Measure your ability to recognize and respond to cyber attacks.

Factsheet

Attack Detection Assessment

verizon✓

Data breaches don't play out in minutes or hours so much as weeks or months.

Research from our Data Breach Investigation Report (DBIR) shows that, on average, the time frame from initial point of intrusion until the victim realizes they have a problem spans almost seven months. In addition, more than two-thirds of all victims learned of a breach from a third party. But the inability to recognize and react to the lead indicators of a cyber attack – before time goes by and it blows up into serious intrusion or data theft – can be a security operation's greatest weakness. That's why response time is critical when it comes to cyber-incident detection and handling.

An Attack Detection Assessment can measure your ability to quickly and efficiently recognize and respond to cyber attacks. The assessment can help you identify attacks with greater speed – helping you discover what's happening and take action sooner in the early stages of an attack.

Close the cyber-attack detection gap

We can evaluate the detection technologies, systems, and incident handling processes you already have in place and provide meaningful and cost-effective ways to help you:

- Improve event detection processes.
- Put incident classification into better practice.
- Streamline the infusion of high-fidelity cyber intelligence.
- Increase alerting and visualization capabilities.
- Limit dwell time and better set the stage for incident triage.

The assessment comprises six phases of engagement:

Phase 1: Defensive Countermeasures

Assessment of your defensive and threat-hunting capabilities, focusing on the selection, positioning, and configuration of technologies in place, including but not limited to firewalls, host and network-based intrusion detection, beacon identification and antivirus.

Phase 2: Raw Event Visibility

We measure your ability to see a clear, detailed picture of external, internal, and partner-related cyber attacks. We look for gaps that limit your view of raw events, enabling them to go undetected.

Phase 3: Incident Classification

At the intersection of digital alert streams and human intervention, we evaluate how you classify incidents by risk or severity and the effectiveness of human and automated incident-classification processes.

Phase 4: Intel Fusion

An analysis of the effectiveness of cyber intelligence combined with your incident handling processes. We assess intelligence sources, collection mechanisms, archive and retention platforms, vetting, and the overall blend of these tactics across log streams.

Phase 5: Visualization and Situational Awareness

We test your selection, deployment, configuration, and use of visualization tools to enable situational awareness and measure how those tools are applied to enhance existing infrastructure and process.

Phase 6: Incident Triage

We'll review your process for handing off designated risky incidents to operational incident-handling or Computer Emergency Readiness Team (CERT) staff, in accordance with your incident response plan, and evaluate the effectiveness of the feedback loop into device tuning.

Once all six phases of the Attack Detection Assessment are complete, we immediately communicate any significant weaknesses or points of security exposure we discover. Next, we present a report of our findings and actionable recommendations to help you enhance your situational awareness of cyber attacks in motion and benchmark current incident-handling capabilities against comparable organizations.

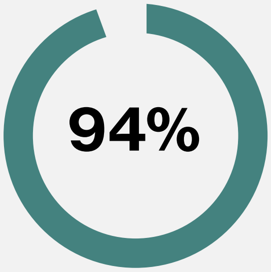
Why Verizon

We're focused on our customers' long-term success and safety – and we draw on years of security experience to help them achieve this.

We analyze security events every day at Verizon's Threat Research Advisory Center. And that means we can keep up with the latest cyber threats. With our substantial risk and incident experience, we can help you understand the real-world security controls that are most effective.

We draw expertise from:

- Over 13 years of forensic investigations
- Over 61 B security events
- Publishing 11 Data Breach Investigations Reports covering 13 years of data – including 10,000+ confirmed breaches and 290,000+ incidents



Of the breaches we've analyzed, 94% of security incidents and 90% of confirmed data breaches fall into one of nine patterns.

On average, we monitor 61+ billion security events annually.

Learn more

Learn how prepared your organization is to recognize and handle threats, so you can accelerate your detection capabilities and strengthen countermeasures.

To find out how an Attack Detection Assessment can help improve your security incident handling and cyber defenses, contact your account manager or visit:

verizonenterprise.com/products/security

verizonenterprise.com