ABOVETHE RISK

IVILEGED USER INSIDER THREAT SURVEY RESULTS – FEDERAL

Did you know that privileged users often are your riskiest employees?

Security from the inside-out is the key to achieving deep visibility and stopping insider threats.

INSIDER THREATS

51%

of organizations feel they have the capability to effectively monitor privileged user activity



63%

of their tools yield too

many false positives

VISIBILITY

are somewhat to not confident at all they have enterprise wide visibility for user access

do not or are unsure if they correlate data from multiple sources, 55% say this is due to lack of resources



BACKGROUND CHECKS

background checks lacking within organizations before issuance of privileged credentials



ACCESS PRIVILEGES

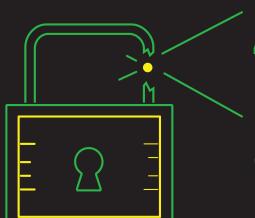


use endpoint monitoring to determine if action taken by an insider was a threat



have no way to gain context around the actual act

SOCIAL ENGINEERING

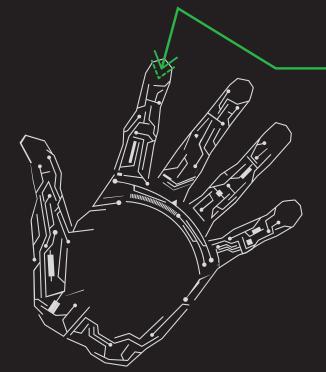


surveyed said malicious insiders would use social engineering to

56%

believe social engineers from outside will target privileged users to obtain access rights

obtain someone's access rights



HUMAN FACTOR



78%

think privileged users believe they are empowered to access all the information they can view

68%

say these same people access sensitive or confidential data out of curiosity



51%

point out organizations assign access to individuals that go beyond their role or responsibility

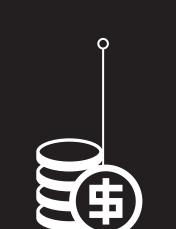
MANUAL PROCESS

44% 23%

2011 2014 2016

use manual processes to certify privileged users

BUDGET



68%

have a dedicated budget, but **57%** say the budget is 10% or less



51%

80%



54%

use SIEM to determ<u>ine if action</u> is an insider threat









