



NETFORENSICS WHITE PAPER

Event Correlation Matters: Practical, Automated Solutions for Protecting Critical Data

Contents

- 1 What is “Event Correlation”?
- 1 The Origins of Event Correlation
- 1 How Does Event Correlation Work?
 - 1 Confirmation of multiple pieces of information
 - 2 Statistical correlation
 - 3 Pattern- or rule-based event correlation
- 2 Does Event Correlation Really Work?
- 2 How is such a program developed?
- 3 Why Event Correlation Matters
 - 1 Event correlation occurs anyway, automating it simply makes it more efficient.
 - 2 The more eyes the better.
 - 3 Event correlation help analysts weed out false alarms.
 - 4 Attacks that otherwise overlooked can be discovered.
 - 5 Missing data are not as much of an obstacle to attack detection.
 - 6 Individual understanding of what really happened can be greatly increased.
 - 7 Event correlation helps produce a manageable level of alerts.
- 4 Some Event Correlation Methods Are Better than Others
- 4 netForensics – Security Information and Event Management Solutions
- 5 Conclusion
- 5 About netForensics

What is “Event Correlation”?

To discuss why event correlation matters, it is first necessary to define event correlation. Wikipedia defines it as “a technique for making sense of a large number of events and pinpointing the few events that are really important in that mass of information.” Wikipedia goes on to say that event correlation reduces a large number of incident alerts to a much smaller, more manageable number...”

In his book *“Intrusion Detection and Prevention”*, Dr. E. Eugene Schultz defines event correlation as “associating sets of events detected through various means and applying knowledge to determine whether they are related and if so, in what manner and to what degree. This kind of correlation requires comparing observations based on different types of parameters such as source and/or destination IP address, an identifiable network route, commands entered by a suspected attacker, and the time in which activity has begun or ended. Data sources can be intrusion detection sensors, logs, databases (such as threat databases), and so forth...”

The Origins of Event Correlation:

Many individuals have the impression that event correlation is unique to information security. Nothing could be further from the truth. Event correlation is a tried and proven concept used extensively in many arenas long before information security professionals began to apply it to intrusion and threat detection. For example, event correlation, in the form of “all source datafusion”, has been used in military intelligence for longer than a half century. It has been used to identify process deficiencies and flow control problems in industrial process control and telecommunications for well over 35 years. Event correlation has also been used in systems and network management to spot systems, network devices, and applications that have crashed, are non-responsive, or are not working properly for well over 25 years. More recently, it has been successfully used in business activity monitoring and service-level management, as well as other areas.

How Does Event Correlation Work?

Event correlation works in a number of ways.

1. Confirmation of multiple pieces of information – At the simplest level, event correlation means having more than one

sensor or reporting device sending redundant information that confirms that an event (such as multiple login failures or unauthorized access to a Windows share) has occurred at a particular point in time.

2. Statistical correlation – A more complex method of event correlation is statistical correlation. This involves taking measurements on two or more variables and then calculating the degree of statistical relationship between the variables. One variable could, for example, be the number of emails sent out by a given system every day. Another variable could be the number of incoming emails to the same system. A legitimate mail server will have a large number of incoming and outgoing messages every day, something that would produce a large, positive value.

If the system in question were compromised and then a spam server were installed on it afterwards, however, one would expect a relatively low number of incoming messages but a high number of outgoing messages, something that would result in a large, negative correlation value.

3. Pattern- or rule-based event correlation – At a much more sophisticated level, pattern or rule-based event correlation means cataloging real world attack patterns and comparing them to information sent by reporting devices on the network in an attempt to identify behaviors indicative of an attack. Some of the most common forms of attacks today are those in which an attacker performs a remote vulnerability scan of another system (the “victim system”), determines the type of attack(s) to which the victim system is vulnerable, and launches one or more attacks in an attempt to exploit the vulnerability(ies).

