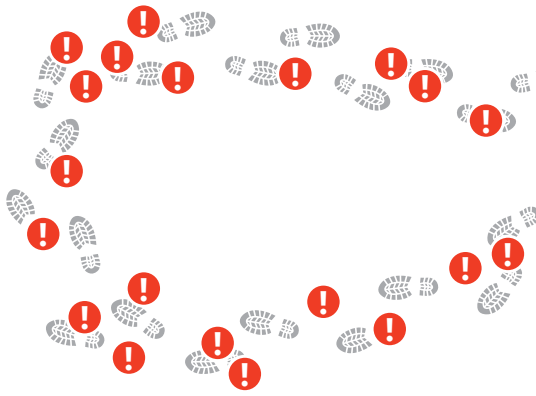
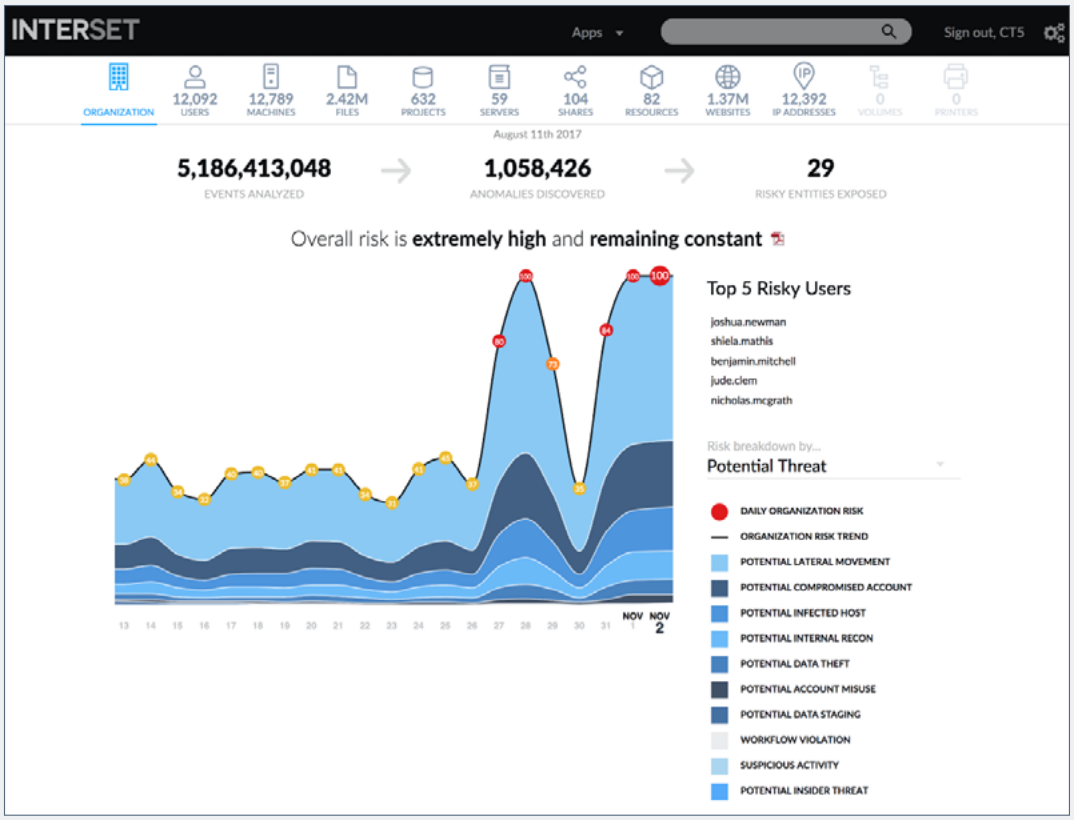
INTERSET

Interset at a Glance

Security analytics give cyber hunters radical advantages in containing cyberthreats. Powered by unsupervised machine learning, Interset distills billions of real-time events into a prioritized list of high-risk entities for accelerated, more accurate threat-hunting.





