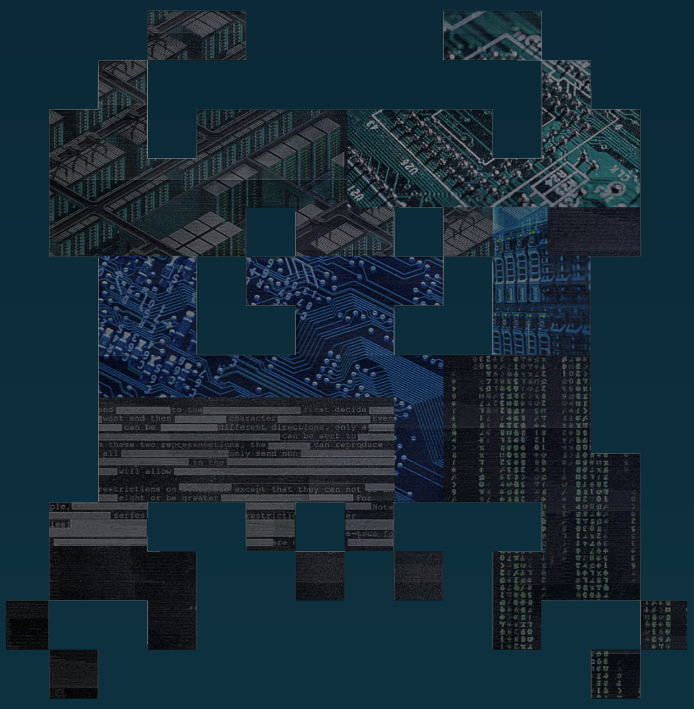
intruder

Intruder Vanguard

We discover weaknesses in your digital infrastructure so hackers don't get to



A selection of success stories from the team running the security operations behind our **Vanguard** service

Intelligence-driven Investigations

The team closely monitors vulnerability disclosures across a range of feeds and news sources. When serious new vulnerabilities are disclosed, the team's first thoughts are –

"how does this affect our **Vanguard** clients?"

A recent critical Exchange vulnerability, nicknamed **Proxylogon** provides a good example. After hearing reports of the vulnerability from Microsoft and from discussions across the security community, Intruder moved to scan its Vanguard clients using proof of concept code as soon as it became available – and before checks were added by the market leading vulnerability scanners. Response time for this vulnerability was key, as active exploitation was being carried out by state-sponsored threat actors.

One of our clients, a major automotive manufacturer, was affected by Proxylogon, and through testing Intruder gained complete control over a vulnerable Exchange server. After receiving a notification from Intruder, the system was patched, and re-testing confirmed that the vulnerability was no longer exploitable. Other Vanguard clients' Exchange servers were tested and found to be unaffected, a reassurance that was also communicated to them.

Vanguard clients have received early warning of similar Exchange weaknesses, such as the high severity **Forgot2kEyXCHANGE**. The Vanguard team tracked this disclosure from its first announcement as part of Microsoft's Patch Tuesday, and quickly identified twenty vulnerable systems over three Vanguard customers, who were all alerted. Patch Tuesdays are frequent drivers to Vanguard investigations.

SMBGhost is another example, a serious and potentially wormable vulnerability affecting Windows systems. An Emerging Threat Scan from Intruder identified SMBGhost on a Vanguard client. Testing however, revealed that exploitation was not successful with public exploits at the time. The client was informed that the scan result may have been a false positive, but remediations were still advised, as the threat of non-public exploits remained.

> Thanks team, much appreciated!
>
> Genetic biotechnology producer

> Thanks guys, this was super helpful.
> We are now patched and protected 🙂
>
> Endpoint protection software provider

Though lacking a catchy name, **CVE-2020-3452** was a similar case. This flaw offers attackers the ability to download arbitrary files from vulnerable Cisco networking devices. After hitting the news, the team identified the vulnerability on systems belonging to two Vanguard clients. Exploitation, however, did not uncover any overly sensitive files.

Security Oversight

The signal to noise ratio from vulnerability scanning isn't always perfect, and an extra set of eyes to review scan results is highly beneficial. False positive elimination is a popular feature of **Vanguard** – where vulnerabilities are manually checked, to remove findings that are not exploitable.