An effective event correlation method would “see” the vulnerability scan from the attacking system (because the victim system or perhaps a nearby firewall or IDS would have reported the scan activity) and watch for any kind of follow-up attack that might launch against the victim. If the attacking system does indeed launch one or more attacks (as evidenced by the victim system’s a nearby firewall’s or IDS’s output) within a defined time limit, an alert is triggered.

Does Event Correlation Really Work?

To answer this question properly, an understanding of how things work in real-life security incident investigations is necessary. Investigations into potential security breaches are almost without exception triggered by a single potential indicator, such as an entry in an audit log or an IDS alert. An experienced investigator, however, would never accept a single as conclusive evidence of a breach. Rather he would seek additional information that would either confirm or refute the possibility that a security-related incident occurred.

For example, if an audit log entry showed access to a system from an unknown IP address occurred at 1:15 in the morning, the first thing an investigator would look for is more evidence (e.g., from an IDS or firewall) that this event actually occurred. If the event occurred is confirmed, the investigator would in all likelihood next look for evidence as to whether the intruder obtained super user level access to the system or access to sensitive files and applications. The point here is that incident investigators, intrusion detection staff, system and network administrators, as well as others engage in event correlation all the time. There is really no other way to determine whether a suspicious event constitutes a security breach, and, if so, how extensive and serious the breach is. Forcing personnel to manually investigate each event is, however, not a very efficient way to perform event correlation. A program that follows the same steps an investigator takes when dealing with potential incidents is much more time and cost efficient.

How is such a program developed?

The answer lies in analyzing how incident investigators and intrusion detection experts go about deciding whether an event, or sequences of events, constitutes an attack. This information can then be used to create a series of programmatic rules—one for each type of attack. The effectiveness of these event correlation rules are thus highly dependent on how well they reflect what incident investigators and intrusion detection experts know about attacks.

A clear example of the effectiveness of event correlation concerns a well-known sequence of events that almost without exception indicates that a successful attack has occurred against a victim system. Attackers often quickly and efficiently exploit a known

vulnerability in a victim system by making a clear text connection to that system from another system. After gaining illegal access to the victim system, attackers then very frequently install and run a hacking utility that creates a “reverse shell,” a remote access method that sets up an encrypted connection from the victim system to the system from which the attack was initiated. The result is that the attacker can now gain remote access to the victim system at will.

Event correlation is ideally suited for detecting a reverse shell—first, a remote, incoming clear text connection must occur, then a remote, outgoing encrypted connection must follow within a reasonable time period. Writing an algorithm that detects this sequence of events is not at all difficult.

Another good example of the effectiveness of event correlation concerns discovering incidents through symptoms that manifest themselves when a system has been successfully attacked and compromised. Very shortly after a break-in or malware installation, changes in critical configuration files such as `/etc/inetd.conf` or `/etc/xinetd.conf` (in Unix and Linux systems) or the Registry Run key (in Windows systems) are likely to occur.

If a series of such changes in several systems suddenly occur all at once after a known attack has occurred, this set of events provides a powerful indication that the systems in question have been compromised. Human observers are unlikely to notice the relationship of these events amidst the sheer plethora of events that occur, however, event correlation algorithms are ideally suited for detecting them. Yet another good example of how effective event correlation is can be demonstrated by detecting attacks that comprise a known pattern.

In many attacks perpetrators break into systems, escalate their privilege level and then use their elevated privileges to turn off auditing and also to delete existing audit logs, thereby covering their tracks. Event correlation algorithms are well suited for identifying these types of patterns. They must simply detect the fact that an attack against a system has occurred and that shortly thereafter auditing has been disabled and/or that one of more type(s) of audit logs has (have) been deleted. Once again, identifying this pattern of events among hundreds or thousands of others is difficult for technical staff members, but very simple

for a programmatic system. Finally, every information security professional knows that the insider threat is the most serious of all, but discovering insider attacks is also one of the most difficult challenges. Event correlation once again provides an almost ideal solution.

