Hewlett Packard Enterprise

Analyze structured and unstructured data for complete security intelligence

HPE IDOL packs for HPE ArcSight ESM

What is IDOL?
HPE IDOL is an information analytics technology that helps you index, search, and analyze human information at scale and in context. It features over 400 data connectors that enable you to access a broad range of enterprise and cloud data sources. You can also use over 500 functions to process information in over 1,000 file types (including tweets, email, images, audio, and video). IDOL's patented pattern-matching technology helps you discover insights that you did not know to look for.

What is ArcSight ESM?
HPE ArcSight ESM is a premier security event management solution that enables you to store, analyze, and correlate millions of events for security event monitoring, from compliance and risk management to security intelligence and operations. ArcSight ESM sifts through millions of log records, correlates them, and provides identity and asset context to find the critical events that matter, in real time, via dashboards, notifications, and reports. ArcSight ESM enables you to accurately prioritize security risks and compliance violations. ArcSight ESM was rated a "Leader" in the most recent Magic Quadrant report by Gartner on SIEM.

Gain unprecedented visibility and context around electronic information and security events

The ability to analyze massive amounts of data—both structured and unstructured—has quickly become all but mandatory for large organizations that must effectively protect themselves against malicious activity. The exponential growth of data has made it more difficult to quickly analyze and derive actionable intelligence that can be used in the security domain.

Today's security analysts typically rely on tools such as Security Information and Event Management (SIEM) systems and log management solutions, both of which focus primarily on the collection and correlation of real-time audit logs from network devices, operating systems, and applications. However, there is a growing need to complement these solutions with more powerful analytics capabilities that can identify anomalies and suspicious activity, as attacks become more sophisticated.

HPE IDOL (Intelligent Data Operating Layer) packs for HPE ArcSight ESM (Enterprise Security Manager) combines IDOL's ability to understand unstructured data with the market-leading SIEM capabilities of ArcSight ESM to give you unprecedented visibility and context around electronic information and security events. Using the solution, you can understand typical data feeds, which include unstructured data such as social media and emails, and structured data from sources such as security devices, and identity and access management systems.

Highlights

- Detect targeted attacks and breaches by combining event data with contextual information found in social media and email content
- Monitor possible data loss by correlating structured and unstructured data from multiple security devices
- Discover negative sentiment in social media and email content
- Access and understand multiple sources of information

There are currently two versions available:

- IDOL Email Analytics Pack for ArcSight ESM monitors high risk users' emails and email attachments for suspicious keywords. This can trigger an alert in ESM, prompting the analyst to drill into the email from the console to quickly validate or dismiss the threat.
- IDOL Social Media Analytics Pack for ArcSight ESM monitors social media identities for negative sentiment about the company. This can trigger alerts in ESM that may signify an impending botnet or other attack.

Today's information security challenges

Today's threat-laden security landscape is more complex than it has ever been. Malicious security breaches are nearly an everyday occurrence. Our headlines are dominated by financial hackings, whether targeting celebrities, wholesale customers, or entire retail organizations. Alongside this news, there are discussions about the impact of cyber warfare on US-China relations. The unfortunate reality of these actions is that the motivations for such activities are numerous, and the perceived rewards are significant.

Together with an evolving threat landscape, there have been many advancements in enterprise IT that contribute to security risks. These advancements have transformed the way information is consumed and the way people interact with mobile devices, the cloud, and social media—all events that have increased the attack surface exponentially, resulting in the following:

- The growth in the number of targets has increased the likelihood of success for our adversaries.
- You are truly only as strong as your weakest link when it comes to information security.
- Protecting your information has become more challenging than ever.

Evolve your strategy to meet today's threats

By applying next-generation capabilities to security challenges, you can move from a reactive approach to one that is more proactive, to eventually derive predictions on potential targets and threats based on incoming information. Specifically, Big Data can be used to find better security intelligence from social media outlets and get a clearer picture of the who, what, when, how, and where.

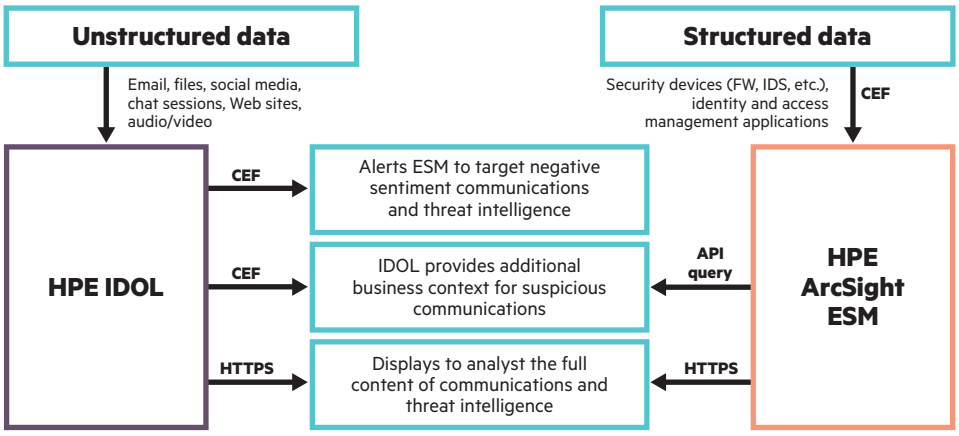
One way to get ahead of the threat curve is to use technology that understands unstructured content. Second, it is possible to start to understand the sentiment of communications to identify potential threats such as numerous negative-sentiment emails being sent from a disgruntled employee. You can also understand the specific business context of data that's leaving the organization, for example, is the data from HR, classified, or proprietary? One way to spot these signs is by analyzing the attachments in emails (and the actual emails) or chat sessions to identify a loss of sensitive data, perhaps before it occurs.

