appdome

SolarWinds Advisory

What the SEC's Actions mean to mobile brands.

Tom Tovar
Co-Creator @ Appdome
January 2024 v2.6

Two Things to Know.

#1 New SEC Rule

4-days to Remediate or Disclose Cyber Incidents.

July 26, 2023, the SEC released a 4-days rule to disclose "any cybersecurity incident" that will have a "material impact or reasonably likely material impact" on the business.

#2 SEC Fraud Indictment

State of Security Must Match Public Statements.

October 30, 2023, the SEC filed an action against SolarWinds & its CISO alleging fraud because their "public statements" about the state of cyber security "were in stark contrast" to the reality.

Fix or Disclose rule driven by...

- **SEC 4-Day Rule**
  - SEC wants cybersecurity disclosure in a *more consistent, comparable, and decision-useful way*
  - Requires companies to disclose:
    - any cybersecurity incident,
    - determined to have a material impact, or
    - is *reasonably likely* to have material impact on the brand or business.
  - If "material impact" occurred, disclose it. If "reasonably likely" but no impact, remediate (fix) fast.
  - Disclose can be avoided only if US Attorney General finds disclosure poses a national security risk.
- **SEC Indictment Against SolarWinds & its CISO**
  - "Standard security practices" like "vulnerability testing," and "penetration testing" are not enough.
  - **The Fraud:** SEC said "public statements and "omissions" on website and in filings concealed the Company's poor cybersecurity posture and "its heightened— and increasing—cybersecurity risks."
  - **No Attack Needed:** SEC said the Company and CISO's actions would have "violated the federal securities laws even if SolarWinds had not experienced a major, targeted cybersecurity attack."
  - State Attorney Generals follow the SEC's lead and charge fraud against companies and their CISOs.

Action Plan to Meet 4-Day Rule.

Automate Cyber Delivery

Use Appdome to accelerate cyber defense delivery and automate rapid response to new attacks to ensure continuous compliance with cyber and fraud objectives with customers and employees.

Defend the Brand Promise

Mobile brands must deploy Android & iOS defenses that deliver protection from cyber attacks, fraud, malware and other threats expressed or implicit in their brand promise, including in cyber pledges, release notes, on websites, etc.

Build a Record of Compliance

Use Appdome to build a record of compliance in your cyber defense and fraud objectives. Appdome offers Certified Secure™ attestation for every build and continuous compliance tracing to prove compliance on demand.

Audit DevSecOps & Waivers

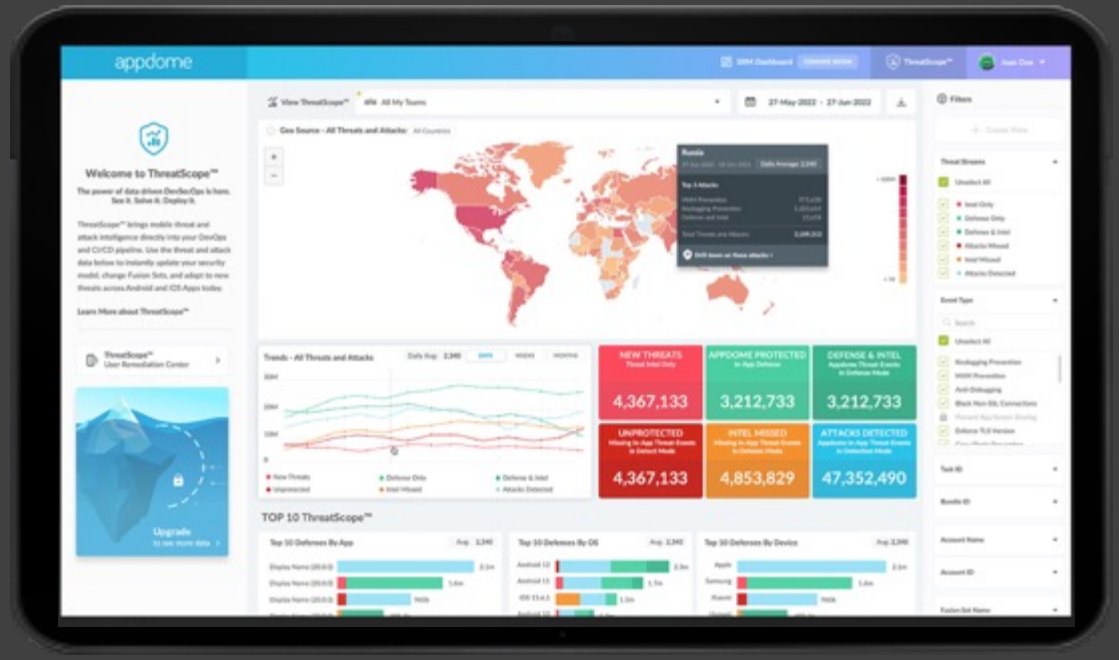
The traditional DevSecOps process can leave an unflattering audit trail of postponed and/or failed remediations that could come back to bite you. Review your risk acceptance waivers for any pattern that might show your brand isn't taking cybersecurity seriously.

Managing Disclosure Requires Visibility.

#3 Defense Alone, Not Enough

Brands can't be reckless or negligent in reporting incidents.

In SolarWinds, SEC said multiple attacks of increasing severity went undetected from unmanaged mobile devices connected to a VPN. With ThreatScope™, you can detect any of 160+ attacks, determine impact, and respond fast.



** Appdome ThreatScope™ Mobile XDR*

About the Author.

Tom Tovar
CO-Creator & CEO
Appdome.

Tom is the co-creator of Appdome. He's started his career as a Stanford-educated, tech-focused, corporate and securities lawyer. Then, he turned his attention toward business operations, mobile development and ethical hacking. He has 25 years in the cyber and networking space, serving in C-Level leadership roles at Netscreen (firewall, SSL company) Nominum (DNS, DDoS Prevention company) and sits on the board of directors at other cyber and technology companies.

Tom would like to point out that this presentation is not legal advice. If you have legal questions, consult your lawyer. ☺

appdome

Thank you!

If you only had 4 days could you deliver...

Tom Tovar
Co-Creator @ Appdome
January 2024 v2.6