Many insider attacks are motivated by the desire to steal corporate secrets or customer credit card data. These attacks can manifest themselves in a number of ways, particularly in the form of remote file downloads. Event correlation algorithms can track file transfers, including file transfers across different systems, by a single user and then issue an alarm when the rate exceeds the configured threshold. To avoid triggering alarms, insider attacks often involve “slow and gradual” download rates designed to “slip under the radar” of detection systems. In event correlation such tactics do little good as the event correlation rules designed to detect multiple file transfers can simply be configured to have longer threshold time intervals.

Why Event Correlation Matters

Event correlation matters for seven major reasons:

- 1. Event correlation occurs anyway, automating it simply makes it more efficient** – Regardless of whether it’s performed by security personnel or by a security system, event correlation is used to detect and mitigate security threats. Use of a specialized system for event correlation (such as a SIEM) simply means that attacks are more likely to be detected quickly and more thoroughly than is possible with people.
- 2. The more eyes the better** – An indication that a suspicious event has occurred from one reporting device may or may not be valid. The same indication from another reporting device and perhaps even another is, in contrast, convincing. Thus, the more systems that can be monitored, the more likely one is to detect attacks.
- 3. Event correlation helps analysts weed out false alarms** – IDSs and personal firewalls tend to have inflated false alarm rates. False alarms trigger unnecessary and frustrating incident response efforts. However, individual indications of false alarms without additional indications do not cause effective event correlation rules to trigger response alerts.
- 4. Attacks that otherwise overlooked can be discovered** – Individual events that are part of an attack pattern are often innocuous. As such, they are likely to be overlooked by IDSs, firewalls, human observers, etc. Analyzing the relationship of each of these events to attack patterns through event correlation is the only reasonable approach to detecting these events.
- 5. Missing data are not as much of an obstacle to attack detection** – A favorite trick of attackers is to disable auditing and to erase audit log files, making missing pieces of attack-related evidence a normal occurrence. Effective event correlation algorithms, however, minimize the impact of this methodology because they look for a variety of patterns based on output from multiple systems, devices and applications. This means they’re able to detect attacks even when one or two pieces of evidence are eliminated.
- 6. Individual understanding of what really happened can be greatly increased** – Event correlation facilitates analyzing the origin and extent of an actual or suspected incident. Correlation of event-related information can lead to a thorough understanding of the nature of an incident and its potential impact. This aids the identification and initiation of effective response strategies that limit damage and mitigate the cause of security-related incidents.
- 7. Event correlation helps produce a manageable level of alerts** – One of the most distracting and bothersome aspects of incident investigation and detection is being bombarded with alerts - something that inevitably occurs without event correlation. Because event correlation is based on indicators from multiple events following known patterns, the number of alerts issued is dramatically reduced allowing personnel to focus on actual events rather than eliminating false positives.

netForensics – Security Information and Event Management Solutions

netForensics SIEM solutions afford organizations greater threat visibility, better security intelligence, and more effective response. And with broad security intelligence, organizations are not only more secure, but also able to achieve and maintain compliant operations.

netForensics patented correlation technologies go beyond simply logging security information, and speed threat identification and provide an accurate picture of risk. These technologies are architected to handle the massive volume of security information from network-related sources as well as server logs, applications, databases, and identity management systems, and pinpoint attacks from the inside and beyond based on a thorough understanding of network and user activity. Our correlation technologies process massive volumes of data from the perimeter down to the core to identify real-time threats and historical patterns. Organizations can clearly see threats that would otherwise go undetected.

nFX SIM One™ is the only SIM solution in the industry to employ four different types of correlation technology to ensure that the real threats are identified rapidly. Multiple layers of event correlation ensure that organizations can obtain unprecedented security visibility and easily identify suspicious patterns of activity that would otherwise go unnoticed. SIM One is designed to efficiently process the high volume of data that comes from security and network devices, core applications, and databases. Only SIM One provides this powerful, all-in-one correlation capability for addressing historical, real-time, and potential threats.

