Files with executable extensions (cgi, asp, aspx, jar, php, exe, com, cmd, sh, bat), are posted to a web server (internal/dmz address), from an external source

Event Sources: Internet Information Server and Apache Logs

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Monitored Log Sources

17. Monitored Log Source Stopped Sending Events

Goal: Alert when a monitored log source has not sent an event in 1 Hour (variable time based on the device).

Trigger: Log collection device must create an event periodically to show how many events have been received, and that this number is >0.

Event Sources: Log collection device.

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute Author retains full rights.

Appendix B – Common Reports

These reports are produced and reviewed monthly, or on demand as needed.

User Activity Reports

1. All Active User Accounts (any valid/successful login by account name in the past 30 days)
2. Active User List by Authentication type
    a. VPN Users
    b. Active Directory Users
    c. Infrastructure Device Access (Firewalls, Routers, Switches, IDS)

    To be reviewed/certified as valid by the administrator/manager for each authentication source.

    Unused accounts should be disabled.

    Any unexpected account usage (default accounts, terminated employees…), should be investigated and explained.

3. User Creation, Deletion and Modification
    a. A list of all user accounts created, deleted or modified by authentication type, to include the date, time, and User ID that made the change.
        i. Active Directory
        ii. RADIUS/TACACS
        iii. Local (Unix, Windows Server...SSH, LSAS…)
4. Access by any Default Account
    a. Guest, Root, Administrator, or other vendor default account usage
5. Access by any terminated employee, expired contractor, or other expired account
6. Access by Privileged Accounts (root, administrator…)

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

   a. Noting time, date, source IP, and where possible source user name that became admin
      i. 'su' log
      ii. Correlation of "Privilege Escalation for User X" followed by Privileged Execution (Server Reboot, Log Clear, File Deletion) on windows
7. Service Account Usage
   a. A list of all service accounts grouped by target address

   This report should be reviewed by the service account user owner and validated monthly.

   Any unexpected use of a service account, or use on an unexpected address should be investigated and explained.

Configuration Change Reports

8. Configuration Change Report
   a. Any configuration changes on monitored devices
      i. Date, Time, and User ID that made the change

Access Reports

9. Access to any protected/monitored device by an untrusted network
   a. VPN Access to Protected Network
   b. Wireless Access to Protected Network
   c. Access by a Foreign Network to a Protected Network
      i. Foreign Country
      ii. Any Non-Internal/Company/Intranet Source Address
   d. Access to a Higher Security Network by a Lower Security Network
10. Internet Usage by Protected Device
   a. Any traffic from a protected device to a network other than the protected and trusted networks.

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Incident Tracking

11. Current Open Ticket List
    a. A list of all incidents not yet closed.
12. Closed Ticket Report
    a. A list of all tickets closed in the past X days (from 1-90).
    b. Details must include the total time the ticket was open (Time to Resolution), the root cause if found, and the person who opened and closed the ticket.
13. Time to Resolution by Ticket Type
    a. For each ticket type (See Attachment A – Required Correlations), the minimum, maximum, and average time to resolution.

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute Author retains full rights.

On Demand Operational Reports

14. User Login Tracking
    a. All Logins for a User ID for the past 30 days - Group by User Name and Source Address

    Use: Identify any Hosts a Terminated/Suspicious employee has logged on to for secondary investigation of those hosts.

15. Host Login Tracking
    a. All logins on a given host for the past 30 days

    Use: Identify who may have compromised a host that is misbehaving.

16. Malware Source Report
    a. A list of host addresses for any identified malware or attack – group by malware name or attack name

    Use: Identify the source IP addresses of any given malware or attack for targeted removal/remediation.

17. Malware Occurrence Report
    a. A count of any given malware (group by IDS signature/Anti-Virus Signature/Attack Name), over the past 30 days.

    Use: Defense Tuning – if <100 occurrences of a signature, block, If >100,000 blocking could disrupt the network. Log only mode on new signatures for 30 days, monitor, and block as appropriate.

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute Author retains full rights.

