ScienceDirect

Network Security
Volume 2021, Issue 4, April 2021, Pages 7-16

Feature

A threshold-based, real-time analysis in early detection of endpoint anomalies using SIEM expertise

Sivaraman Eswaran, Aruna Srinivasan, Prasad Honnavalli

Show more

Share Cite

https://doi.org/10.1016/S1353-4858(21)00039-8
Get rights and content

IT functions in organisations produce enormous quantities of data, logs and events. In the current IT world, handling a large amount of data is a challenging task and it is the responsibility of network administrators to transmit and store the data securely. If any data is disclosed or tampered with by an attacker, either locally or remotely, then the impact can be very high. To overcome this, firewall and intrusion detection system (IDS) and intrusion prevention system (IPS) solutions are used to verify all packets on the network.

Section snippets

Understanding security

A security information and event management (SIEM) system provides a security analysis procedure to understand the overview of security in an organisation. SIEM tools collect, analyse, normalise and correlate all files and evaluate incoming data from various sources, resulting in a centralised view of logs. For a SIEM to function well, you need to understand the format of the log-line that the SIEM system should process next. Due to complications in uniquely identifying the logs at run-time, …

Threat intelligence

It is difficult to predict the wide range of objectives and methods used to accomplish attacks. Traditional cyber security approaches are not enough in this scenario. Organisations need to recruit cyber security professionals to extract threat intelligence to uncover unknown threats and build defensive mechanisms in advance to protect their IT assets. Threat intelligence is the process of recognising or determining any ‘unknown threats’ that the organisation can identify, and defence mechanisms …

Existing work

SIEM offers real-time analysis of security alerts produced by network devices and applications. Security event management (SEM) deals with real-time monitoring, correlation of events, notifications and console views. The other part is security information management (SIM), which delivers long-term storage, analysis and reporting of log data.15, 16

A SEM system centralises the storage and exploration of logs and allows real-time analysis that enables the security analyst to quickly take …

Splunk server

Having the vision statement, “To make machine data accessible, usable and valuable to everybody”, Splunk provides a wide range of products to convert machine data into valuable information by monitoring and analysing all activities. This process is known as operational intelligence, which is an exclusive value proposition of Splunk.

Splunk IT Service Intelligence uses event analytics and machine learning to make operations simpler, rank problem resolution and align IT with the business.[20] It not …

Configuring the forwarder

Configuring the forwarder should be done before it is used for forwarding data. A configuration tells the forwarder what data to send and where to send it. As the universal forwarder does not have Splunk Web, a configuration has to be done during the installation (Windows systems only). To perform post-installation configuration:

- Use the command line interface (CLI) that allows you to do almost all configuration in a minimal number of steps, but does not provide complete access to the …

…

Tracing C2 servers

The network is the medium for all device communications, thus network sources such as the firewall and proxies contain complete details of all activities among users and hosts. For example, a web proxy contains all records of all web communications between an internal host and any external web servers. Analysing web proxy data traffic events can help determine malicious activities in the network such as whether command and control (C2) activities are happening in the network.[23] Security …

Threat detection

Splunk enables rapid security investigation and analysis. It can immediately help the user to identify an indication of compromise and quickly determine the scope and the cause of threats, such as the patterns of authentication failure across the entire infrastructure which reveals potential bad actors.[24] Using Splunk's Search Processing Language (SPL) search command, you can check for any event with a failed password in the event logs. As you search for the keyword ‘fail’, Splunk SPL searches …

Threat validation

Within our search results, Splunk allows for further analysis by providing drill-down capabilities that provide full context for the analysis. Note that we need to add the source IP address as an additional search condition, resulting in a focused search with all failed password activity from that workstation.

The result of this drill-down search shows actual raw events from different web servers interacting with this workstation: these activities serve as our evidence for validating the threat. …

Scoping

By analysing the scope and impact of activities initiated by the host, we can pinpoint the nature of activities by the attacker to make an accurate determination about how to remediate threats. To make some conclusive mitigation decisions, initially verify where the access attempts were successful, what credentials and privileges were used and what actions were applied to the targeted system database.

