Supplementary Materials
ChinaVis Data Challenge 2018
Mini Challenge 1 Reviewers Guide

This document provides a detailed reviewers guide for mini challenge 1, including the background of the questions, the description of the provided data, the tasks assigned to the participants as well as the potential answers with supporting evidence.

1. Submission

(1) Answer sheet: After completing the visual analysis of the provided data, the competition teams should accurately answer the questions in an illustrated manner and submit their entries in Microsoft Word or PDF format;

(2) Video: Participants need to make ONE video to explain their visual analysis process, and submit it in WMV format. The total length of the video must be less than 5 minutes;

(3) Paper: Participants are required to summarize the characteristics of their visual analysis methods in a paper, whose format requirements are consistent with the ChinaVis papers. The paper should be submitted in Microsoft Word or PDF format and its length should not exceed 2 pages.

2. Background & Analytical Questions

HighTech is an Internet company with several hundreds of employees, who are affiliated with five departments, including one finance department, one human resource department, and three development departments. The company is devoting numerous efforts to a new product. Recently, since the product is to be released, the company is sensitive to all the anomalies happened internally. To protect the core interests of the company and make sure the success of the releasement of the new product, the company executive decides to form an internal threat intelligence analysis group. The task of this group is to analyze potential security threats based on the internal gathered data within the company. In the process of analyzing threat intelligence, the complexity of data processing requires the efforts of the intelligent machine, meanwhile insider threat detection and recognition requires the experience, cognition, and judgment of human experts. Visual analytics combines human intelligence with machine computational intelligence, which is a great weapon for analysts to deal with the threat intelligence. Suppose you are a member of this group, please design and implement a visual analytics solution, to help the company solve the following analytical questions:

Challenge 1.1: Analyze the organizational structure of the company and the affiliations of all employees. (Your submission for this question should contain no more than 5 images and 500 words)

Challenge 1.2: Analyze the daily working behaviors of the employees, and illustrate the regular behavior patterns according to each department. (Your submission for this question should contain no more than 8 images and 1000 words)

Challenge 1.3: Find at least 5 abnormal events, and analyze the potential relationship among these events. Please summarize the valuable threat intelligence and illustrate how you achieved these by visual analytics. (Your submission for this question should contain no more than 10 images and 1500 words)

3. Data Description

The following data is provided to the participants: server logging in logs, web browsing logs, email logs, TCP traffic logs and punching logs.

Server logging in log: An employee can use their own workstation or jump servers to log into the servers or databases. This log records this login. For example, when using commands like SSH, SCP, applications like XSHELL, or using SFTP to transfer files, such login logs can be generated. In addition, the database login logs also can be generated when a client login in the database.

login.csv		
Name	**Meaning**	**Description**
time	recording time	--
user	user name	the user name used when conducting the login process
proto	protocol of the application	e.g. SSH, mysql, etc.
dip	destination IP	login target IP
dport	destination port	login target port
sip	source IP	login source IP
sport	source port	login source port
state	the result of the login	success or failure

Web browsing log: This log records all the internal employees' website visiting behaviors. *Time* is the log generation time; *sip* is the client IP; *sport* is the client port; *dip* is the server IP; *dport* is the server port; and *host* is the servers' domain. If the visiting is directly conducted through IP, the DNS process can be omitted and the head of HTTP records the host as null.

weblog.csv		
Name	**Meaning**	**Description**
time	recording time	--
sip	source IP	client IP
sport	source port	application port of the client
dip	destination IP	server IP
dport	destination port	application port of the server
Host	visiting host name	host field of HTTP

Email log: This log records the email servers' activities. *Time* is the sending/receiving time; *proto* is the email protocol; *sip* and *dip* are the sending and receiving IP address, respectively; *sport* and *dport* are the corresponding ports; *from* and *to* are the sender and receivers of the email. Because the content of email is private, we only provide the email subject.

email.csv		
Name	**Meaning**	**Description**
time	sending / receiving time	described in the head
proto	protocol	SMTP
sip	source IP	source IP
sport	source port	source port
dip	destination IP	destination IP
dport	destination port	destination port
from	a person who sends the email	from the header's corresponding
to	person(s) who receives the email	when there are multiple receivers, use the ";" to separate
subject	email subject	email subject

TCP traffic log: This log records all TCP connections occur within the company. *Stime* and *dtime* are the connection time and disconnection time, respectively. *Proto* is the protocol value of the IP head. *Sip* and *dip* are the connecting and connected IP address, while *sport* and *dport* are the corresponding ports. In the connection phase, *uplink_length* counts the total bytes that sip sends to the dip, vice versa for the downlink_l*ength*. An email behavior, web browsing behavior, or server logging behavior can generate one or multiple TCP records.

tcpLog.csv		
Name	**Meaning**	**Description**
stime	starting time of TCP connection	the time of receiving the first SYN
dtime	ending time of TCP connection	the time of receiving the last bytes
proto	protocol	IP header field
dip	destination IP	destination (server side) IP
dport	destination port	destination (server side) port
sip	source IP	source (client side) IP
sport	source port	source (client side) port
uplink_length	uplink total bytes number	calculating the total bytes from stime to dtime
downlink_length	downlink total bytes number	calculating the total bytes from stime to dtime

Punching log: This log records the work starting and ending time of the employees. If the *checkin* and *checkout* field are both 0, it indicates that the employee didn't come to work, which means that each absent employee also has a record. In addition, if an employee didn't come, he/she would receive an email reminder on the following day.

checking.csv		
Name	**Meaning**	**Description**
id	employee ID	--
day	date	--
checkin	work check-in time	--
checkout	work check-out time	--

4. Ground Truth

4.1 Event List

Plot Lines	Event ID	Event name	Importance Degree	Occurrence time	Event summary
Product data leakage	E1	account stealing	important	2017-11-03 2017-11-04 2017-11-06	An employee failed to log into an account frequently, but finally succeeded
	E2	product data peeping	important	2017-11-16 20:22	An Employee illegally peeped product data on a server
	E3	product data leakage	important	2017-11-24 12:43~12:44	An employee stolen confidential data and leaked out
	E4	the Spy resignation	important	2017-11-27	Employee resignation
Key asset damage	E5	database failure	medium	2017-11-16 19:22	Database failed due to a wrong operation; numerous database alarm emails were sent to employees
	E6	database maintenance	medium	2017-11-16 19:00-23:00	Database maintenance after failure
	E7	the DB Deleter resignation	medium	2017-11-27	Employee resignation
Branch events	E8	jump server event	general	2017-11-17 2017-11-21 2017-11-27 2017-11-30	Employees uploaded data to external servers through a stepping stone server
	E9	resignation event	general	2017-11-27	Employee resignation
	E10	tourist event	general	2017-11-27~ 2017-11-30	Employees left company and went travel
	E11	group activity event	general	2017-11-02 2017-11-09 2017-11-16 2017-11-23 2017-11-30	Employees collectively participated in group activity
	E12	financial department overtime work event	general	2017-11-19 2017-11-25 2017-11-26	Employees in the finance department worked overtime at the end of the month
	E13	VPN remote access event	general	2017-11-04 2017-11-05 2017-11-11 2017-11-12 2017-11-18 2017-11-19 2017-11-25 2017-11-26 2017-11-28	Employees used VPN to remotely link to the company's intranet
	E14	traffic monitoring system failure	general	2017-11-10~ 2017-11-28	A TCP traffic monitoring system bug caused the network protocol type of some mailing records are marked as http in the TCP traffic logs and smtp in the Email logs simultaneously.

4.2 Major Players

Player name	Employee id	Department	IP	Events
Spy	1487	Development 3	10.64.105.4	E1, E2, E3, E4, E6, E11
DB deleter	1376	Development 3	10.64.105.219	E5, E6, E7, E11
DB maintainer	1284	Development 3	10.64.105.95	E6

4.3 Main Plots

4.3.1 Product Data Leakage

HighTech has constantly been engaged in a fierce business competition with another company. To gain an edge in the competition, the rival company bribed P1487, an employee in HighTech's third development department. P1487, whom we call “The Spy”, was required to steal relevant data of the new product to weaken HighTech. To complete the task without being discovered, P1487 formulated a plan. Firstly, he stole a leader’s account to gain the high data acquisition right. When solving a sudden database failure, he used the stolen account to locate the target server where the product data was stored. A few days later, P1487 used the stolen account to log into a server, and used it as a jumping server to log into the target server. Lastly, P1487 uploaded the confidential data to an external server. After completing his mission, P1487 filed for resignation at the end of the month. The specific process of the main plot is shown below.