Billions of events are distilled into millions of anomalies, then into a prioritized list of actionable threat leads

An enterprise executive can download reports that summarize immediate organizational risks.

Sep 27, 2017 1

The Interset Platform

The Interset Platform is an analytics product that surfaces abnormal Behaviors from Behavioural Data. It uses advanced analytics to score Behaviors and Entities between one and one hundred from multiple Behavioural Analytics.

The higher the Score, the higher the Risk.

The Threat Hunter Interface

The Threat Hunter Interface observes all Behaviors or Alerts and aggregates them into Risky Hours which is presented visually over lengths of time.

For example, a user who triggers 30 high risk Alerts in the same hour will have one high risky hour for that hour that combines all of those Alerts. This combination makes it easier to understand and to use the results appropriately.

Risky Hours can be expanded to view their Behavioural Anomalies and the results can be explored dynamically. The Risky Hours can then be exported for easier communication across individuals or business functions.

The Report

The report contains different types of information depending on what the user has selected or filtered.

If no Entities (like users or projects) are selected, the report will only contain information that applies to the organization as a whole. This includes information like Top Risky Users, Top Risky Projects, "bot-like" users (accounts identified as bots or scripts) and other organizational information.

If Entities are selected, a section will be created for each, which enables for the addition or removal of pages as needed.

This report can be generated as often as needed with different selections, filters and time ranges. The generated PDF can then be saved, disseminated and managed accordingly.

Sep 27, 2017 16

Work Schedule

All Users, All Time

Working days and working hours represent the average of all users in the organization, for all time.

Working Days

This visualization represents the overall level of activity on individual days of the week, comparing each minute of an individual day, for all users, against the usual activity for that same minute of the day, across all time.

Taller columns indicate more activity, and therefore the most normal work days. Shorter columns indicate less activity, and therefore less normal work days.

Use this information to examine the baseline normal work day activity across the organization.

This report excludes data generated by bots and bot-like users.

Working Hours

This visualization represents the overall level of activity at different times of the day, comparing each minute of an individual day, for all users, against the usual activity for that same minute of the day, across all time.

The slices that extend to the rim of the clock represent the most user activity, and therefore the most normal work hours. The smallest slices, those closest to the center of the clock, represent the least user activity, and therefore the least normal working hours.

Use this information to examine the baseline normal working hour activity across the organization.

This report excludes data generated by bots and bot-like users.