Focused drill-down is a fast way to validate specific incidents by rapidly selecting groups of …

Proposed system

The experimental testbed (Figure 3) consists of a Splunk SIEM tool and Windows host machines H1, H2, …, HN. Splunk accumulates all the logs from the connected network devices. Splunk Forwarders are installed manually in all host machines. The Splunk forwarder collects and sends the event logs to the central SIEM server. The Splunk server monitors several devices for different logs such as system logs, application logs, windows event logs, etc.

The data flow diagram proposed system is showed in …

Experimental results

As an attack unfolds, infections can create a complex chain of activities that makes it difficult to scope the potential impact. By applying statistical approaches to our data, the baseline of all activities can be calculated to isolate the outliers caused by ransomware.

Since we do not know the pattern of malicious activity, we cannot explicitly define the event patterns. Hence we want to search for the baseline activities that indicate the compromise. The solution is to analyse the anomalies …

Step 1: Collect sysmon events

From the system data, let us select events with event codes equal to 1 that represent 'process has started', as shown in Figure 6. Here we need to analyse all the process start events, and events with long command-line arguments. It requires the calculation of every process command-line argument length, and the average of argument and standard deviation of length per host, which was used to compare the current process argument length. With the threshold, we calculate – based on average and …

Step 2: Calculate command length anomaly

We create a new field based on either a calculation or a transformation. This allows us to define formulae without having to develop code outside of Splunk to address the need for specific data transformation. This eval command creates a new field called command line cmdlen, which calculates the length of the command line field. For each calculation, the length of the variables uses the eval function for the command line field, as shown in Figure 7. …

Step 3: Compute baseline

To find the baseline for comparison, we employed eventstats to calculate the average command-line length per host and stdev(cmdlen) to calculate the standard deviation of the command-line length. These calculated numbers were to identify the outliers.

The result of eventstats puts additional calculated fields in the field's panel. By using the eventstats function, we are calculating each average and standard deviation based on each host. In other words, each host will have its calculated …

Step 4: Calculate average and standard deviation

Now, with these calculated numbers, we can apply the stats command to aggregate the summary of necessary fields, summarising them by the host and command-line length, as shown in Figure 9. The stats command converts the view into statistics view, displaying the results in a tabular format, showing the analysis of various command process argument lengths. The result of the stats command shows each host and command line with its command-line length span, the host's average command-line length and …

Step 5: Define threshold value

To define the threshold value f(x), where we look for any activity with a command-line length of four times the average and the standard deviation of command-line length per host (avgperhost and sdperhost), shown in Figure 10.

The eval command has been used to define a calculated field called the threshold. After evaluating the command length, a rule has been written to detect the events crossing the threshold value, as shown in Figure 11. The threshold value f(x) is calculated as follows: ***f*** …

Step 6: Threat detection, investigation and validation

From the calculation of the previous step, here we compare the current event's command-line length (ie, maxlen) with the host's command-line length (ie, f(x)). Using the 'where' command, we filter events, where the current process's command-line length is larger than the threshold.

The result in Figure 12 shows that we8105desk host has executed the command with a command-line argument 4,490 characters long. The average and standard deviation of command-line arguments on this host appear to be …

Conclusion

In this article, a real-time zero-day anomaly detection and isolation system is formulated. The proposed system is a blend of signature, statistical and behaviour-based detection techniques. This addresses the real-time anomaly with current approaches in zero-day attack detection.

Our experimental analysis provides an overall solution to security concerns, using the Splunk SIEM. This solution aids in analysing the anomalies and the granular activities occurring on the endpoint. The work can be …

About the authors

Dr Sivaraman Eswaran received an ME degree in computer science and engineering from Karpagam University, India in 2013 and a PhD degree in computer science from Bharathiar University, India in 2019. He is currently working as associate professor with the Computer Science and Engineering Department, PES University, Bangalore. He is a research member of the Centre for Information Security, Forensics and Cyber Resilience (ISFCR) at PES University. He is a CompTIA Security+ …

…

…

Recommended articles

References (28)

Ying Lin *et al.*

‘The design and implementation of the host-based intrusion detection system’

Liu Jiang *et al.*

‘Design and implementation of network forensic system based on intrusion detection analysis’

Yong-Ho Kim *et al.*

‘A study on cyberthreat prediction based on intrusion detection event for APT attack detection’

Multimedia Tools and Applications (2014)

Duc Le *et al.*

‘Exploring anomalous behaviour detection and classification for insider threat identification’

International Journal of Network Management (2020)

Aaron Zimba *et al.*

‘A dive into the deep: demystifying Wannacry crypto- ransomware network attacks via digital forensics’

International Journal on Information Technologies & Security (2012)

Muddu, Sudhakar; Tryfonas, Christos; Zadeh, Joseph; Beebe Bond, Alexander; Athalye, Ashwin. 'Anomaly detection based on...