4.3.1.1 Account Stealing

P1487 attempted to log into the accounts of leaders P1080, P1211, and P1228 on November 3, 4 and 6, 2017, respectively. After several failures, P1487 successfully cracked the password of P1228’s account because of the weak complexity.

4.3.1.2 Product Data Peeping

On November 16, 2017, P1487 signed up for a company group activity, but he actually did not participate because he had to maintain a failed database server. During the maintenance process, P1487 used P1228’s account to log into the target server 10.50.50.44, to check whether the server has important data related to the release of the new product.

4.3.1.3 Product Data Leakage

On November 24, 2017, P1487 logged into the server 10.50.50.43 at 12:43 using the account of P1228. Thereafter, he used this server as a jump server to log into the target server 10.50.50.44. Lastly, he uploaded the product data to the external server 13.250.177.223.

4.3.1.4 The Spy Resignation

P1487 frequently browsed recruitment websites and received many emails from headhunters. On November 27, 2017, he filed for resignation.

4.3.2 Key Asset Damage

The third development department employee P1376, whom we called “The DB Deleter”, had already planned to resign. Therefore, he recently was absent-minded often. On November 16, 2017 at 19:22,

P1376 accidentally carried out an incorrect operation and caused a database failure on a critical server. Subsequently, two other employees in this department received database alarm emails. These three people simultaneously maintained the database that night. P1376 filed for resignation at the end of the month because of the serious effect of his misconduct. The specific process of the plot is shown below.

4.3.2.1 Database Failure

On November 16, 2017 at 19:22, employee P1376 accidentally caused a database failure on server 10.63.120.70. Thereafter, P1487 (The Spy) and P1284 received database alert emails.

4.3.2.2 Database Maintenance

The three employees, namely, P1376, P1487, and P1284, simultaneously maintained the database that night and left the company after completing the work at approximately 23:30.

4.3.2.3 The DB Deleter resignation

P1376 frequently browsed recruitment websites and received numerous emails from headhunters in this month. After the database failure event, he filed for resignation on November 27, 2017.

4.4 Branch Events

4.4.1 Jump Server Event

On November 17, 21, 27, and 30, 2017, four employees, namely, P1183, P1273, P1169, and P1151, uploaded data to the external server 13.250.177.223. Unlike P1487, these four employees were merely performing their duties.

4.4.2 Resignation Event

P1281 encountered a major family-related incident, thereby prompting him to file for resignation on November 27, 2017.

4.4.3 Tourist Event

Four employees, namely, P1149, P1352, P1383, and P1389, planned to travel together. These employees frequently browsed travel websites from November 20 to 24, 2017, and sent their leave mail to their own leaders on Friday, November 24, 2017. Their travel scheme was from November 25 to 30, 2017.

4.4.4 Group Activity Event

Every Thursday morning at 9:30, the HR department would send emails to all employees to invite them to participate in group sports exercises, such as badminton. Employees who wished to participate would reply and depart between 19:00 and 19:20.

4.4.5 Financial Department Overtime Work Event

On the weekends of November 19, 25, and 26, 2017, most employees in the finance department worked overtime due to the busy financial work at the end of November 2017 in the company.

4.4.6 VPN Remote Access Event

Eight employees, namely, P1147, P1283, P1284, P1328, P1334, P1376, P1487, and P1494, used VPN to remotely connect to the company's intranet to work overtime during the weekend. P1059 did not report to the company on Tuesday, November 28, 2017. He accessed the intranet and approved the resignation applications of two employees, namely, P1376 (The DB Deleter) and P1487 (The Spy), through VPN.

4.4.7 Traffic Monitoring System Failure

A bug in the TCP log system caused the smtp network protocol of some email records to be marked as http from November 10 to 28, 2017.

5. Reference Answers

Overall requirements:

1. Answer the questions accurately and concisely;
2. Explore answers mainly through visual analysis techniques;
3. Present and explain the answers in a visual way;
4. We encourage the participants to give any reasonable new findings other than the reference answers;
5. We encourage the participants to introduce intelligent algorithms in their entries;
6. We encourage the participants to develop novel visual analysis systems;
7. We encourage the participants to use analytical tools developed by their own team/company.

5.1 Challenge 1.1

Analyze the organizational structure of the company and the affiliations of all employees. (Your submission for this question should contain no more than 5 images and 500 words);

HighTech's organizational structure is relatively simple and clear. The company has one executive and five departments, namely the finance department, the human resource department, the development department 1,2,3. Each department has one manager and a certain number of employees. And the three development departments are divided into several teams, each of which has a team leader. Further information is as follows:

Departments	size	manager	employees（team leaders are marked in red）
Executive	1	1067	--
Finance	24	1041	1368,1347,1255,1248,1327,1439,1137,1370,1467,1226,1369,1186,1213,1451,1124, 1431,1293,1253,1342,1498,1108,1180,1346
HR	18	1013	1104,1499,1371,1184,1251,1295,1312,1433,1165,1300,1378,1473,1118,1363,1249, 1110,1149
Development 1	88	1007	1087, 1151, 1220, 1286, 1141, 1494, 1373; 1115, 1233, 1423, 1471, 1243, 1491, 1464, 1169, 1408, 1183, 1425, 1357, 1459, 1455; 1230, 1167, 1182, 1354, 1265, 1129, 1252, 1223, 1404, 1200; 1172, 1132, 1490, 1246, 1466, 1475, 1314, 1397, 1436, 1480, 1257, 1345, 1477; 1192, 1282, 1403, 1303, 1210, 1340, 1140, 1484; 1199, 1348, 1391, 1278, 1197, 1486; 1092, 1270, 1344, 1112, 1308, 1301; 1125, 1307, 1398, 1113; 1224, 1281, 1275, 1406, 1323, 1102, 1299, 1134, 1326, 1106, 1416, 1205, 1195, 1221, 1495, 1393, 1429, 1351, 1417;
Development 2	62	1068	1154, 1176,1315, 1152,1420; 1191, 1428, 1483, 1469, 1156, 1456, 1204, 1435; 1207, 1189, 1330, 1319, 1296, 1399, 1263, 1103; 1100, 1139, 1481, 1385, 1147, 1321, 1493, 1458, 1170, 1379, 1305, 1234,1362, 1405, 1159, 1474; 1098, 1343, 1127, 1496, 1277, 1334; 1209, 1460, 1126, 1322, 1339, 1388, 1349, 1153; 1060, 1359, 1457, 1328, 1145, 1306, 1440, 1396, 1446, 1336;
Development 3	106	1059	1080, 1364, 1181, 1449, 1311, 1193, 1422, 1194, 1297, 1384, 1376; 1211, 1411, 1287, 1382, 1231, 1365, 1284, 1497, 1164; 1101, 1356, 1241, 1461, 1313, 1352, 1175, 1350, 1179, 1338, 1325;

			1143, 1434, 1380, 1438, 1367, 1355, 1279, 1163, 1324, 1304, 1381, 1217; 1119, 1135, 1238, 1244, 1268, 1401, 1148, 1274, 1360, 1390, 1291; 1155, 1421, 1216, 1470, 1409, 1462, 1444, 1332, 1206, 1283, 1389, 1267; 1058, 1261, 1171, 1333, 1424, 1445, 1450, 1202, 1130, 1383, 1245, 1489; 1228, 1290, 1465, 1178, 1177, 1174, 1394, 1487, 1273; 1096, 1402, 1478, 1239, 1500, 1254; 1079, 1262, 1395, 1219, 1482; 1057, 1173, 1374, 1410, 1361, 1150, 1142;

5.2 Challenge 1.2

Analyze the daily working behaviors of the employees, and illustrate the regular behavior patterns according to each department. (Your submission for this question should contain no more than 8 images and 1000 words);