Sep 27, 2017 21

Most Accessed Servers

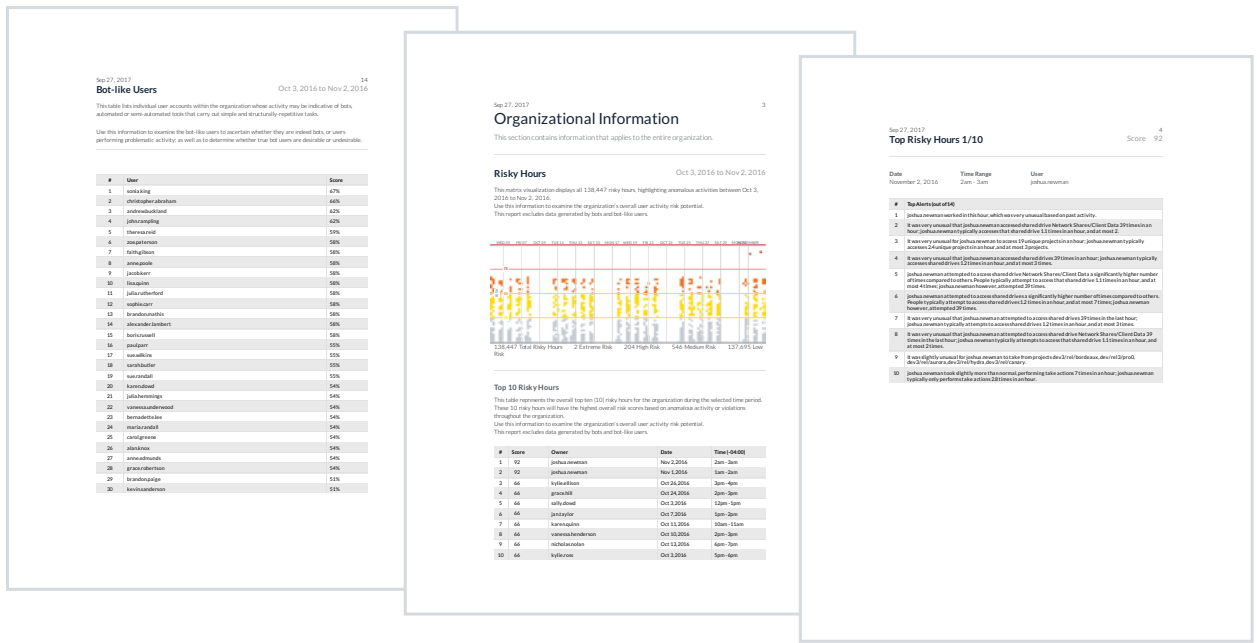
Oct 3, 2016 to Nov 2, 2016

This table lists the most accessed servers between Oct 3, 2016 to Nov 2, 2016.

Use this information to examine the riskiest servers most frequently accessed.

This report excludes data generated by bots and bot-like users.

#	Accesses	Server
1	136610	MTM-WSRV01.interset-dev.ca
2	84790	MDM-WSRV01.interset-dev.ca
3	81975	VPM-CFDB01.interset.int
4	80049	Direct-BE01.interset.com
5	79857	MPM-UWEB01B.interset.ext
6	72704	TIA-SSRV00.interset.com
7	71217	NPMC.interset.com
8	70613	PPA.interset.com
9	67927	FTXDC2.interset.com
10	67341	OTTAWADC.interset.com
11	67011	MLM-WSRV02B.interset-ll.ext
12	65527	FIBE.interset.ext
13	64504	MPM-CSRV01.interset.int
14	63883	LM-WSRV02A.interset-ll.ext
15	63238	SBS.interset.com
16	60718	CINCO-SSRV00.interset.ext
17	58957	SSLC.interset.com
18	55615	CORTEX-SSRV00.interset.ext
19	55312	INDYA.interset.com
20	53472	SOLEIL.interset.com
21	51418	SHANNON.interset.com
22	45870	FLARE.interset.int



Sep 27, 2017 14

Bot-like Users

Oct 3, 2016 to Nov 2, 2016

This table lists individual user accounts within the organization whose activity may be indicative of bots, automated or semi-automated tools that carry out simple and structurally-repetitive tasks.

Use this information to examine the bot-like users to ascertain whether they are indeed bots, or users performing problematic activity; as well as to determine whether true bot users are desirable or undesirable.

#	User	Score
1	sonia.king	67%
2	christopher.abraham	66%
3	andrew.buckland	62%
4	john.rampling	62%
5	theresa.reid	59%
6	zoe.paterson	58%
7	faith.gibson	58%
8	anne.poole	58%
9	jacob.kerr	58%
10	lisa.quinn	58%
11	julia.rutherford	58%
12	sophie.carr	58%
13	brandon.mathis	58%
14	alexander.lambert	58%
15	boris.russell	58%
16	paul.parr	55%
17	sue.wilkins	55%
18	sarah.butler	55%
19	sue.randall	55%
20	kamin.dowd	54%
21	julia.hemmings	54%
22	vanessa.underwood	54%
23	bernadette.lee	54%
24	mario.randall	54%
25	carol.greene	54%
26	alan.knox	54%
27	anne.edmunds	54%
28	grace.robertson	54%
29	brandon.paige	51%
30	kevin.sanderson	51%

Sep 27, 2017 3

Organizational Information

This section contains information that applies to the entire organization.

