HP ARCSIGHT EXPRESS 3.0

Security Intelligence for a Faster World

HP Enterprise Security Business Whitepaper

ENTERPRISE SECURITY

Overview

The amount of digital data is exploding exponentially. It is being generated, transmitted and exchanged much faster, by more sources and in different formats than ever before. At the same time, the number of attempts to infiltrate organizations to steal and profit from the unauthorized use of critical data is skyrocketing. Not only are financially motivated criminals conducting more attacks on organizations, there has also been a dramatic increase in the number of data theft attempts by nation states and politically motivated hacking groups.

Along with the spike in data theft incidents, there has also been a dramatic increase in the complexity of the methods that malicious hackers create to execute these attacks. The average attack now has eight attack vectors, compared to just two a few years ago. Specialist groups are developing and bringing different techniques together in an organized fashion – combining several customized pieces to target software and application vulnerabilities and holes in network protocols. And, they use combinations of technological and social engineering tools to execute data breaches.

This whitepaper describes a fundamentally new technological innovation that enables HP ArcSight SIEM solutions to maintain the security of organizational IT assets by detecting more incidents and addressing larger sets of log data.

An Explosion of Data

Eric Schmidt, the former CEO of Google, stated that we now create as much data in just two days as we did from the dawn of man until the year 2003[1]. This means that over 90% of all data that exists today has been created in the last two years alone.

This data is being generated from a wide variety of sources and includes both personal consumer data and business data. Consumer data consists of personal content, like photographs and videos, social media activity and communication exchanges via electronic means, including email, voice and text data. Business data includes email, transaction records, online and debit/credit/electronic purchases, customer data, health information, click streams and countless other records used by organizations to operate on a daily basis.

All of this data crosses multiple information technology systems during different stages of creation, use and storage. These transactions result in numerous log events generated on the IT systems creating, transmitting and housing this data, which directly translates into a corresponding explosion of log data. Processing all of this additional log data for security and storing it for compliance and forensics is starting to pose a problem for current SIEM solutions.

- IDC estimates that in 2011, it will take only seconds to create one petabyte of new data[2].
- Data will grow at a rate of almost 40% every year, according to the McKinsey Global Institute[3].
- Verizon and the United States Secret Service investigated 800 new compromise incidents in 2010. In contrast, the entire dataset from 2004 to 2009 was just over 900 incidents![4]

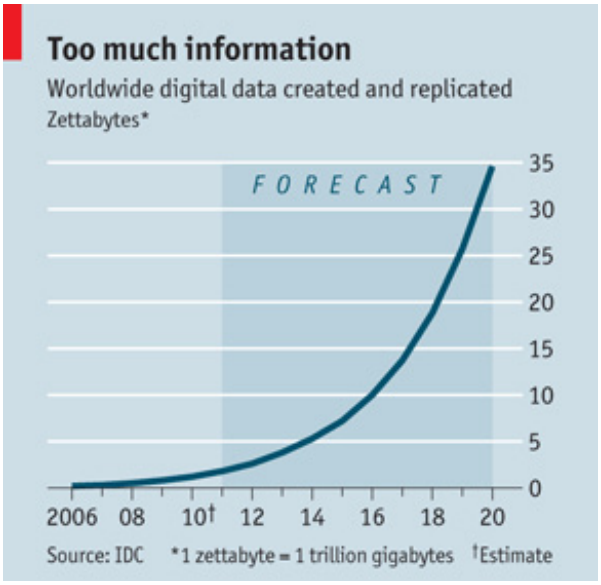

Figure 1. Annual data creation is growing exponentially. (Source: IDC Digital Universe Report, 2010)

Risks Associated with Big Data

In September 2010, authorities in London arrested nineteen people for fraud and the theft of approximately $30 million of digital assets.[5] The leader was 20 years old and conducted the operation from a single laptop using the Zeus Trojan, a piece of malicious software designed to covertly steal banking information. Incidents like these are commonplace because of the vast amount of information and the many different systems involved when conducting the simplest business transactions. Hackers use this complexity to commit fraud and illegally benefit at the expense of individuals and corporations.

With the exponential growth of digital data, event log data created by the systems processing it has grown proportionally. Existing SIEM technologies are finding it harder and harder to scale efficiently with the log data, and to process, correlate and prioritize incidents effectively.

1 http://techcrunch.com/2010/08/04/schmidt-data/
2 IDC 2011 Digital Universe Report
3 http://www.mckinsey.com/mgi/publications/big_data/pdfs/MGI_big_data_full_report.pdf
4 Verizon/United States Secret Service Data Breach Report, 2011
5 http://news.softpedia.com/news/ZeuS-Gang-Responsible-for-30-Million-Fraud-Busted-in-UK-158579.shtml

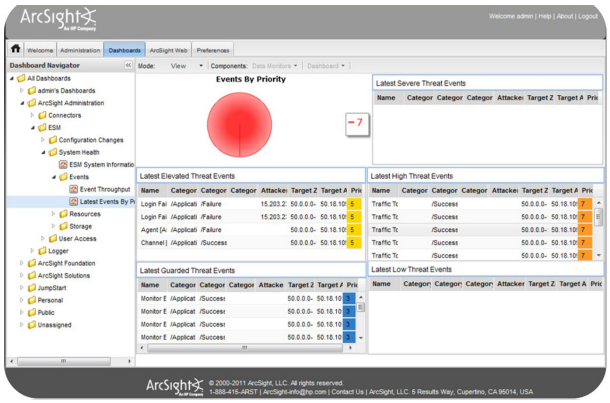

Figure 2: HP ArcSight Express enables accurate prioritization and alerting for very large data sets and event log volumes.