We recommend to discuss the employees' work behaviors by department. You can find the priorities of each department from their differences in working hours, mail topics, commonly used servers and preferred websites. Further information is as follows:

Departments	Work Time	Accessible Servers	Preferred Websites (traffic to the sites are arranged in descending order)	Description
Finance	08:00-17:00	10.63.120.70(OA), 10.5.71.60(Email),	email.hightech.com, OA.hightech.com, www.baidu.com, www.google.com, ju.taobao.com, www.so.com, www.bankcomm.com, ai.taobao.com, store.apple.com, ent.163.com.	The work of this department is mainly related to finance
HR	09:00-18:00	10.63.120.70 (OA), 10.5.71.60 (Email),	email.hightech.com, OA.hightech.com, www.google.com, www.yahoo.com, www.baidu.com, ai.taobao.com, www.ccb.com, china.alibaba.com, ju.taobao.com, www.baihe.com.	The work of this department includes attendance, performance appraisal, welfare guarantees, and recruitment.
Development 1	09:00-18:00	These servers are frequently accessed: 10.5.71.60(Email), 10.63.120.70(OA), 10.50.50.26(git), 10.50.50.27(jira), 10.50.50.28(lib01), 10.50.50.29(lib02) These servers are also accessed: 10.7.133.15, 10.7.133.16, 10.7.133.18, 10.7.133.19, 10.7.133.20, 10.50.50.33, 10.50.50.37, 10.50.50.38, 10.50.50.40, 10.50.50.43,	email.hightech.com, git.hightech.com, OA.hightech.com, jira.hightech.com, lib01.hightech.com, lib02.hightech.com, www.baidu.com, www.programmer.com.cn, www.ruanyifeng.com, www.yahoo.com.	This department is mainly responsible for development and technology sharing. (There is no significant difference in the responsibilities of the three development departments)

		10.50.50.46, 10.50.50.48, 10.50.50.49.		
Development 2	09:00-18:00	These servers are frequently accessed： 10.5.71.60(Email), 10.63.120.70(OA), 10.50.50.26(git), 10.50.50.27(jira), 10.50.50.28(lib01), 10.50.50.29(lib02) These servers are also accessed： 10.7.133.15, 10.7.133.16, 10.7.133.21, 10.7.133.22, 10.50.50.30, 10.50.50.31, 10.50.50.33, 10.50.50.35, 10.50.50.36, 10.50.50.37, 10.50.50.38, 10.50.50.40, 10.50.50.41, 10.50.50.43, 10.50.50.44, 10.50.50.45, 10.50.50.46, 10.50.50.48.	email.hightech.com, git.hightech.com, OA.hightech.com, jira.hightech.com, lib01.hightech.com, lib02.hightech.com, www.ruanyifeng.com, www.baidu.com, www.tianya.cn, www.csdn.net.	This department is mainly responsible for development and technology sharing. (There is no significant difference in the responsibilities of the three development departments)
Development 3	10:00-19:00	These servers are frequently accessed： 10.5.71.60(Email), 10.63.120.70(OA), 10.50.50.26(git), 10.50.50.27(jira), 10.50.50.28(lib01), 10.50.50.29(lib02) These servers are also accessed： 10.7.133.16, 10.7.133.19, 10.7.133.20, 10.50.50.31, 10.50.50.33, 10.50.50.34, 10.50.50.36, 10.50.50.37, 10.50.50.38, 10.50.50.39, 10.50.50.40, 10.50.50.41, 10.50.50.42, 10.50.50.43, 10.50.50.44, 10.50.50.46, 10.50.50.47, 10.50.50.48, 10.50.50.49.	email.hightech.com, git.hightech.com, OA.hightech.com, jira.hightech.com, lib01.hightech.com, lib02.hightech.com, www.baidu.com, www.google.com, www.programmer.com.cn, www.ruanyifeng.com.	This department is mainly responsible for development and technology sharing. (There is no significant difference in the responsibilities of the three development departments)

Supplementary explanation:

1. The lunch break is 12:30~13:30, during which employees usually have lunch, nap, and some of them also incline to surf the Internet.
2. Only the three development departments have server login operations.
3. The working hours of the department leaders are flexible. Thus, they have more lateness and absenteeism, but this is not something to be vigilant about.
4. The email topics of the finance department are about financial analysis, funding, accounting, taxation, cost control, reimbursement, etc. The email topics of the human resource department are about recruitment, performance appraisal, labor contracts, attendance, welfare guarantees, etc. The email topics of the development departments are about demand analysis, software development, etc.

5.3 Challenge 1.3

Find at least 5 abnormal events, and analyze the potential relationship among these events. Please summarize the valuable threat intelligence and illustrate how you achieved these by visual analytics. (Your submission for this question should contain no more than 10 images and 1500 words).

All 14 events in the 4.1 event list can be considered as anomalous events. In order to better describe the whole story, we recommend classifying and aggregating all 14 events. For example, In the reference answer, we aggregated all the events into 9 “aggregate events”, namely product data leakage, key asset damage, jump server event, resignation event, tourist event, group activity event, financial department overtime work event, VPN remote access event, traffic monitoring system failure. For more details, pay attention to the following events description.

5.3.1 Product Data Leakage

Account stealing 1: On 2017-11-03, employee 1487 (IP: 10.64.105.4) tried to log into the server 10.50.50.44 for multiple times, using 1080, a team leader’s account, but failed. Typical data records are as follows, which are extracted from the login.csv log file of 2017-11-03:

proto	dip	dport	sip	sport	state	time	user
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 9:58:48	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 10:40:34	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 10:41:55	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 10:49:32	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 11:25:42	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 11:26:56	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 12:01:34	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 12:14:00	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 14:43:57	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 14:51:53	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 15:09:11	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 15:10:29	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 15:22:15	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 15:39:11	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 16:21:26	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 16:30:17	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 17:08:55	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 17:36:17	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 17:39:44	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 18:10:04	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 18:27:25	1080
ssh	10.50.50.44	22	10.64.105.4	49195	error	2017/11/3 19:07:12	1080

Account stealing 2: On 2017-11-04, employee 1487 (IP: 10.64.105.4) tried to log into the server 10.50.50.44 for multiple times, using 1211, a team leader’s account, but also failed. Typical data records are as follows, which are extracted from the login.csv log file of 2017-11-04:

proto	dip	dport	sip	sport	state	time	user
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 9:50:35	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 11:00:40	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 11:05:31	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 11:30:19	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 11:52:53	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 12:20:24	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 12:29:41	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 12:41:38	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 13:02:42	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 14:56:28	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 14:56:42	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 15:51:05	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 15:55:10	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 16:12:34	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 16:36:33	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 17:32:00	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 17:32:43	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 18:24:58	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 18:30:01	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 19:30:52	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 19:46:05	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 19:57:21	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 20:10:59	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 21:43:43	1211
ssh	10.50.50.44	22	10.64.105.4	49200	error	2017/11/4 21:46:28	1211

Account stealing 3: On 2017-11-06, employee 1487 (IP: 10.64.105.4) tried to log into the server 10.50.50.44 for multiple times, using 1228, a team leader's account, and finally succeeded after a number of failures. Typical data records are as follows, which are extracted from the login.csv log file of 2017-11-06:

proto	dip	dport	sip	sport	state	time	user
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 19:20:08	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 19:16:50	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 18:58:32	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 18:49:43	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 17:50:01	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 17:38:03	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 17:00:33	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 16:42:07	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 16:34:31	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 16:11:30	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 14:33:35	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 14:09:48	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 14:09:27	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 12:50:15	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 12:41:51	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 12:30:49	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 12:11:20	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 11:35:17	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 10:37:59	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 10:27:00	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 10:21:58	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 10:17:49	1228
ssh	10.50.50.44	22	10.64.105.4	49197	error	2017/11/6 10:07:44	1228
ssh	10.50.50.44	22	10.64.105.4	49197	success	2017/11/6 19:42:57	1228