Risky Hours

Oct 3, 2016 to Nov 2, 2016

This matrix visualization displays all 138,447 risky hours, highlighting anomalous activities between Oct 3, 2016 to Nov 2, 2016.
Use this information to examine the organization's overall user activity risk potential.
This report excludes data generated by bots and bot-like users.

138,447 Total Risky Hours | 2 Extreme Risk | 204 High Risk | 546 Medium Risk | 137,695 Low Risk

Top 10 Risky Hours

This table represents the overall top ten (10) risky hours for the organization during the selected time period. These 10 risky hours will have the highest overall risk scores based on anomalous activity or violations throughout the organization.
Use this information to examine the organization's overall user activity risk potential.
This report excludes data generated by bots and bot-like users.

#	Score	Owner	Date	Time (-04:00)
1	92	joshua.newman	Nov 2,2016	2am - 3am
2	92	joshua.newman	Nov 1,2016	1am - 2am
3	66	kyliealllison	Oct 26,2016	3pm - 4pm
4	66	gracehill	Oct 24,2016	2pm - 3pm
5	66	sally.dowd	Oct 3,2016	12pm - 1pm
6	66	jessaylor	Oct 7,2016	5pm - 2pm
7	66	karen.quinn	Oct 11,2016	10am - 11am
8	66	vanessa.henderson	Oct 10,2016	2pm - 3pm
9	66	nicholas.nolan	Oct 13,2016	6pm - 7pm
10	66	kylie.ross	Oct 3,2016	5pm - 6pm