Cuckoo Sandbox — Automated Malware Analysis, home page

Falk, Courtney. 'An ontology for threat intelligence'. European Conference on Cyber Warfare and Security,...

Bingham, Skyler; Chandrakar, Mahendra; Gowin, Lawrence; Korte, Ryan. 'Systems and methods for generating network threat...

Spike Dog *et al.*

'Strategic cyberthreat intelligence sharing: a case study of IDS logs'

View more references

Cited by (15)

A method for satellite time series anomaly detection based on fast-DTW and improved-KNN

2023, Chinese Journal of Aeronautics

> *Citation Excerpt :*
>
> …Moreover, due to the limited expression ability of the threshold value method, it is unable to analyze the relationship between different sensor variables and the anomalies on the timing characteristics. It will miss the multi-variable point anomalies or the anomalies with timing characteristics.3 Model-based anomaly detection methods are also widely applied in anomaly detection.4…

Show abstract

Threat classification model for security information event management focusing on model efficiency

2022, Computers and Security

> *Citation Excerpt :*
>
> …In this section, we describe previous studies that have used neural network-based models to

> classify and detect threats. We classify previous studies for SIEM into the following categories: 1) large-scale event data management (El Arass et al. 2019; R. Andrade et al., 2018; Cinque et al., 2021), 2) signature-based threat detection (B.D. Bryant et al., 2020; Eswaran et al., 2021), and 3) machine learning (ML)-based threat detection (Kim., 2014; Lee et al., 2019; Naseer et al., al.,2018; A. Kim et al., 2020). Large-scale event data management for SIEM includes large event data processing (El Arass et al., 2019; R. Andrade et al., 2018) and unstructured event data processing (Cinque et al., 2021)....

Show abstract

The functional safety assessment of cyber-physical system operation process described by Markov chain

2022, Scientific Reports

Detection and quantification of anomalies in communication networks based on LSTM-ARIMA combined model

2022, International Journal of Machine Learning and Cybernetics

Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures

2021, Sensors

Investigation of Cyber Situation Awareness via SIEM tools: a constructive review

2021, Proceedings - 6th International Conference on Computer Science and Engineering, UBMK 2021

View all citing articles on Scopus

About the authors

Dr Sivaraman Eswaran received an ME degree in computer science and engineering from Karpagam University, India in 2013 and a PhD degree in computer science from Bharathiar University, India in 2019. He is currently working as associate professor with the Computer Science and Engineering Department, PES University, Bangalore. He is a research member of the Centre for Information

Security, Forensics and Cyber Resilience (ISFCR) at PES University. He is a CompTIA Security+ certified professional, Microsoft Certified Professional and EMC Academic Associate. He is a member of IEEE and a life member of the Computer Society of India and the Indian Society for Technical Education. He has published several research articles in refereed international journals and conferences. His research interests include cloud computing and cyber security.

Aruna Srinivasan completed her BTech in CSE from Anna University, Tamil Nadu and did her masters and received the Gold Medal for MTech in Computer Science and Engineering from Visvesvaraya Technological University in 2018. She worked in the IT industry for five years in the field of data warehousing and gained expertise on various ETL and reporting tools. She is working as an assistant professor in the department of Computer Science and Engineering and pursuing a PhD in the field of cyber forensics at the Information Security, Forensics and Cyber Resilience Centre (ISFCR), PES University. She is a CompTIA certified Network+ professional.

Prasad Honnavalli is a professor in the Computer Science and Engineering department of PES University. He is director of the PESU Centre for Information Security, Forensics and Cyber Resilience (ISFCR) and director of the PESU Centre for Internet of Things (IoT) with a focus on security. He is an accomplished executive with over 30+ years of professional experience in end-to-end programme management / delivery of multiple, large, complex system integration programmes encompassing IT technology transformation, IT infrastructure, complex cloud engagements, software development, automation, IT security, and managed services. He has published several research articles in refereed international journals and conferences.

View full text