Product data peeping: At 2017-11-16 20:22, employee 1487 (IP: 10.64.105.4) logged into the server 10.50.50.44 and peeped the new product's data with 1228's account. Typical data record is as follows, which is extracted from the login.csv log file of 2017-11-16:

proto	dip	dport	sip	sport	state	time	user
ssh	10.50.50.44	22	10.64.105.4	49210	success	2017/11/16 20:22:04	1228

Product data leakage: During 2017-11-24 12:43~12:44, 1487 (IP: 10.64.105.4) took advantage of logged 1228's account and logged into the server 10.50.50.43. Then, using server 10.50.50.43 as a stepping stone, 1487 logged into the server 10.50.50.44. Typical data records are as follows, which are extracted from the login.csv log file of 2017-11-24:

proto	dip	dport	sip	sport	state	time	user
ssh	10.50.50.43	22	10.64.105.4	49173	success	2017/11/24 12:43:41	1228
ssh	10.50.50.44	22	10.50.50.43	13949	success	2017/11/24 12:43:51	1228

Now let's pay attention to the TCP records of the server 10.64.105.4, 10.50.50.43, and 10.50.50.44 during 2017-11-24 12:43~12:44. Server 10.64.105.4 (1487's IP) used SSH protocol to access the server 10.50.50.43, then the server 10.50.50.43 used the same protocol to access the server 10.50.50.44, finally the server 10.50.50.44 used the SSH protocol to access 13.250.177.223 (external unknown server). And it can be noticed that there was a large traffic about 600MB of data was uploaded. Typical data records are as follows, which are extracted from the tcpLog.csv log file of 2017-11-24:

stime	dtime	proto	dip	dport	sip	sport	uplink_length	downlink_length
2017/11/24 12:43:41	2017/11/24 12:43:51	ssh	10.50.50.43	22	10.64.105.4	49173	8367	5060
2017/11/24 12:43:51	2017/11/24 12:44:01	ssh	10.50.50.44	22	10.50.50.43	13949	1552	4993
2017/11/24 12:44:11	2017/11/24 12:44:21	ssh	13.250.177.223	22	10.50.50.44	8256	600006998	1343

The Spy resignation: Known from the attendance records and mail records, the employee 1487 submitted a resignation request on 2017-11-27, which was approved on 2017-11-28. After that, 1487 never came back to company again. Typical data records are as follows, which are extracted from the checking.csv log file of 2017-11-29 and 2017-11-30:

id	day	checkin	checkout
1487	2017/11/29	0	0
1487	2017/11/30	0	0

The data records of the employee 1487 resignation event are as follows, which are extracted from the email.csv log file of 2017-11-27 and 2017-11-28:

time	proto	sip	sport	dip	dport	from	to	subject
2017/11/27 14:20:00	smtp	10.64.105.4	49174	10.5.71.60	25	1487@hightech.com	hr@hightech.com	[Resignation Letter]
2017/11/28 10:14:00	smtp	10.1.4.17	4124	10.5.71.60	25	it@hightech.com	1487@hightech.com	[Notice] Device has been returned, please pass.
2017/11/28 10:55:00	smtp	10.64.105.146	3870	10.5.71.60	25	1228@hightech.com	1487@hightech.com	Reply: Resignation Application Review: approved
2017/11/28 11:27:00	smtp	10.1.4.17	4075	10.5.71.60	25	Finance@hightech.com	1487@hightech.com	[Notice] All Reimbursement ment has been settled, please pass.
2017/11/28 15:40:00	smtp	10.1.4.17	4127	10.5.71.60	25	kaoqin@hightech.com	1487@hightech.com	[Notice] Attendance is normal, and the remaining annual leave is 0. The salary isn't in arrears, please pass.
2017/11/28 16:04:00	smtp	10.64.106.49	3878	10.5.71.60	25	1059@hightech.com	1487@hightech.com	Reply: Resignation Application Review: approved
2017/11/28 16:18:00	smtp	10.1.4.17	3833	10.5.71.60	25	notice@hightech.com	1487@hightech.com	[Notice] The Result of the resignation application: approved. Resignation procedures:finished

5.3.2 Key Asset Damage

Database failure: After 2017-11-16 20:00, due to the possible database failure, a large number of emails with the subject "EmergencyDataBaseFatalError" were found in the email records of employees 1487 (10.64.105.4) and 1284 (10.64.105.95). Typical data records are as follows, which are extracted from the email.csv log file of 2017-11-16:

time	sip	sport	dip	dport	from	to	subject
2017/11/16 20:01:00	10.63.120.70	19387	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:01:00	10.63.120.70	19391	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:06:00	10.63.120.70	19392	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:06:00	10.63.120.70	19414	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:07:00	10.63.120.70	19419	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:07:00	10.63.120.70	19440	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:08:00	10.63.120.70	19448	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:08:00	10.63.120.70	19469	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:09:00	10.63.120.70	19482	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:09:00	10.63.120.70	19484	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:12:00	10.63.120.70	19486	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:12:00	10.63.120.70	19490	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:17:00	10.63.120.70	19507	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:17:00	10.63.120.70	19522	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:20:00	10.63.120.70	19529	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:20:00	10.63.120.70	19534	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:28:00	10.63.120.70	19555	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:28:00	10.63.120.70	19564	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:37:00	10.63.120.70	19577	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:37:00	10.63.120.70	19592	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:46:00	10.63.120.70	19596	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:46:00	10.63.120.70	19615	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:55:00	10.63.120.70	19621	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 20:55:00	10.63.120.70	19634	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 21:13:00	10.63.120.70	19658	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 21:13:00	10.63.120.70	19660	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 21:18:00	10.63.120.70	19692	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 21:18:00	10.63.120.70	19696	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 21:21:00	10.63.120.70	19702	10.5.71.60	25	alert@hightech.com	1487@hightech.com	EmergencyDataBaseFatalError!
2017/11/16 21:21:00	10.63.120.70	19714	10.5.71.60	25	alert@hightech.com	1284@hightech.com	EmergencyDataBaseFatalError!

Database maintenance: Employees 1487, 1376, and 1284 used the SSH protocol to log into the server 10.63.120.70 (OA) between 19:00 ~ 23:00 due to the database failure on server 10.63.120.70. They successfully maintained the failed server between 19 :00~ 23:00 and then left the company. Typical data records are as follows, which are extracted from the login.csv of 2017-11-16:

proto	dip	dport	sip	sport	state	time	user
ssh	10.63.120.70	22	10.64.105.219	49906	success	2017/11/16 19:22:00	1376
ssh	10.63.120.70	22	10.64.105.4	49347	success	2017/11/16 20:31:00	1487
ssh	10.63.120.70	22	10.64.105.95	49193	success	2017/11/16 21:45:00	1284
ssh	10.63.120.70	22	10.64.105.95	49226	success	2017/11/16 23:22:00	1284

The DB Deleter resignation: Known from the attendance records and mail records, employee 1376 submitted a resignation request on 2017-11-27, which was approved on 2017-11-28. After that, 1376 never came back to company again. Typical data records are as follows, which are extracted from the checking.csv of 2017-11-29 and 2017-11-30:

id	day	checkin	checkout
1376	2017/11/29	0	0
1376	2017/11/30	0	0

The data records of the employee 1376 resignation event are as follows, which are extracted from the email.csv log file of 2017-11-27 and 2017-11-28:

time	sip	sport	dip	dport	from	to	subject
2017/11/27 17:36:00	10.64.105.219	49181	10.5.71.60	25	1376@hightech.com	hr@hightech.com	[Resignation Letter]
2017/11/28 13:13:00	10.64.105.175	3886	10.5.71.60	25	1080@hightech.com	1376@hightech.com	Reply：Resignation Application Review: approved
2017/11/28 13:30:00	10.1.4.17	4098	10.5.71.60	25	it@hightech.com	1376@hightech.com	[Notice] Device has been returned, please pass.
2017/11/28 13:49:00	10.64.106.49	4017	10.5.71.60	25	1059@hightech.com	1376@hightech.com	Reply：Resignation Application Review: approved
2017/11/28 14:41:00	10.1.4.17	4657	10.5.71.60	25	kaoqin@hightech.com	1376@hightech.com	[Notice] Attendance is normal, and the remaining annual leave is 0. The salary isn't in arrears, please pass.
2017/11/28 16:04:00	10.1.4.17	3842	10.5.71.60	25	Finance@hightech.com	1376@hightech.com	[Notice] All Reimbursement ment has been settled, please pass.
2017/11/28 16:30:00	10.1.4.17	3912	10.5.71.60	25	notice@hightech.com	1376@hightech.com	[Notice] The Result of the resignation application: approved. Resignation procedures:finished

5.3.3 Jump Server Event

In 2017-11-17, 2017-11-21, 2017-11-27, 2017-11-30, four employees of 1183, 1273, 1169, and 1151 uploaded data to the external server 13.250.177.223 through two springboards.