Figure 3: HP ArcSight Express 3.0 includes a new administrative console that simplifies SIEM system management.

HP ArcSight Express delivers a breakthrough technological innovation to address the problem of increased log volumes. This innovation, called the ArcSight Correlation Optimized Retention and Retrieval Engine (CORR-Engine), moves away from the limits of a relational DBMS. It provides the ability to correlate larger sets of log data faster than ever before, to scale to higher log processing volumes, and to archive larger volumes of log data for extended periods using an efficient data store.

By combining the ArcSight market-leading correlation engine with the precise capability of the CORR-Engine security, analysts are finally able to keep pace with the speed and volume of streaming log data, and at the same time, reduce the risk they face in a high-speed threat environment.

Correlation-Optimized, Retention and Retrieval Engine

The HP ArcSight Express CORR-Engine replaces the traditional RDBMS-based data store to deliver the scale and speed required by SIEM solutions to deal with the new threat landscape – one in which attacks targeting organizations are much faster, are propagating across many different systems and involve many more attack vectors.

The ArcSight CORR-Engine is a revolutionary solution for high-speed correlation and long-term data retention. It moves away from the limitations of a general-purpose RDBMS, to a data store that is optimized to support the extremely rigorous demands of speed, scalability and storage efficiency when dealing with large volumes of streaming log data.

The ArcSight CORR-Engine uses a highly customized flat file repository with a "write once, read many" approach to remove the traditional RDBMS bottleneck that prevents high-speed correlation. With this bottleneck removed, the ArcSight in-memory correlation engine can ingest log events at much higher rates – up to three times faster under normal conditions and up to five times in burst scenarios compared to the previous version of ArcSight Express on similar hardware.

The ArcSight CORR-Engine also enables extremely fast data retrieval for forensic analysis and compliance reporting, delivering up to five times the read performance when compared to the previous version of ArcSight Express running on similar hardware. With the HP ArcSight Express correlation capability, analysts are able to focus on the events that matter most. It empowers security, compliance and anti-fraud personnel to quickly identify and prevent network and security attacks from a single unified correlation and analysis console.

The ArcSight CORR-Engine is part of an integrated security event collection, correlation and archival system that works together to deliver a powerful defense to protect against faster and more complex threats. This system includes:

- **HP ArcSight Connectors**
  ArcSight Connectors provide universal data collection from over 300 unique devices without the need to deploy agents across the enterprise. The data is normalized and categorized into the ArcSight Common Event Format (CEF) for easy correlation and analysis. The ArcSight Connector architecture enables future-proof monitoring, as the system will continue to work even when network technologies are swapped out and replaced with those from new vendors.

- **Regulation-Specific Compliance Packages**
  ArcSight Express 3.0 enables faster compliance reporting through the use of pre-built, regulation-specific Compliance Insight Packages that include rules, reports, alerts and dashboards for specific regulations. The content necessary for audits for a variety of standards and mandates (SOX, HIPAA, PCI, NIST, and FISMA) are built in to the product in a simple, easy-to-read fashion. Security administrators no longer have to spend days or weeks merging data from several different sources for the auditor. With ArcSight Express, organizations gain the ability to satisfy auditors faster and more cost effectively than ever before, and are prepared for any additional mandates that may be passed in the future.
- **HP ArcSight Threat Response Manager**
  ArcSight Express 3.0 works with ArcSight Threat Response Manager (TRM) to give security administrators the ability to respond faster to incidents, reducing the impact an event has on the company operations. Through the TRM module, ArcSight Express creates the best threat mitigation plan for each enterprise. Once the plan is approved, organizations can execute on that mitigation plan and document the changes taken. This shrinks the response time to seconds and provides a documented record for rollback or IT audits.

Summary

Organizations are now faced with orders-of-magnitude more business data and the resultant log data than they did just a few short years ago.

The HP ArcSight Express CORR-Engine is based on a breakthrough architecture that is capable of processing the abundance of log data generated by business systems today. Using ArcSight Express 3.0, security analysts are now able to detect the increased volume of complex multi-vector security incidents as soon they happen. The ArcSight CORR-Engine also makes this data available for automated compliance reporting and faster time-to-resolution through an intuitive, workflow-driven response.

ArcSight Express 3.0 with the CORR-Engine addresses today's security threats, improves compliance reporting, and enables organizations to process larger amounts of data with fewer resources.

ESP-BWP013-040109-02, Created September 2011