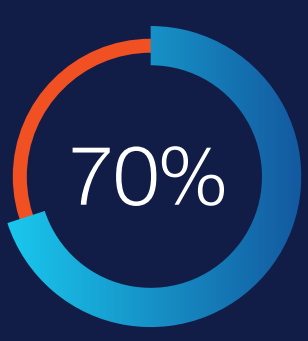
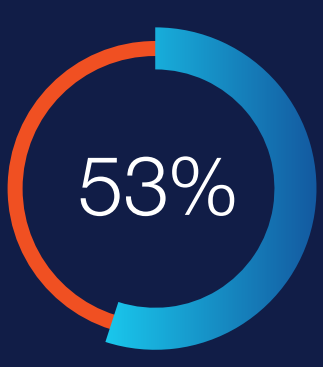
SECURONIX™

7 THINGS TO LOOK FOR IN AN INSIDER THREAT SOLUTION

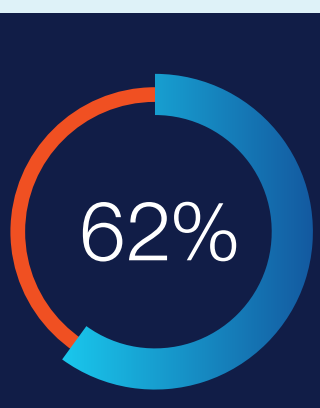
THE GROWING PROBLEM WITH INSIDER THREAT



70% of organizations confirm insider attacks are becoming more frequent.[1]



While the true cost of a major security incident is not easy to determine, the most common estimate is less than $100,000 per successful insider attack (53%). Thirty-one percent of cybersecurity experts expect damages between $100,000 to $500,000.[1]



62% of insider threats detected were aimed at exfiltrating data. The exfiltration of data deemed sensitive continues to be the most common insider threat.[2]

STOPPING THREATS IS COMPLICATED

Companies are Moving to the Cloud

56% The shift to cloud computing is making the detection of insider attacks more difficult, as confirmed by 56% of cybersecurity professionals.[1]

40% Only 40% of organizations monitor user behavior across their cloud footprint.[1]

User Privacy Concerns

73% User privacy is a significant concern in the context of insider threat monitoring for seven out of ten organizations we surveyed (73%).[1]

Insider Threats are Already Inside the Company

56% Because insiders often have elevated access privileges to sensitive data and applications, it becomes increasingly difficult to detect malicious activity (56%).[1]

60% 60% of insider threats involve employees planning to leave the company.[2]

7 Things to Look For The Securonix Insider Threat Solution

Centralized Logs and Identity Context
- The ability to ingest a variety of technical and non-technical data, such as badge data.

Identity and Access Correlation
- Build a comprehensive profile of every entity: users, IP addresses, and hosts.
- Enrich events with entity context including identity, asset, geolocation, threat intelligence and data from lookup tables.

Behavior and Peer Analytics
- Behavioral analytics detect deviations from what is deemed as “normal” behavior for accounts, users, and systems.
- Peer-based analytics detect outliers within a peer group – such as a department, division, or a job function.

Insider Threat Specific Content
- Includes out-of-the-box content for basic insider threat monitoring.
- Provides the ability to create custom content for specific use cases.
- Incorporates user behavior-based anomaly detection.

Threat Chains
- Facilitate stitching or chaining individual events into one holistic threat.

Investigation and Response
- Provide the necessary context needed for complete investigations.
- Facilitate the necessary escalation and triage workflow.

Data Privacy
- Role-based access controls restrict users to only the data they are entitled to.
- Data masking protects individual privacy.
- A full audit trail records all activity that takes place.
- Approved and certified by over 15 works councils across Europe, Africa, and Asia.

LEARN MORE

- 2020 Securonix Insider Threat Report
- Justifying Your Insider Threat Program
- Insider Threats: Why It Continues to Matter Today

Sources

[1] 2019 Insider Threat Survey Report: https://www.securonix.com/resources/2019-insider-threat-survey-report/
[2] 2020 Securonix Insider Threat Report: https://www.securonix.com/resources/2020-insider-threat-report/

SECURONIX™

www.securonix.com