At 2017-11-17 14:49, 1183 logged into 10.7.133.20 from his own client 10.64.105.165, then logged into 10.50.50.40 from 10.7.133.20 and uploaded data to 13.250.177.223. Typical data records are as follows, which are extracted from the login.csv and tcpLog.csv of 2017-11-17:

proto	dip	dport	sip	sport	state	time	user
ssh	10.7.133.20	22	10.64.105.165	2744	success	2017/11/17 14:49:28	1183
ssh	10.50.50.40	22	10.7.133.20	11013	success	2017/11/17 14:49:38	1183

stime	dtime	proto	dip	dport	sip	sport	uplink_length	downlink_length
2017/11/17 14:49:28	2017/11/17 14:49:38	ssh	10.7.133.20	22	10.64.105.165	2744	421	7189
2017/11/17 14:49:38	2017/11/17 14:49:48	ssh	10.50.50.40	22	10.7.133.20	11013	312	6605
2017/11/17 14:50:18	2017/11/17 14:50:28	ssh	13.250.177.223	22	10.50.50.40	14888	20006912	3486

At 2017-11-21 13:31, 1273 logged into 10.50.50.49 from his own client 10.64.105.244, then logged into 10.50.50.34 from 10.50.50.49 and uploaded data to 13.250.177.223. Typical data records are as follows, which are extracted from the login.csv and tcpLog.csv of 2017-11-21:

proto	dip	dport	sip	sport	state	time	user
ssh	10.50.50.49	22	10.64.105.244	3700	success	2017/11/21 13:31:00	1273
ssh	10.50.50.34	22	10.50.50.49	7798	success	2017/11/21 13:31:10	1273

stime	dtime	proto	dip	dport	sip	sport	uplink_length	downlink_length
2017/11/21 13:31:00	2017/11/21 13:31:10	ssh	10.50.50.49	22	10.64.105.244	3700	6209	7846
2017/11/21 13:31:10	2017/11/21 13:31:20	ssh	10.50.50.34	22	10.50.50.49	7798	8150	4837
2017/11/21 13:31:20	2017/11/21 13:31:30	ssh	13.250.177.223	22	10.50.50.34	5691	20005071	3417

At 2017-11-27 21:02, 1169 logged into 10.50.50.37 from his own client 10.64.105.199, then logged into 10.50.50.46 from 10.50.50.37 and uploaded data to 13.250.177.223. Typical data records are as follows, which are extracted from the login.csv and tcpLog.csv of 2017-11-27:

proto	dip	dport	sip	sport	state	time	user
ssh	10.50.50.37	22	10.64.105.199	4181	success	2017/11/27 21:02:54	1169
ssh	10.50.50.46	22	10.50.50.37	11886	success	2017/11/27 21:03:04	1169

stime	dtime	proto	dip	dport	sip	sport	uplink_length	downlink_length
2017/11/27 21:02:54	2017/11/27 21:03:04	ssh	10.50.50.37	22	10.64.105.199	4181	6080	1307
2017/11/27 21:03:04	2017/11/27 21:03:14	ssh	10.50.50.46	22	10.50.50.37	11886	3423	2738
2017/11/27 21:03:44	2017/11/27 21:03:54	ssh	13.250.177.223	22	10.50.50.46	10270	20001728	532

At 2017-11-30 17:19, 1151 logged into 10.50.50.49 from his own client 10.64.105.73, then logged into 10.7.133.16 from 10.50.50.49 and uploaded data to 13.250.177.223. Typical data records are as follows, which are extracted from the login.csv and tcpLog.csv of 2017-11-30:

proto	dip	dport	sip	sport	state	time	user
ssh	10.50.50.49	22	10.64.105.73	5591	success	2017/11/30 17:19:27	1151
ssh	10.7.133.16	22	10.50.50.49	7781	success	2017/11/30 17:19:37	1151

stime	dtime	proto	dip	dport	sip	sport	uplink_length	downlink_length
2017/11/30 17:19:27	2017/11/30 17:19:37	ssh	10.50.50.49	22	10.64.105.73	5591	7352	1157
2017/11/30 17:19:37	2017/11/30 17:19:47	ssh	10.7.133.16	22	10.50.50.49	7781	4017	1365
2017/11/30 17:19:47	2017/11/30 17:19:57	ssh	13.250.177.223	22	10.7.133.16	13476	20006308	1488

5.3.4 Resignation Event

Known from the attendance records and mail records, employee 1281 submitted a resignation request on 2017-11-27, which was approved on 2017-11-28. After that, 1281 never came back to company again. Typical data records are as follows, which are extracted from the checking.csv of 2017-11-29 and 2017-11-30:

id	day	checkin	checkout
1281	2017/11/29	0	0
1281	2017/11/30	0	0

The data records of the employee 1281 resignation event are as follows, which are extracted from the email.csv log file of 2017-11-27 and 2017-11-28:

time	proto	sip	sport	dip	dport	from	to	subject
2017/11/27 15:33:00	smtp	10.64.105.44	49204	10.5.71.60	25	1281@hightech.com	hr@hightech.com	[Resignation Letter]
2017/11/28 10:21:00	smtp	10.64.105.171	4286	10.5.71.60	25	1007@hightech.com	1281@hightech.com	Reply：Resignation Application Review: approved
2017/11/28 12:49:00	smtp	10.64.105.137	4763	10.5.71.60	25	1224@hightech.com	1281@hightech.com	Reply：Resignation Application Review: approved
2017/11/28 13:32:00	smtp	10.1.4.17	3885	10.5.71.60	25	kaoqin@hightech.com	1281@hightech.com	[Notice] Attendance is normal, and the remaining annual leave is 0. The salary isn't in arrears, please pass.
2017/11/28 13:39:00	smtp	10.1.4.17	4673	10.5.71.60	25	Finance@hightech.com	1281@hightech.com	[Notice] All Reimbursement ment has been settled, please pass.
2017/11/28 14:16:00	smtp	10.1.4.17	4256	10.5.71.60	25	it@hightech.com	1281@hightech.com	[Notice] Device has been returned, please pass.
2017/11/28 14:56:00	smtp	10.1.4.17	3819	10.5.71.60	25	notice@hightech.com	1281@hightech.com	[Notice] The Result of the resignation application: approved. Resignation procedures:finished

5.3.5 Tourist Event

Known from the attendance records and mail records that employees 1149, 1352, 1383, and 1389 applied for leave on 2017-11-24 (Friday) and did not come to the company during 2017-11-27 to 2017-11-30. Combined with the web access records, these employees frequently visited the travel websites from 2017-11-20 to 2017-11-24, so we can conclude that they may plan to travel together.