Monthly Summary Reports

These reports are produced and reviewed monthly.

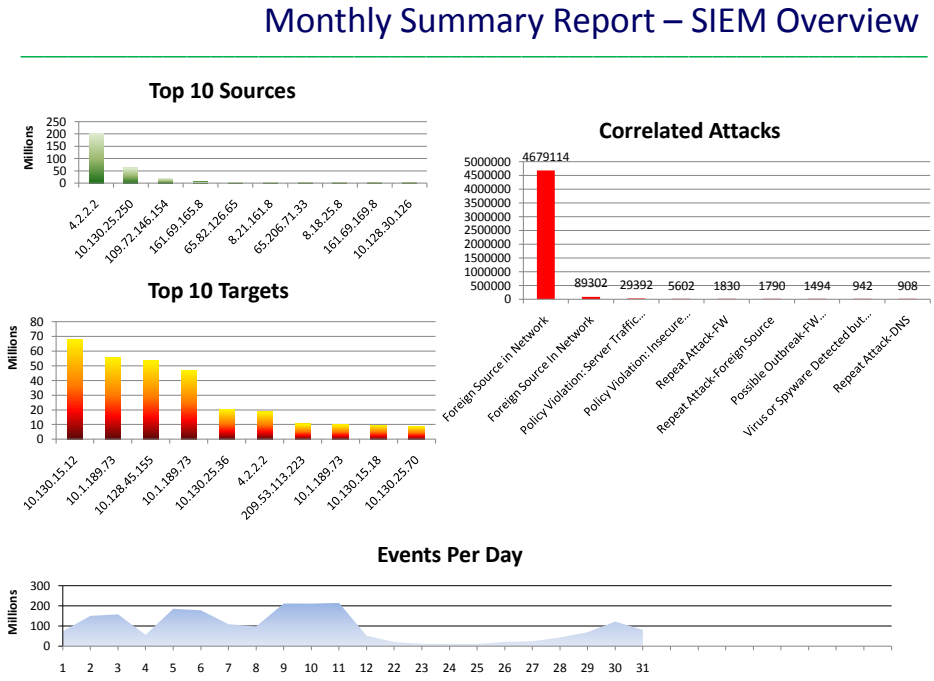
1. Top Sources & Destinations
    a. Filtered to remove known servers.
2. Total Correlated Events/Events of Interest
    a. Grouped and totaled by Event of Interest/Correlation name
3. Total Events / Day / Log Source
4. Top 10 Events Per Log Source (Anti-Virus, IDS…)
5. Top 10 Failed Logins
    a. Grouped by Source IP (Top 10 sources of failed logins)
    b. Grouped by Target User Name (Top 10 accounts with failed logins)
6. Web Content Filter Summary
    a. Top 10 Destinations by Domain Name
    b. Top 10 Blocked Sources by IP Address
    c. Top 10 Blocked Sources grouped by Network (subnet)
7. Foreign Attacker Report
    a. Top 10 Source Countries involved in Attacks (FW, IDS, AV, AUTH…)
    b. Top 10 Sources IPs of Foreign Attacks
    c. Top 10 Destinations of Foreign Attacks

© 2010 SANS Institute, Author retains full rights.

David Swift, dgswift@verizon.net

Appendix C – Sample Summary Reports

The reports below were produced from CSV raw data output from a production SIEM, graphed in Excel, and combined for visual presentation in Power Point.

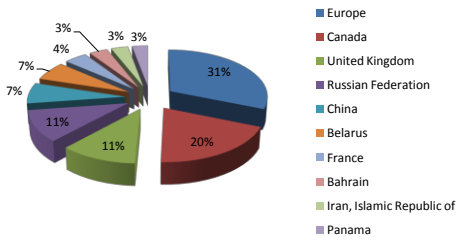


David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Monthly Summary Report – Foreign Attackers

