CASE STUDY

NESSUS USER PROFILES

THE CONSULTANT

Cybersecurity consultants play pivotal roles in a constantly shifting threat and vulnerability landscape. They must not only keep abreast of changes to the compliance and threat landscape but also back up their comprehensive knowledge of security with sound practices and reliable tools – including Nessus, the world's No. 1 vulnerability assessment solution.

Key responsibilities

Consultants help clients of all kinds – enterprises, small businesses and everything in between, across all industries – identify and properly address cyberthreats. Jobs run a wide gamut in terms of clients' tech experience: One day, a pro consultant will assist the leader of a company who is knowledgeable but lacks the budget to hold down full-time IT staff; the next they may be working with a national business that has an IT team but is still using legacy systems. As such, flexibility is of the essence for consultants, and so is the ability to explain threats clearly and succinctly.

While specific duties vary, consultants typically handle the following tasks:

- Integrating security controls into a client's IT environment.
- Identifying weaknesses in systems and software.
- Monitoring vendor and third-party information.
- Analyzing potential risks (including compliance issues).
- Compiling and presenting reports on findings and offering recommendations for threat mediation and ongoing mitigation.

Common challenges

Identifying new threats and vulnerabilities is a high priority for any cybersecurity consultant, as these almost always pose a greater danger than malware or other exploits that are known quantities. But if an inferior vulnerability assessment tool is used, or one that is otherwise limited in terms of scope and depth, there's a significant chance that vulnerabilities might be missed.

An inadequate scanning solution will also make it more difficult to achieve full visibility and find the root cause of any undetected vulnerabilities that the network, its hosts or both may be harboring. Clients will expect their cybersecurity consultants to present detailed reporting on any vulnerabilities that are uncovered, and if the right tools aren't used, it may not be possible to create truly customized reports, which won't be as useful to customers.

Identifying new threats and vulnerabilities is a high priority for any cybersecurity consultant, as these almost always pose a greater danger than malware or other exploits that are known quantities.

How Nessus helps

Nessus is No. 1 in vulnerability assessment. The solution's accuracy and level of coverage notably outpaces competing tools and has the fewest instances of false positives. This is a major advantage for consultants. This is in no small part due to the hard work of the Tenable Research team, which works relentlessly to develop plugins that address the newest vulnerabilities and threats. When high-profile threats emerge, Tenable Research releases coverage within 24 hours. Nessus is particularly effective when used as a supplementary tool in the context of a penetration test, because scans will quickly identify network areas or hosts that deserve the most intense scrutiny.

Because every client a consultant faces is vastly different, the ability to customize scans is critical, and Nessus makes it easy to do just that. Additionally, the Nessus license is transferable, further simplifying the workload of busy consultants who must quickly move back and forth between customers.

Ready to get started?

TRY NESSUS FREE FOR 7 DAYS

tenable®