On 2017-11-24, these four employees sent emails for leaving to their manager, respectively. Typical data records are as follows, which are extracted from the email.csv of 2017-11-24:

time	sip	sport	dip	dport	from	to	subject
2017/11/24 10:56:00	10.64.105.79	49220	10.5.71.60	25	1389@hightech.com	1155@hightech.com	Note for Leave
2017/11/24 15:19:00	10.64.106.11	49196	10.5.71.60	25	1149@hightech.com	1013@hightech.com	Casual Leave
2017/11/24 15:50:00	10.64.105.60	49173	10.5.71.60	25	1383@hightech.com	1058@hightech.com	Leave for 4 days, and hope to be approved.
2017/11/24 18:15:00	10.64.105.174	49198	10.5.71.60	25	1352@hightech.com	1101@hightech.com	Note for Leave

They did not come to the company from 2017-11-27 to 2017-11-30. Typical data records are as follows, which are extracted from the checking.csv from 2017-11-27 to 2017-11-30:

id	day	checkin	checkout
1149	2017/11/27	0	0
1352	2017/11/27	0	0
1383	2017/11/27	0	0
1389	2017/11/27	0	0
1149	2017/11/28	0	0
1352	2017/11/28	0	0
1383	2017/11/28	0	0
1389	2017/11/28	0	0
1149	2017/11/29	0	0
1352	2017/11/29	0	0
1383	2017/11/29	0	0
1389	2017/11/29	0	0
1149	2017/11/30	0	0
1352	2017/11/30	0	0
1383	2017/11/30	0	0
1389	2017/11/30	0	0

5.3.6 Group Activity Event

At 9:30 of 2017-11-02, 2017-11-09, 2017-11-16, 2017-11-23, 2017-11-30 (all are Thursday), HR (hr@hightech.com) sent emails to all the employees (allstaff@hightech.com) to invite them to participate in group sports exercises, such as playing ball. Those who wished to participate would reply and leave the company to join in the activity before 19:30.

Group activity event 1：On 2017-11-02, 1352, 1376, 1383, 1487, 1339, 1149, 1313, 1261, 1389, 1330, 1356 signed up for the group activity. Typical data records are as follows, which are extracted from the email.csv of 2017-11-02:

time	proto	sip	sport	dip	dport	from	to	subject
2017/11/2 9:30:00	smtp	10.1.4.17	49163	10.5.71.60	25	hr@hightech.com	allstaff@hightech.com	Playing, Welcome Everyone to Participate
2017/11/2 10:05:00	smtp	10.64.105.174	49188	10.5.71.60	25	1352@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/2 10:10:00	smtp	10.64.105.219	49189	10.5.71.60	25	1376@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/2 10:28:00	smtp	10.64.105.60	49220	10.5.71.60	25	1383@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/2 10:50:00	smtp	10.64.105.4	49161	10.5.71.60	25	1487@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/2 11:07:00	smtp	10.64.106.18	49163	10.5.71.60	25	1339@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/2 11:08:00	smtp	10.64.106.11	49188	10.5.71.60	25	1149@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/2 11:28:00	smtp	10.64.105.154	49214	10.5.71.60	25	1313@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/2 11:34:00	smtp	10.64.105.239	49181	10.5.71.60	25	1261@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/2 11:43:00	smtp	10.64.105.79	49163	10.5.71.60	25	1389@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/2 11:52:00	smtp	10.64.105.70	49201	10.5.71.60	25	1330@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/2 11:56:00	smtp	10.64.106.41	49193	10.5.71.60	25	1356@hightech.com	hr@hightech.com	Re:Sign Up

Employees who signed up and left the company to join in the activity between 19:00~19:20. Typical data records are as follows, which are extracted from the checking.csv of 2017-11-02:

id	day	checkin	checkout
1313	2017/11/2	2017-11-02 08:49:31	2017-11-02 19:00:08
1149	2017/11/2	2017-11-02 09:15:54	2017-11-02 19:02:29
1383	2017/11/2	2017-11-02 09:25:05	2017-11-02 19:03:21
1487	2017/11/2	2017-11-02 09:51:12	2017-11-02 19:05:49
1261	2017/11/2	2017-11-02 09:58:44	2017-11-02 19:07:12
1376	2017/11/2	2017-11-02 09:55:52	2017-11-02 19:07:18
1389	2017/11/2	2017-11-02 09:47:57	2017-11-02 19:13:00
1356	2017/11/2	2017-11-02 09:57:41	2017-11-02 19:13:13
1330	2017/11/2	2017-11-02 08:13:13	2017-11-02 19:16:30
1352	2017/11/2	2017-11-02 09:49:54	2017-11-02 19:16:52
1339	2017/11/2	2017-11-02 08:50:25	2017-11-02 19:17:32

Group activity event 2：On 2017-11-09, 1389, 1313, 1261, 1330, 1383, 1149, 1376, 1352, 1487 signed up for the group activity. Typical data records are as follows, which are extracted from the email.csv of 2017-11-09:

time	proto	sip	sport	dip	dport	from	to	subject
2017/11/9 9:30:00	smtp	10.1.4.17	49189	10.5.71.60	25	hr@hightech.com	allstaff@hightech.com	Playing, Welcome Everyone to Participate
2017/11/9 10:01:00	smtp	10.64.105.79	49188	10.5.71.60	25	1389@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/9 10:44:00	smtp	10.64.105.154	49201	10.5.71.60	25	1313@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/9 11:05:00	smtp	10.64.105.239	49198	10.5.71.60	25	1261@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/9 11:07:00	smtp	10.64.105.70	49219	10.5.71.60	25	1330@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/9 11:10:00	smtp	10.64.105.60	49210	10.5.71.60	25	1383@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/9 11:23:00	smtp	10.64.106.11	49199	10.5.71.60	25	1149@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/9 11:42:00	smtp	10.64.105.219	49212	10.5.71.60	25	1376@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/9 11:55:00	smtp	10.64.105.174	49235	10.5.71.60	25	1352@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/9 11:58:00	smtp	10.64.105.4	49181	10.5.71.60	25	1487@hightech.com	hr@hightech.com	Re:Sign Up

Employees who signed up and left the company to join in the activity between 19:00~19:20. Typical data records are as follows, which are extracted from the checking.csv of 2017-11-09:

id	day	checkin	checkout
1313	2017/11/9	2017-11-09 08:49:05	2017-11-09 19:01:38
1376	2017/11/9	2017-11-09 09:56:16	2017-11-09 19:03:41
1261	2017/11/9	2017-11-09 10:16:19	2017-11-09 19:07:39
1149	2017/11/9	2017-11-09 08:40:25	2017-11-09 19:07:51
1389	2017/11/9	2017-11-09 09:34:49	2017-11-09 19:08:53
1330	2017/11/9	2017-11-09 08:12:41	2017-11-09 19:10:40
1487	2017/11/9	2017-11-09 09:40:24	2017-11-09 19:15:50
1352	2017/11/9	2017-11-09 09:49:58	2017-11-09 19:15:56
1383	2017/11/9	2017-11-09 09:38:29	2017-11-09 19:16:15

Group activity event 3：On 2017-11-16, 1352, 1487, 1383, 1376, 1389, 1149, 1356, 1189, 1330, 1261, 1339, 1313 signed up for the group activity. Typical data records are as follows, which are extracted from the email.csv of 2017-11-16:

time	proto	sip	sport	dip	dport	from	to	subject
2017/11/16 9:30:00	smtp	10.1.4.17	49197	10.5.71.60	25	hr@hightech.com	allstaff@hightech.com	Playing, Welcome Everyone to Participate
2017/11/16 10:08:00	smtp	10.64.105.174	49171	10.5.71.60	25	1352@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/16 10:14:00	smtp	10.64.105.4	49220	10.5.71.60	25	1487@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/16 10:30:00	smtp	10.64.105.60	49174	10.5.71.60	25	1383@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/16 11:02:00	smtp	10.64.105.219	49204	10.5.71.60	25	1376@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/16 11:06:00	smtp	10.64.105.79	49183	10.5.71.60	25	1389@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/16 11:11:00	smtp	10.64.106.11	49168	10.5.71.60	25	1149@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/16 11:15:00	smtp	10.64.106.41	49185	10.5.71.60	25	1356@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/16 11:28:00	smtp	10.64.105.212	49159	10.5.71.60	25	1189@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/16 11:36:00	smtp	10.64.105.70	49203	10.5.71.60	25	1330@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/16 11:44:00	smtp	10.64.105.239	49195	10.5.71.60	25	1261@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/16 11:50:00	smtp	10.64.106.18	49177	10.5.71.60	25	1339@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/16 11:51:00	smtp	10.64.105.154	49192	10.5.71.60	25	1313@hightech.com	hr@hightech.com	Re:Sign Up

