

A large manufacturer uses Cronus's CyBot to secure its network

A leading cement producer in Israel, required an efficient and continuous pen testing solution and vulnerability management tool to help keep critical business process safe and create a smarter remediation plan

COMPANY SUMMARY

One of the largest manufacturers in Israel in the construction industry.

Deal size: 1000 IP

CHALLENGES

The manufacturer was looking for an alternative to manual pen testing and rigorous and ineffective blind patching that did not effectively stop hackers. The cement industry is relatively conservative and low tech, there is no internal expertise on hacking or pen testing. Therefore the company was dependent on outsourced personnel for its pen testing and remediation needs.

SOLUTION

Cronus Cyber Technologies has developed the CyBot, the first machine-based penetration testing solution that can deploy globally and mimics human ethical hackers that work 24/7, provide a map of global attack path scenarios so you can fix only the vulnerabilities that matter. The CyBots Pro's were installed in the client's network and quickly shown how hackers could penetrate and leap within the network to reach critical assets. Using the Cronus Dashboard and reporting tools, the manufacturer can now manage their own pen testing in-house and receive a smart shortlist of remediations that will effectively stop potential hackers from reaching critical assets.

BENEFITS

- In-house IT can manage the CyBot, not need to outsource penetration testing
- Continuous 24/7 pen testing
- On premise installation
- No false positives, No false positives
- Actionable business and security insights
- Smart shortlist of remediation's that effectively block potential attack path scenarios
- Intuitive dashboard