Top 10 Source Countries

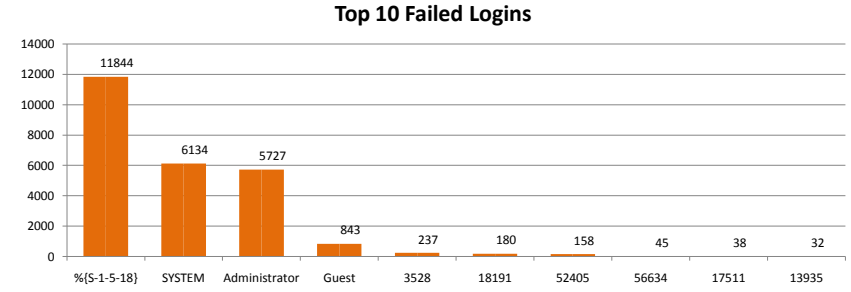


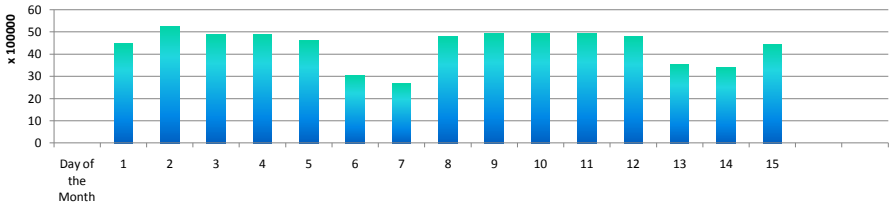
Top 10 Foreign Attackers

109.72.146.154	Europe	15393914
188.72.213.59	Belarus	2977444
91.212.135.186	Russian Federation	2699576
91.212.135.136	Russian Federation	2249550
91.205.41.235	United Kingdom	1758810
193.104.12.102	Panama	1375574
64.71.246.28	Canada	1056001
91.205.41.164	United Kingdom	1042430
24.153.22.142	Canada	996563
109.72.146.155	Europe	962600

A large number of the attacks, are targeting DNS (port 53), and may have been exploiting previous weaknesses now patched with Windows 2008 upgrades to DNS Servers and Domain Controllers.

Monthly Summary Report – Authentication





David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Monthly Summary Report - NIPS

Network Intrusion Prevention Systems (NIPS)

Blocked Attacks

WORM: W32/Netsky@MM Worm 163	399
SMTP: Incorrect MIMEHeader with Executable Attachment Found 94	146
WORM:W32/MyWife.d@MM 48	45
SHELLCODE: Shellcode Detectedfor HP PA-RISCFamily CPUs 23	33
WORM: W32/Zafi@MM Worm 23	29
DCERPC: SRVSVC Buffer Overflow 20	25
NETBIOS-SS: Microsoft Server Service Remote Code Execution Vulnerability 5	4
PCANYWHERE:Host Logon Engine Buffer Overflow 2	3
WORM: W32/Netsky@MM Worm VariantsII 2	3
BACKDOOR: Web Serve CT Backdoor 2	2
SMB: NLTMSSP_AUTHUnauthorized ChangeServiceConfigW Request 1	1
Total:	690

Severity Counts

Blocked	690
High	8,902
Medium	9,148,414
Low	7,017,018
Unclassified	37,092,444
Total:	**53,267,468**

Approximately 700 malicious attacks were blocked in the past 30 days

Top 10 Blocked Attacks



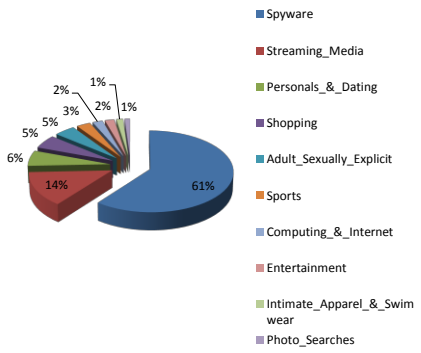
- WORM: W32/Netsky@MM Worm 163
- SMTP: Incorrect MIMEHeader with Executable Attachment Found 94
- WORM:W32/MyWife.d@MM 48
- SHELLCODE: Shellcode Detectedfor HP PA-RISCFamily CPUs 23
- WORM: W32/Zafi@MM Worm 23
- DCERPC: SRVSVC Buffer Overflow 20
- NETBIOS-SS: Microsoft Server Service Remote Code Execution Vulnerability 5
- PCANYWHERE:Host Logon Engine Buffer Overflow 2
- WORM: W32/Netsky@MM Worm VariantsII 2
- BACKDOOR: Web Serve CT Backdoor 2
- SMB: NLTMSSP_AUTHUnauthorized ChangeServiceConfigW Request 1