Sep 27, 2017 4

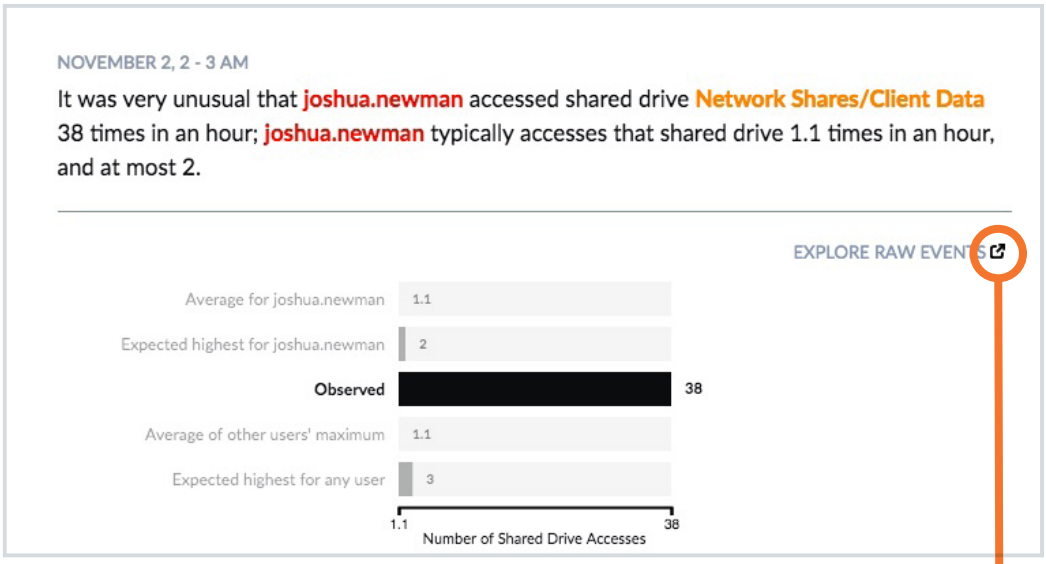
Top Risky Hours 1/10

Score 92

Date	Time Range	User
November 2, 2016	2am - 3am	joshua.newman

#	Top Alerts (out of 14)
1	joshua.newman worked in this hour, which was very unusual based on past activity.
2	It was very unusual that joshua.newman accessed shared drive Network Shares/Client Data 39 times in an hour; joshua.newman typically accesses that shared drive 1.1 times in an hour, and at most 2.
3	It was very unusual for joshua.newman to access 19 unique projects in an hour; joshua.newman typically accesses 2.4 unique projects in an hour, and at most 3 projects.
4	It was very unusual that joshua.newman accessed shared drives 39 times in an hour; joshua.newman typically accesses shared drives 1.2 times in an hour, and at most 3 times.
5	joshua.newman attempted to access shared drive Network Shares/Client Data a significantly higher number of times compared to others. People typically attempt to access that shared drive 1.1 times in an hour, and at most 4 times. joshua.newman however, attempted 39 times.
6	joshua.newman attempted to access shared drives a significantly higher number of times compared to others. People typically attempt to access shared drives 1.2 times in a hour, and at most 7 times; joshua.newman however, attempted 39 times.
7	It was very unusual that joshua.newman attempted to access shared drives 39 times in the last hour; joshua.newman typically attempts to access shared drives 1.2 times in an hour, and at most 3 times.
8	It was very unusual that joshua.newman attempted to access shared drive Network Shares/Client Data 39 times in an hour; joshua.newman typically attempts to access that shared drive 1.1 times in an hour, and at most 2 times.
9	It was slightly unusual for joshua.newman to take from projects dev3/rel/bardeaux, dev/rel3/pro0, dev3/rel/aurora, dev3/rel/hydra, dev3/rel/canary.
10	joshua.newman took slightly more than normal, performing take actions 7 times in a hour; joshua.newman typically only performs take actions 2.8 times in an hour.

The security team can access details about prioritized, validated threats through the risk dashboard. This relieves them of a lengthy discovery process, by communicating relevant data in just a few clicks.



Interset's security analytics leverage data from multiple data sources, for the most comprehensive view of enterprise risk and contextual threat detection across these datatypes.

From these data sources, unsupervised machine learning evaluates the risks of normal digital footprints—of users, machines, files, projects, servers, shares, resources, websites, and IP addresses—to spot abnormalities.

Account Misuse	Compromised Account	Data Staging/Theft	Infected Host	Internal Recon	Lateral movement	Fraud
Authentication Logs	Authentication Logs	Endpoint Logs	Web Proxy Logs	Authentication Logs	Authentication Logs	Expense
Directory Service Logs	Directory Service Logs	Directory Service Logs	Directory Service Logs	IP Repository Logs	IP Repository Logs	
Endpoint Logs	Operating System Logs	IP Repository Logs	Endpoint Logs	File Share Logs	File Share Logs	
Operating System Logs	File Share Logs	Printer Logs	NetFlow Logs	Operating System Logs	Operating System Logs	
File Share Logs	VPN Logs	Web Proxy Logs		Resource Access Logs	Resource Access Logs	
VPN Logs	Resource Access Logs	Printer Logs		Endpoint Logs	Endpoint Logs	
Resource Logs	IP Repository Logs	NetFlow Logs		NetFlow Logs	NetFlow Logs	
IP Repository Logs		Email Logs				
Printer Logs						

Current data sources processed by Interset

For a full list of features, please contact Interset at sales@interset.com.

INTERSET

Contact **sales@interset.com**

Interset, an AI security analytics company, empowers security teams to identify and respond to the threats that matter before data is stolen. Interset's self-learning threat detection platform leverages AI and machine learning to measure the unique digital footprint of systems and users, distilling billions of events into a handful of prioritized threat leads. What used to take months, can now take minutes. Interset is backed by In-Q-Tel and trusted to protect critical data in finance, critical infrastructure, high-tech manufacturing, healthcare, utility and energy industries. Visit us at **interset.ai**, and follow us on **Twitter**, **LinkedIn**, and **Facebook**.