Security Maturity:

Where is my organization in the journey to reducing risk?

Secureworks



Secureworks' Security Maturity **Evaluation Identifies Common Steps** In the Path to Cyber Resilience

No two organizations are alike, and the same can be said for their short-term cybersecurity priorities. Yet a 2018 survey by Secureworks found that there are similarities in the steps that organizations take over time to successfully achieve cyber resilience. According to Secureworks survey of cybersecurity leaders, companies further along in the security maturity journey shared common operational, governance, preparedness and cloud security capabilities. Follow the path below to compare your journey to security maturity versus other respondents.

MATURITY TIERS

PROFILES OF

Guarded

Informed

Integrated

Resilient



limited customization and a focus on compliance. The security team is typically embedded within the overall IT organization with split responsibility between IT and Security, managed by mid-level managers. These organizations tend to not have CISO-level leadership. Cloud solutions are often run independent of the security team.

These organizations implement basic network protection often using off-the-shelf tools and technology with



still fall under the overall IT department. The security teams have started to standardize IR procedures and, operationally, integrate multiple TI sources. They tend to implement more layered defense tactics and leverage more security technology. They also extend their influence into the business with more input, but still have limited control over cloud services.

These organizations approach security with a proactive face, often customizing and extending their IR, endpoint and TI capabilities into the company operations. Their security teams are larger and have more resources available to manage advanced security operations, augmenting their in-house capability with third parties to give better coverage across the business. The security leader, often a C-level executive, applies

security thinking to business strategy and operations planning.

These organizations often have security teams with their own senior leadership and reporting structures yet



enabling them to withstand or recover quickly from security issues. These organizations have larger inherent risk due to the nature of their business and integrate advanced techniques like AI and ML into the security infrastructure. The business, as a whole, is engaged in security planning and execution. Given the level of expertise, these organizations typically have large internal staffs and a C-level CISO who provides regular Board-level reports on security matters.

These organizations standardize and embed security activities within and across business operations,



started hiring inhouse IR staff

73%

of Informed

organizations have

Explore automated integration of TI;

multiple feeds to

infrastructure and

business

Consider hiring Incident Response experts in-house and build a proactive IR program

Establish

organization-wide

communication framework for critical

threat events

providers to gain better visibility, reduce noise and

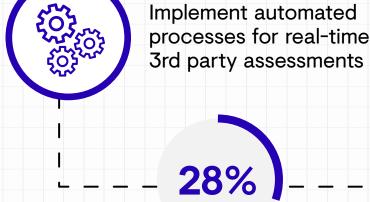
organizations have 3rd party evaluation process Leverage security services

of Informed

evaluation process

INTEGRATED

take the right action



of Integrated organizations

do real time, automated

evaluation of 3rd Party

providers

Begin to automate key process workflows and response activities to known threat scenarios using orchestration platforms

Security & Business **Executive teams**

Ο 🗆 Δ

Conduct table top IR

exercises with IT,

address "Shadow" cloud issues

27%

of Integrated organizations

RESILIENT

of Resilient

organizations

deepen real time log management

Integrate TI data

directly into security

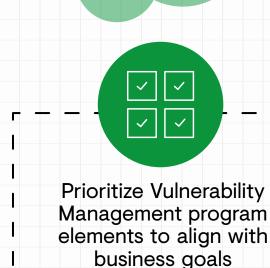
workflows and

technologies

Reduce

"shadow" cloud

service usage



capabilities

Deepen real-time log

analytics capabilities

management and

of Resilient organizations increase Increase use of orchestration

Journey continues as

business evolves

operations To find out exactly where your company sits in the security maturity journey and how you compare to peers, take the complimentary Secureworks Security

use of orchestration

across security

across security

operations

Find out More:

Maturity Evaluation. To review the comprehensive results of our 2018 Security

Maturity Survey, read our E-Book.