4

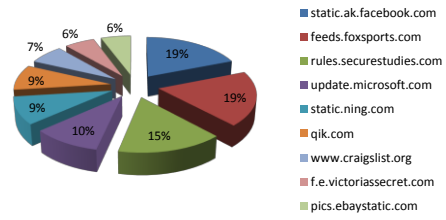
Monthly Summary Report - WCF

Web Content Filtering (WCF)

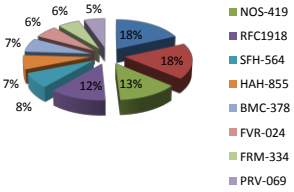
Top Blocked Categories



Top Blocked Destinations



Top Blocked Locations



5

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Appendix D – Record of Authority and Retention

The protected network consists of all routed RFC1918 addresses (10.x.x.x, 172.16.x.x, 192.168.x.x), and the company's public addresses consisting of network range A.

The network ranges B, C, and D are desktops with no local data storage of Personally Identifiable Information (PII) and not in scope.

The network range E is our DMZ, and has public facing servers for web, email, DNS, and other services, and all relevant security events are logged to our log management server X, and retained for 1 year, and sent to our security event management device Y for event correlation and threat detection where they are stored for 90 days online.

The network range F is for internal servers with PII and other protected data and all relevant security events are logged to our log management server X, and retained for 1 year, and sent to our security event management device Y for event correlation and threat detection where they are stored for 90 days online.

Trouble tickets are automatically created by threats detected on our security event management server, and their related follow up, analysis and remediation are stored on our ticket server Z.

Replace A,B,C,D…X,Y, and Z with the appropriate systems for the organization in scope.

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Appendix E - Compliance Regulations Basics and Links

SOX / SARBOX -Sarbanes Oxley

http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03763:

Applies to all publicly traded companies. A majority of the regulations apply to auditing, the board of directors, disclosures, and improper trading. Section 404 (below), is interpreted to apply to IT. SOX, as it reads, is highly subjective with few IT specifics. ISO7799, PCI, or HIPPA provide better implementation specifics that you may wish to follow.

Full text of bill: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf

GLBA, GLB -Gramm-Leach-Bliley Act

http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/content-detail.html

Applies to the financial services industry (Insurance, Securities, Banking)
Specifically makes pretexting illegal.

With the exception of a few specific acts being made illegal, and fair credit and consumer rights being spelled out, little of the legislation is directly applicable to IT. ISO7799 is referred to as a starting point in many of the legislative summaries and practical implementation guides. PCI or HIPPA provide more tangible implementation specifics, that should, if followed, also provide proper controls for GLBA as well.

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

HIPAA – Health Insurance Portability and Accountability Act

HIPAA applies to healthcare, medical records, insurance, and other medical related business. The standard and summaries are quite lengthy and verbose in nature, but not difficult to implement, and relatively IT friendly with quite a bit of latitude in methods and implementation specifics. Most technical controls will be in section 164.308.
Summary and Links:
http://www.hhs.gov/ocr/hipaa/
Public Law (2003):
http://aspe.hhs.gov/admnsimp/pl104191.htm

FISMA - Federal Information Security Act

(HR 2458-51) http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
A snoozefest of legalese with little that is actionable in IT terms.
Ironically though FISMA legislation has the least IT related detail, it requires the most from IT to comply as specified in the related NIST and FIPS standards for implementation and compliance.

FISMA discusses a pyramid of goals based on Availability, Integrity and Confidentiality in order to provide security.