IDOL and ESM: market leaders in Information Analytics and SIEM

The integration of IDOL and ArcSight ESM offers a wide range of capabilities, including the ability to:

- Detect negative sentiment in social media and email content
- Monitor possible data loss by correlating structured and unstructured data from multiple security devices to get a complete picture
- Access and understand multiple sources of information
- Use sophisticated and granular sentiment analysis the solution can be set to alert an analyst of possible intellectual property/data loss and/or possible attacks.

What is Common Event Format?
The Common Event Format (CEF) is an open log management standard, created to simplify log management challenges. It uses a standardized format, allowing you to easily collect and aggregate data for analysis by an enterprise log management system.



As an example of how you can use the IDOL/ArcSight ESM solution, when IDOL detects an email or social media thread containing negative sentiment, it generates an event in the Common Event Format (CEF) and sends it to ArcSight ESM. Another example, IDOL can analyze information to provide additional business context regarding communications going in or out of an organization. For instance, IDOL can analyze the body of an email, the attachments, and the recipients to provide additional context beyond the subject line.

Bi-directional integration
The integration between HPE IDOL and ArcSight ESM is bi-directional. Therefore, an analyst using ArcSight ESM can query IDOL for additional information regarding an event the analyst has seen in ArcSight, and IDOL can send CEF events to ArcSight. This can be a powerful tool in facilitating an analyst's investigation into an incident.

The IDOL/ESM integration consists of a content bundle, open source tool (lynx), and CEF connector on the ESM side, as well as connectors to the email server, Web Services, and the HPE IDOL engine.

Much more than a DLP solution

The IDOL/ESM integration provides all the capabilities of a data loss prevention (DLP) solution, but adds sentiment analysis, and in some cases, predictive analysis that can be used to determine the loss of sensitive data and/or potential internal or external threats—all through single pane of glass. IDOL can provide statistical weight, without going to the data source, and can categorize the data leak type (for example, HR, R&D, Finance data) along with a view of the data leaked.

Use case #1: Social media monitoring for negative sentiment

Let's assume that a current employee has posted a review on Glassdoor (an employer review site) expressing dissatisfaction with his or her current employer and the possibility of leaving to go work for a competitor. IDOL has detected this post and sent an event in CEF to ArcSight ESM, where a correlation rule is triggered and an analyst is alerted to the incident.

Unfortunately, at this point, the analyst does not know who posted this, as these reviews are anonymous. Using HPE ArcSight Identity View and logs collected by ArcSight from the proxy, it can be determined that at approximately the same times as this post was created, the user jsmith, who is a presales engineer, visited this exact post.

Using this information, the company can be alerted that this employee is a flight risk and then monitor the employee for insider threats.

Use case #2: Email monitoring for potential data loss

IDOL has been monitoring the Exchange server inbound/outbound database in real time and indexing user emails and attachments to build business context regarding the subject and sentiment of the email. IDOL has sent ArcSight ESM an alert identifying a potentially suspicious email containing source code from the disgruntled employee who posted the Glassdoor review.

Upon further investigation within ArcSight ESM, using logs collected from Exchange, the analyst determines that this same user emailed the source code to the user's personal account. Given the earlier posting to the employer review site, it may be that this employee is looking to take some code if the employee leaves and joins a competitor. Using these tools, an analyst can detect this and avoid a potentially devastating scenario.

Use case #3: Social media monitoring for hacktivist threats

IDOL has been configured to crawl social media feeds and known hacktivist IRC channels for threads containing an organization's name and information related to malicious activities. When a thread is detected, a CEF event is sent to ArcSight ESM alerting an analyst of this potential DDOS attack, along with the poster's handle and the sentiment evaluation of the post.

The analyst can access the URL from the ArcSight console and read the thread. After investigating, if the analyst believes there is indeed an attack being planned on the company and other similar companies, proactive action can be taken to tighten up firewall rules, update IDS and AV signatures, and host vulnerabilities to fend off the attack.

Summary

By combining the ability to analyze unstructured data using HPE IDOL with the powerful correlation engine of ArcSight ESM, along with the enhanced interoperability made possible by the Common Event Format, HPE IDOL packs for ArcSight ESM provide organizations with actionable information that enables proactive action against potentially compromising activities. This level of analysis goes far beyond what is provided by SIEM solutions alone, and helps you to stay vigilant in today's challenging environment.

Learn more
hpe.com/idol

Sign up for updates

Hewlett Packard Enterprise

4AA5-8322ENW, February 2017, Rev. 1