Employees who signed up and left the company to join in the activity between 19:00~19:20 except 1487 and 1376. Typical data records are as follows, which are extracted from the checking.csv of 2017-11-16:

id	day	checkin	checkout
1356	2017/11/16	2017-11-16 09:41:24	2017-11-16 19:01:31
1261	2017/11/16	2017-11-16 09:56:18	2017-11-16 19:02:23
1383	2017/11/16	2017-11-16 10:00:28	2017-11-16 19:02:53
1189	2017/11/16	2017-11-16 08:35:06	2017-11-16 19:03:59
1313	2017/11/16	2017-11-16 08:56:09	2017-11-16 19:06:58
1330	2017/11/16	2017-11-16 08:13:35	2017-11-16 19:07:17
1352	2017/11/16	2017-11-16 09:58:20	2017-11-16 19:07:58
1389	2017/11/16	2017-11-16 09:34:56	2017-11-16 19:10:25
1149	2017/11/16	2017-11-16 08:41:15	2017-11-16 19:14:09
1339	2017/11/16	2017-11-16 09:05:05	2017-11-16 19:14:45
1487	2017/11/16	2017-11-16 09:44:56	2017-11-16 23:34:45
1376	2017/11/16	2017-11-16 09:55:58	2017-11-16 23:46:55

Group activity event 4：On 2017-11-23, 1471, 1475, 1473, 1371, 1474, 1189, 1359, 1411, 1348, 1268, 1165 signed up for the group activity. Typical data records are as follows, which are extracted from the email.csv of 2017-11-23:

time	proto	sip	sport	dip	dport	from	to	subject
2017/11/23 9:30:00	smtp	10.1.4.17	49186	10.5.71.60	25	hr@hightech.com	allstaff@hightech.com	Playing, Welcome Everyone to Participate
2017/11/23 10:08:00	smtp	10.64.105.221	49170	10.5.71.60	25	1471@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/23 10:09:00	smtp	10.64.105.240	49202	10.5.71.60	25	1475@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/23 10:22:00	smtp	10.64.106.6	49184	10.5.71.60	25	1473@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/23 10:38:00	smtp	10.64.106.32	49177	10.5.71.60	25	1371@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/23 10:48:00	smtp	10.64.105.17	49169	10.5.71.60	25	1474@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/23 10:50:00	smtp	10.64.105.212	49224	10.5.71.60	25	1189@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/23 11:01:00	smtp	10.64.105.75	49211	10.5.71.60	25	1359@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/23 11:02:00	smtp	10.64.105.167	49166	10.5.71.60	25	1411@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/23 11:21:00	smtp	10.64.105.163	49173	10.5.71.60	25	1348@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/23 11:34:00	smtp	10.64.105.228	49163	10.5.71.60	25	1268@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/23 11:40:00	smtp	10.64.106.5	49209	10.5.71.60	25	1165@hightech.com	hr@hightech.com	Re:Sign Up

Employees who signed up and left the company to join in the activity between 19:00~19:20. Typical data records are as follows, which are extracted from the checking.csv of 2017-11-23:

id	day	checkin	checkout
1474	2017/11/23	2017-11-23 08:55:34	2017-11-23 19:00:59
1471	2017/11/23	2017-11-23 08:41:54	2017-11-23 19:04:09
1165	2017/11/23	2017-11-23 08:24:16	2017-11-23 19:07:30
1348	2017/11/23	2017-11-23 09:27:57	2017-11-23 19:08:40
1268	2017/11/23	2017-11-23 09:52:23	2017-11-23 19:11:20
1473	2017/11/23	2017-11-23 08:46:13	2017-11-23 19:11:29
1189	2017/11/23	2017-11-23 09:01:56	2017-11-23 19:11:48
1359	2017/11/23	2017-11-23 07:22:57	2017-11-23 19:13:12
1411	2017/11/23	2017-11-23 09:37:04	2017-11-23 19:14:18
1371	2017/11/23	2017-11-23 08:31:57	2017-11-23 19:16:21
1475	2017/11/23	2017-11-23 08:53:22	2017-11-23 19:16:43

Group activity event 5：On 2017-11-30, 1424, 1333, 1169, 1314, 1338, 1139, 1489, 1265 signed up for the group activity. Typical data records are as follows, which are extracted from the email.csv of 2017-11-30:

time	proto	sip	sport	dip	dport	from	to	subject
2017/11/30 9:30:00	smtp	10.1.4.17	49180	10.5.71.60	25	hr@hightech.com	allstaff@hightech.com	Playing, Welcome Everyone to Participate
2017/11/30 10:06:00	smtp	10.64.105.136	49214	10.5.71.60	25	1424@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/30 10:21:00	smtp	10.64.105.32	49221	10.5.71.60	25	1333@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/30 10:51:00	smtp	10.64.105.199	49163	10.5.71.60	25	1169@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/30 11:07:00	smtp	10.64.105.45	49200	10.5.71.60	25	1314@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/30 11:08:00	smtp	10.64.105.91	49179	10.5.71.60	25	1338@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/30 11:19:00	smtp	10.64.105.134	49185	10.5.71.60	25	1139@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/30 11:21:00	smtp	10.64.105.132	49178	10.5.71.60	25	1489@hightech.com	hr@hightech.com	Re:Sign Up
2017/11/30 11:25:00	smtp	10.64.105.170	49198	10.5.71.60	25	1265@hightech.com	hr@hightech.com	Re:Sign Up

Employees who signed up and left the company to join in the activity between 19:00~19:20. Typical data records are as follows, which are extracted from the checking.csv of 2017-11-30:

id	day	checkin	checkout
1489	2017/11/30	2017-11-30 10:02:21	2017-11-30 19:01:35
1314	2017/11/30	2017-11-30 08:54:12	2017-11-30 19:02:22
1139	2017/11/30	2017-11-30 08:46:40	2017-11-30 19:07:56
1338	2017/11/30	2017-11-30 09:41:24	2017-11-30 19:08:21
1424	2017/11/30	2017-11-30 10:18:07	2017-11-30 19:11:17
1169	2017/11/30	2017-11-30 08:41:13	2017-11-30 19:13:40
1333	2017/11/30	2017-11-30 09:41:56	2017-11-30 19:17:34
1265	2017/11/30	2017-11-30 08:30:55	2017-11-30 19:17:44

5.3.7 Financial Department Overtime Work Event

On 2017-11-19, 2017-11-25, and 2017-11-26, most of employees in the finance department came to the company to work overtime. The statistics about the overtime work are as follows:

Department	Total Number	Date	Overtime Number
Finance	24	2017-11-19(Sunday)	15
		2017-11-25(Saturday)	20
		2017-11-26(Sunday)	21

5.3.8 VPN Remote Access Event

Normally, if an employee does not come to the company but still generates TCP traffic, that is because he/she uses VPN to remotely link to the company's intranet to work. An abnormal event, that is, employees generate TCP traffic without punching in or punching out (No check record or the checkin

and checkout of check records are 0), usually happens on Saturday and Sunday. The involved employees include 1147, 1283, 1284, 1328, 1334, 1376, 1487, 1494, 1059. Further information is as follows:

Date	Week	Weekday/Weekend	Involved personnel	Event description
2017-11-04	Saturday	Weekend	1487	Employee used VPN to remotely link to the company's intranet to work overtime.
2017-11-05	Sunday	Weekend	1147, 1328, 1334, 1494	Employees used VPN to remotely link to the company's intranet to work overtime.
2017-11-11	Saturday	Weekend	1147, 1328, 1376, 1487, 1494	Employees used VPN to remotely link to the company's intranet to work overtime.
2017-11-12	Saturday	Weekend	1376	Employee used VPN to remotely link to the company's intranet to work overtime.
2017-11-18	Saturday	Weekend	1147, 1283, 1284, 1328, 1334, 1376, 1487, 1494	Employees used VPN to remotely link to the company's intranet to work overtime.
2017-11-19	Sunday	Weekend	1487	Employee used VPN to remotely link to the company's intranet to work overtime.
2017-11-25	Saturday	Weekend	1283, 1284, 1376, 1487	Employees used VPN to remotely link to the company's intranet to work overtime.
2017-11-26	Sunday	Weekend	1376, 1487	Employees used VPN to remotely link to the company's intranet to work overtime.
2017-11-28	Tuesday	Weekday	1059	A manager used VPN to remotely link to the company's intranet to approve the resignation of two employees (1376 and 1487) of his own department.