Rules-Based Correlation – The SIM One rules-based correlation engine can perform 100 million state checks per second, so you can make sense out of massive amounts of data in real time. Importantly, SIM One allows users to apply conditional logic to identify zero-day as well as most-likely attack scenarios. SIM One is the only SIM solution to implement multi-state rules that require meeting a series of conditions within a specified time period prior to an alert being issued. This protocol reduces the number of rules security analysts must write and maintain – since rules for a particular vulnerability can be nested – and also reduces the number of false positives.

Vulnerability Correlation – SIM One is one of the only SIM solutions that supports vulnerability correlation without writing rules. Security teams can immediately reap the benefits of vulnerability correlation, identifying potential threats to high-value assets by correlating scanner and IDS data. Security personnel can also prioritize patching efforts to reduce risk without losing time writing and maintaining rules.

Statistical Correlation – SIM One applies statistical algorithms out-of-the-box to automatically determine incident severity, assigning a threat score based on asset value. Statistical correlation analyzes network behavior and identifies threats based on the presence and severity of anomalous event patterns.

Historical Correlation – With historical correlation, security analysts can identify repeating patterns of attacks, as well as automated and slow attacks that may be veiled within millions of raw security events. Historical correlation allows for quick detection of previously unrecognized malicious events, adding another level of defense to your security program. With the ability to review past events, analysts are better positioned for real-time detection of future zero-day attacks.

nFX Cinxi One™, netForensics line of hybrid SIM and Log Management appliances, are fast, effective and exceptionally affordable. Easy to deploy and use, all Cinxi appliances feature advanced correlation technologies and real-time monitoring for rapidly identifying and prioritizing threats. Add to that, comprehensive log collection, documentation and storage, and organizations can now cost-effectively meet compliance demands while enhancing their overall security posture. Cinxi offers flexible deployment options to accommodate any size networking environment.

MetaRules Intelligent Correlation and Analysis – Security threats aren't getting any less complex, which is why signatures and low-level event rules are no longer effective for identifying network attacks. Cinxi counters those increasingly sophisticated threats with an intelligent event correlation engine and proprietary MetaRules. MetaRules go well beyond simple rules and signatures by incorporating an advanced logic system that performs real-time attack detection through identification of threat pattern sequences and behaviors across disparate network devices. This means Cinxi can deliver faster, more accurate security event correlation and alerting while virtually eliminating false positives.

Vulnerability Scan Integration and Correlation – By incorporating vulnerability data from an existing database of known vulnerabilities, as well as vulnerability assessments from products such as Nessus, Qualys and McAfee Foundscan, Cinxi provide actionable intelligence on the true threats to critical assets. Based on these correlated events, Cinxi can alert administrators to the incidents that have the potential to exploit your systems. With these capabilities, IT managers and security specialists have everything they need to detect, respond, and resolve even the most sophisticated security events when and where they happen.

Conclusion

Event correlation technologies provide a myriad of benefits in addition to simplistic log management products which merely collect and store logs. These log management products make it incumbent on security staff to attempt manual event correlation, virtually assuring that any attack or breach, if discovered, will only be discovered long after it has occurred. Automated, real-time event correlation is an essential component of an effective security practice and should be part of all security strategies and operational policies. netForensics', the pioneer of SIM technology in 1999, leads the industry with patented event correlation technologies that provide a proactive means to discovering attacks as they occur and enable a rapid response - before real damage occurs.

About netForensics

netForensics delivers security compliance solutions that help stop the ever-increasing attacks that threaten organizations. netForensics not only solves security compliance challenges, but provides the proof needed to address the myriad of regulatory and internal governance requirements.

netForensics' solutions enable governments and organizations address external and internal threats, mitigation, log management and reporting. Governments and companies of all sizes around the world rely on netForensics to gain unparalleled security visibility, prevent costly downtime, and maintain compliant operations.