SenSage AP

Big Data Security and Compliance Analytics

NO ORGANIZATION IS IMMUNE TO INSIDER THREATS

Insider threats are on the rise and are among the most difficult to detect. A person you know and presumably trust — an employee, a former employee, a contractor or business associate — through accidental or malicious actions can put your organization and digital assets at risk. IgniteTech's SenSage AP Insider Threat is uniquely suited to help organizations deal with this growing problem.

DETECTING INSIDER THREATS WITH SENSAGE AP

Most organizations focus their threat detection on perimeter defenses such as firewalls, antivirus and IDS/IPS. Insider threats are immune to these defenses since the threat is already inside the network. To detect these kinds of threats, you need to look at historical activity in your environment and identify new, unknown behaviors.

IgniteTech's SenSage AP is uniquely suited to help organizations deal with the growing problem of insider threats. For careful detection, you need to look at patterns of behavior over periods of time. The vast majority of breaches are discoverable in the log data that machines generate. SenSage AP uses advanced analytics and modeling of log data, as well as other information, to simplify the process of detecting insider threats

Detecting insider threats is a three-step process:

Step 1: SenSage AP Insider Threat pulls data from four different sources: 1) email behavior, 2) internet upload behavior, 3) login behavior and 4) HR information. Each data source comes pre-configured with a best-practice weight based on published research. Tuning of the weights is also possible. (For example, your organization may have a very email-centric culture, so in your organization, email could be weighted higher than outbound Internet traffic.

Step 2: The insider threat data model then executes several statistical algorithms incorporating the weighted importance and calculates a risk number for every individual in the organization. Each day's summary information is stored in a rolling table of metrics for comparison over time.

Step 3: Reports can be run daily or at any frequency you need. The results of the calculations are displayed in an Executive Insider Threat Dashboard. Each individual is listed based on their risk indicator score and how that score deviates from the average. You can quickly see the historical trend of the three highest-risk individuals.

If your organization discovers an individual who may be a threat, you need access to the original log data for investigation and possible legal proceedings. Although SenSage AP Insider Threat can normalize the data across various sources when querying in order to conduct complex analytics, it also retains all information in its original format so you have proof in a court of law.

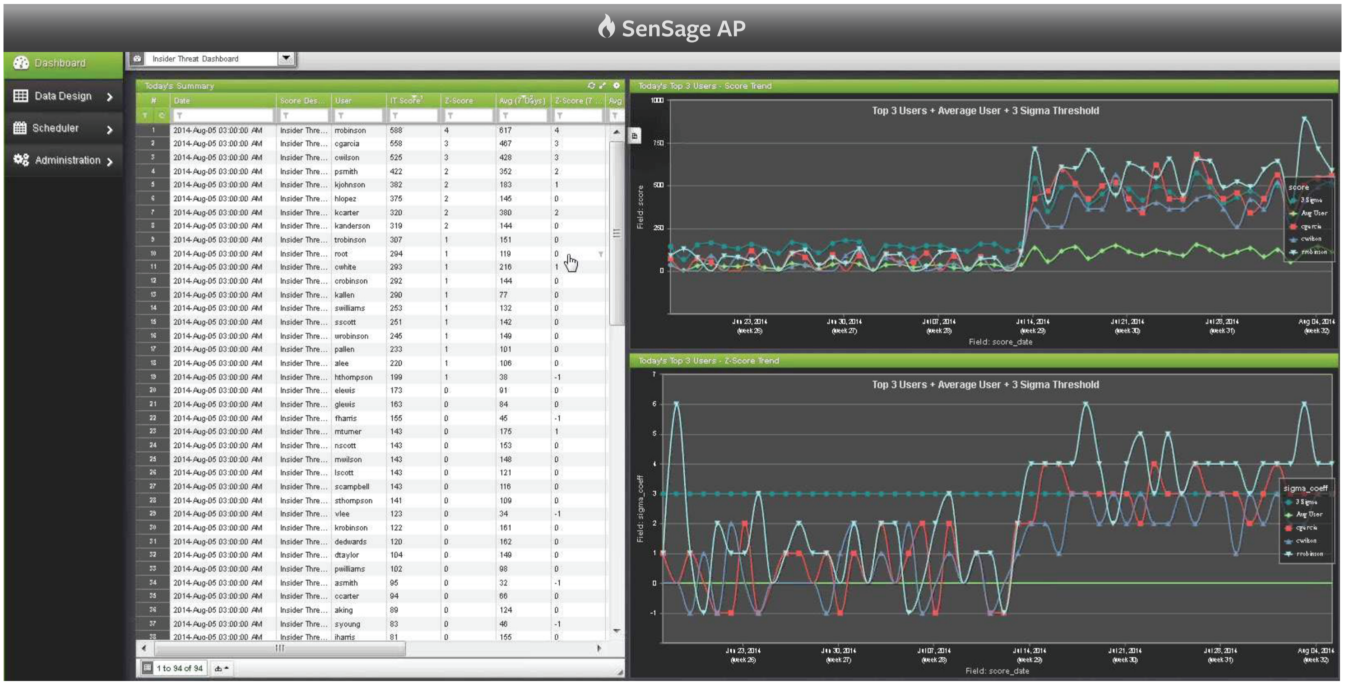
IGNITETECH™

START PROTECTING YOUR ORGANIZATION TODAY

No organization is immune to insider threats. Whether through negligence or malicious intent, individuals with access to your security practices, data and computer systems can put your confidential or commercially valuable data, intellectual property and computer systems at risk.