5.3.9 Traffic Monitoring System Failure

From 2017-11-10 to 2017-11-28, there are some TCP records that have a network protocol type of http but a destination port of 25 (smtp protocol port). The destination IP address of this kind of TCP records are 10.5.71.60 (mail server). Thus, we further check the TCP traffic logs and the email logs to explore the corresponding mail records, finding the network protocol types of these records are inconsistent in two types of logs. The network protocol is smtp in the email logs, but http in the TCP traffic logs. This error is caused by a failure of the logging system. Typical error log information is as follows (the TCP traffic logs and the email logs are connected through source IP, destination IP, time, sport and dport):

stime	proto	dip	dport	sip	sport	proto (email.csv)	from	to	subject
2017/11/10 10:09:22	http	10.5.71.60	25	106.3.154.30	4236	smtp	liangzi@163.net	1376@hightech.com	Please contact me if you want high annual salary
2017/11/10 12:27:42	http	10.5.71.60	25	204.79.197.203	4199	smtp	zhaopin@msn.com	1376@hightech.com	Your resume has not been viewed
2017/11/10 13:16:42	http	10.5.71.60	25	217.12.13.41	3865	smtp	wanglin@yahoo.com.cn	1376@hightech.com	Reply: Your resume has been viewed, please contact me as soon as possible!
2017/11/10 13:52:58	http	10.5.71.60	25	113.108.216.17	4687	smtp	liuqian@sina.com	1376@hightech.com	Reply: Your resume has been viewed, please contact me as soon as possible!
2017/11/11 12:07:14	http	10.5.71.60	25	13.107.42.11	4273	smtp	wujia@hotmail.com	1487@hightech.com	[Job promotion]The system matches you with high salary position, please login in and view
2017/11/11 12:16:53	http	10.5.71.60	25	113.108.216.17	3854	smtp	liqiu@sina.com	1487@hightech.com	7 HRs have viewed your resume
2017/11/11 12:54:30	http	10.5.71.60	25	123.58.177.21	3924	smtp	lucy@126.com	1487@hightech.com	[Notice] You have an invitation to check
2017/11/11 13:04:17	http	10.5.71.60	25	183.61.185.93	4478	smtp	lucy@21cn.com	1376@hightech.com	[Phone Interview Notice Invitation]
2017/11/11 13:07:06	http	10.5.71.60	25	203.78.142.12	3846	smtp	liuqian@qq.com	1376@hightech.com	[Notice] You have an invitation to check
2017/11/11 13:13:56	http	10.5.71.60	25	203.78.142.12	4372	smtp	zhangzhe@qq.com	1376@hightech.com	[Notice] You have an invitation to check
2017/11/11 15:45:42	http	10.5.71.60	25	220.181.90.34	3831	smtp	erdongsheng@sohu.com	1487@hightech.com	Your resume has not been viewed
2017/11/12 9:52:14	http	10.5.71.60	25	123.125.50.182	4582	smtp	liuqian@ask.com	1487@hightech.com	Ten friends have praised your work experience
2017/11/12 11:15:03	http	10.5.71.60	25	220.181.90.34	4659	smtp	liming@sohu.com	1376@hightech.com	Reply: Your resume has been viewed, please contact me as soon as possible!
2017/11/12 12:06:53	http	10.5.71.60	25	172.217.160.101	3922	smtp	job@gmail.com	1376@hightech.com	Your resume has not been viewed
2017/11/12 13:26:04	http	10.5.71.60	25	123.58.177.20	4316	smtp	erdongsheng@163.com	1376@hightech.com	[Phone Interview Notice Invitation]
2017/11/12 15:32:14	http	10.5.71.60	25	114.80.130.60	4441	smtp	liqiu@56.com	1487@hightech.com	3 HRs have viewed your resume
2017/11/12 17:05:47	http	10.5.71.60	25	113.108.216.17	4661	smtp	erdongsheng@sina.com	1376@hightech.com	3 HRs have viewed your resume
2017/11/12 18:56:18	http	10.5.71.60	25	203.78.142.12	4098	smtp	Mark@qq.com	1487@hightech.com	[Job promotion]The system matches you with high salary position, please login in and view

stime	proto	dip	dport	sip	sport	proto (email.csv)	from	to	subject
2017/11/27 11:45:35	http	10.5.71.60	25	113.108.216.17	4269	smtp	liuqianqian@sina.com	1487@hightech.com	Reply: Your resume has automatically entered the talent pool.
2017/11/27 12:52:29	http	10.5.71.60	25	114.80.130.60	4431	smtp	liuqianqian@56.com	1487@hightech.com	[Writing Examination Invitation]
2017/11/27 14:20:46	http	10.5.71.60	25	10.64.105.4	49174	smtp	1487@hightech.com	hr@hightech.com	[Resignation Letter]
2017/11/27 15:15:07	http	10.5.71.60	25	211.150.82.8	4237	smtp	maku@263.net	1376@hightech.com	Reply：Your resume has been viewed, please contact me as soon as possible
2017/11/27 15:33:37	http	10.5.71.60	25	10.64.105.44	49204	smtp	1281@hightech.com	hr@hightech.com	[Resignation Letter]
2017/11/27 16:56:41	http	10.5.71.60	25	123.58.177.20	4763	smtp	Mark@163.com	1376@hightech.com	8 head-hunting have viewed your resume
2017/11/27 17:36:33	http	10.5.71.60	25	10.64.105.219	49181	smtp	1376@hightech.com	hr@hightech.com	[Resignation Letter]
2017/11/27 19:07:19	http	10.5.71.60	25	123.58.177.20	3932	smtp	Mark@163.com	1487@hightech.com	Reply：Your resume has been viewed, please contact me as soon as possible
2017/11/27 21:50:43	http	10.5.71.60	25	123.58.177.21	4291	smtp	hr@126.com	1487@hightech.com	Please contact me if you want high annual salary
2017/11/28 10:14:03	http	10.5.71.60	25	10.1.4.17	4124	smtp	it@hightech.com	1487@hightech.com	[Notice] Device has been returned, please pass.
2017/11/28 10:21:28	http	10.5.71.60	25	10.64.105.171	4286	smtp	1007@hightech.com	1281@hightech.com	Reply：Resignation Application Review: approved
2017/11/28 10:55:17	http	10.5.71.60	25	10.64.105.146	3870	smtp	1228@hightech.com	1487@hightech.com	Reply：Resignation Application Review: approved
2017/11/28 12:49:06	http	10.5.71.60	25	10.64.105.137	4763	smtp	1224@hightech.com	1281@hightech.com	Reply：Resignation Application Review: approved
2017/11/28 13:13:13	http	10.5.71.60	25	10.64.105.175	3886	smtp	1080@hightech.com	1376@hightech.com	Reply：Resignation Application Review: approved
2017/11/28 13:32:34	http	10.5.71.60	25	10.1.4.17	3885	smtp	kaoqin@hightech.com	1281@hightech.com	[Notice] Attendance is normal, and the remaining annual leave is 0. The salary isn't in arrears, please pass.
2017/11/28 13:49:14	http	10.5.71.60	25	10.64.106.49	4017	smtp	1059@hightech.com	1376@hightech.com	Reply：Resignation Application Review: approved
2017/11/28 14:16:38	http	10.5.71.60	25	10.1.4.17	4256	smtp	it@hightech.com	1281@hightech.com	[Notice] Device has been returned, please pass.
2017/11/28 14:41:30	http	10.5.71.60	25	10.1.4.17	4657	smtp	kaoqin@hightech.com	1376@hightech.com	[Notice] Attendance is normal, and the remaining annual leave is 0. The salary isn't in arrears, please pass.
2017/11/28 15:40:09	http	10.5.71.60	25	10.1.4.17	4127	smtp	kaoqin@hightech.com	1487@hightech.com	[Notice] Attendance is normal, and the remaining annual leave is 0. The salary isn't in arrears, please pass.
2017/11/28 16:04:01	http	10.5.71.60	25	10.1.4.17	3842	smtp	Finance@hightech.com	1376@hightech.com	[Notice] All Reimbursement ment has been settled, please pass.