Applies to governmental agencies, governmental contractors and telecommunications providers who provide services to anything deemed related to national security (very broad stroke). Also applies to Federal agencies, contractors, and any other company or organization that uses or operates an information system on behalf of a federal agency.

PCI – Payment Card Industry

https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html

Applies to merchants and processors of Visa or Mastercard transactions.

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Unlike SOX and GLBA, The standard is quite straight forward and IT specific and should be read and reviewed in it's entirety.

NERC - North American Electric Reliability Corporation

NERC stands for North American Electric Reliability Corporation (NERC), which is subject to Federal Energy Regulatory Commission (FERC) mandates and control. NERC applies to companies that generate, provider, or transmit energy. The primary focus of NERC is on SCADA, which stands for *supervisory control and data acquisition* devices and networks.

The majority of IT related policies will be found in the Critical Infrastructure Protection Standards (CIP) standards.

© 2010 SANS Institute, Author retains full rights.

David Swift, dgswift@verizon.net

Appendix F- Control Frameworks

COSO – 5 Internal Control Components – Primary Reference for SOX

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information & Communication
5. Monitoring

COBIT – 4 Domains – www.itgi.org

1. Planning and Organization
2. Acquisition and Implementation
3. Deliver and Support
4. Monitor and Evaluate

Stated Goals:

Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance, Reliability

Information Systems Audit and Control Association® (ISACA®) Certified auditors, and COBIT references. www.isaca.org

SAS 70 http://www.sas70.com/about.htm

Statement on Auditing Standards (SAS) No. 70, *Service Organizations,* is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). There are two classifications of SAS70 audits – Type I (no verification), and Type II (with test and verification and documentation supporting testing of controls).

FISCAM Federal Information System Controls Audit Manual

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Appendix G – Best Practices and Compliance Links

NIST – National Institute of Standards and Technology

(800 series) http://csrc.nist.gov/publications/nistpubs/

Even if you're not subject to federal compliance, a NIST has a wealth of good documentation on securing nearly any type of device that can help in meeting any compliance goal. Most of the publications are free and available for electronic download.

ISO/IEC – International Organization for Standards/ International Electrotechnical Commission

17799 / 27002:2005 Code of Practice for Information Security Management
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

DOJ - Department of Justice

With respect to log usage for forensics, auditing and compliance, the department of justice standard states:

[1]Rules of evidence "If a business routinely relies on a record, that record may be used as evidence." http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm

If you ever intend to prosecute a cyber crime, knowing and complying with DOJ standards of evidence and custody of evidence will significantly improve your chances.

FIPS - Federal Information Processing Standards

http://www.itl.nist.gov/fipspubs/
http://csrc.nist.gov/publications/fips/index.html

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

CIS - Center for Internet Security

http://www.cisecurity.org/

CMS - Centers for Medicare and Medicaid Services

http://www.cms.hhs.gov/

DISA Defense Information Systems Agency

http://iase.disa.mil/policy.html

GAAP – Generally Accepted Accounting Principles

Set by the Financial Accounting Standards Board (FASB), may appear as FASB-#

Related: American Institute of Certified Public Accountants (AICPA)

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.

Appendix H – SIEM & Log Management Vendors

ArcSight	http://www.arcsight.com/
EIQ Networks	http://www.eiqnetworks.com/
Intellitactics	http://www.intellitactics.com/int/
LogLogic	http://www.loglogic.com/
LogRhythm	http://logrhythm.com/default.aspx
NitroSecurity	http://nitrosecurity.com/
Novel Sentinel	http://www.novell.com/products/sentinel/
OpenService	http://www.openservice.com/
Q1 Labs	http://www.q1labs.com/
RSA enVision	http://www.rsa.com/node.aspx?id=3182
SenSage	http://www.sensage.com/
Splunk	http://www.splunk.com/
Syslog NG	http://www.balabit.com/network-security/syslog-ng/
TriGeo	http://trigeo.com/

David Swift, dgswift@verizon.net

© 2010 The SANS Institute Author retains full rights.