THE BEST INSIDER THREAT SOLUTION AVAILABLE TODAY

- The more data you add to Splunk, the slower it performs. With SenSage AP Insider Threat, there is no performance penalty for storing years, or even decades, of data.
- Hadoop performance suffers between parsing different data formats and running reports against complex queries. SenSage AP Insider Threat parses hundreds of different data formats automatically and expeditiously, with an easy-to-use graphical interface.
- Point-specific insider threat solutions are limited.
  - — Solutions like Lancope only look at network traffic — just one small portion of the data you need to analyze to deduce where insiders may be lurking.
  - — Solutions like Veriato require agents for snooping on employees. Agents can be disabled and/or bypassed and are difficult to maintain.
  - — Solutions like Palantir require immense financial investment and months before providing initial value.
  - — Solutions like Securonix have proprietary analytics that you can't see, modify and extend on your own, making it difficult to tailor to your specific enterprise.



Today's Summary

#	Date	Score Des...	User	IT Score	Z-Score	Avg (7 Days)	Z-Score (7 ...	Avg
1	2014-Aug-05 03:00:00 AM	Insider Thre...	rrobinson	588	4	617	4	
2	2014-Aug-05 03:00:00 AM	Insider Thre...	cgarcia	558	3	467	3	
3	2014-Aug-05 03:00:00 AM	Insider Thre...	cwilson	525	3	428	3	
4	2014-Aug-05 03:00:00 AM	Insider Thre...	psmith	422	2	352	2	
5	2014-Aug-05 03:00:00 AM	Insider Thre...	kjohnson	382	2	183	1	
6	2014-Aug-05 03:00:00 AM	Insider Thre...	hlopez	375	2	145	0	
7	2014-Aug-05 03:00:00 AM	Insider Thre...	kcarter	320	2	380	2	
8	2014-Aug-05 03:00:00 AM	Insider Thre...	kanderson	319	2	144	0	
9	2014-Aug-05 03:00:00 AM	Insider Thre...	trobinson	307	1	151	0	
10	2014-Aug-05 03:00:00 AM	Insider Thre...	root	294	1	119	0	
11	2014-Aug-05 03:00:00 AM	Insider Thre...	cwhite	293	1	216	1	
12	2014-Aug-05 03:00:00 AM	Insider Thre...	crobinson	292	1	144	0	
13	2014-Aug-05 03:00:00 AM	Insider Thre...	kallen	290	1	77	0	
14	2014-Aug-05 03:00:00 AM	Insider Thre...	swilliams	253	1	132	0	
15	2014-Aug-05 03:00:00 AM	Insider Thre...	sscott	251	1	142	0	
16	2014-Aug-05 03:00:00 AM	Insider Thre...	wrobinson	245	1	149	0	
17	2014-Aug-05 03:00:00 AM	Insider Thre...	pallen	233	1	101	0	
18	2014-Aug-05 03:00:00 AM	Insider Thre...	alee	220	1	106	0	
19	2014-Aug-05 03:00:00 AM	Insider Thre...	hthompson	199	1	38	-1	
20	2014-Aug-05 03:00:00 AM	Insider Thre...	elewis	173	0	91	0	
21	2014-Aug-05 03:00:00 AM	Insider Thre...	glewis	163	0	84	0	
22	2014-Aug-05 03:00:00 AM	Insider Thre...	fharris	155	0	45	-1	
23	2014-Aug-05 03:00:00 AM	Insider Thre...	mturner	143	0	175	1	
24	2014-Aug-05 03:00:00 AM	Insider Thre...	nscott	143	0	153	0	
25	2014-Aug-05 03:00:00 AM	Insider Thre...	mwilson	143	0	148	0	
26	2014-Aug-05 03:00:00 AM	Insider Thre...	lscott	143	0	121	0	
27	2014-Aug-05 03:00:00 AM	Insider Thre...	scampbell	143	0	116	0	
28	2014-Aug-05 03:00:00 AM	Insider Thre...	sthompson	141	0	109	0	
29	2014-Aug-05 03:00:00 AM	Insider Thre...	vlee	123	0	34	-1	
30	2014-Aug-05 03:00:00 AM	Insider Thre...	krobinson	122	0	161	0	
31	2014-Aug-05 03:00:00 AM	Insider Thre...	dedwards	120	0	162	0	
32	2014-Aug-05 03:00:00 AM	Insider Thre...	dtaylor	104	0	149	0	
33	2014-Aug-05 03:00:00 AM	Insider Thre...	pwilliams	102	0	98	0	
34	2014-Aug-05 03:00:00 AM	Insider Thre...	asmith	95	0	32	-1	
35	2014-Aug-05 03:00:00 AM	Insider Thre...	ccarter	94	0	66	0	
36	2014-Aug-05 03:00:00 AM	Insider Thre...	aking	89	0	124	0	
37	2014-Aug-05 03:00:00 AM	Insider Thre...	syoung	83	0	46	-1	
38	2014-Aug-05 03:00:00 AM	Insider Thre...	iharris	81	0	155	0	

1 to 94 of 94

SenSage AP Insider Threat's Configurable Executive Dashboard

FOR MORE INFORMATION

Contact: success@ignitetech.com
Visit: ignitetech.com/sensage-ap
Follow: linkedin.com/company/ignite-tech