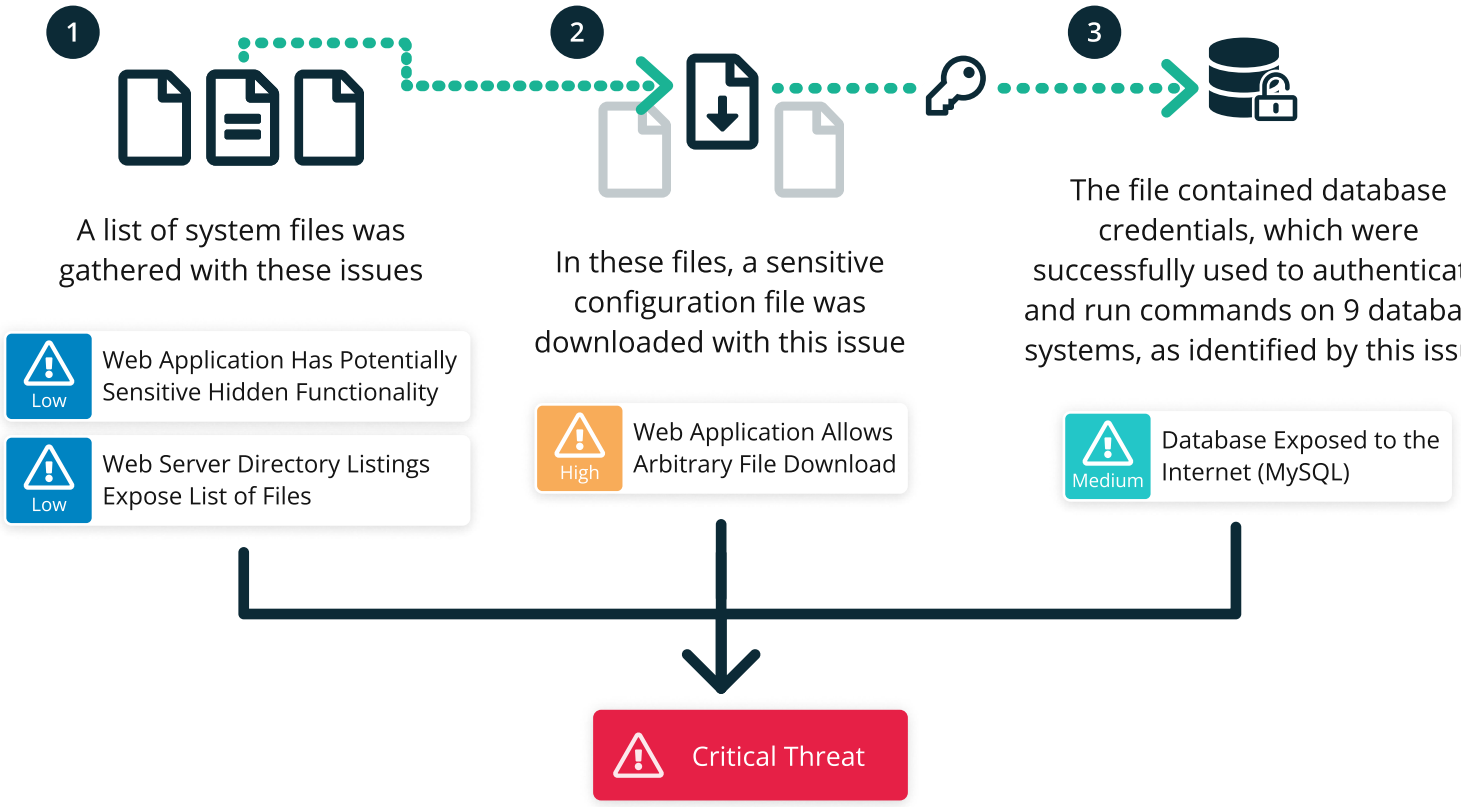
Conversely, there are also cases where legitimate threats don't receive as much attention as we believe they deserve, which is when the team steps in. After reviewing a client's monthly scan, Intruder's analysts noted that a SQL injection vulnerability had been 'snoozed' – effectively hiding it from reporting. The Vanguard team demonstrated that this weakness was in fact exploitable and could be used to gain direct access to a database system. The database housed sensitive personal information of site users, the leakage of which could have posed regulatory ramifications. The client prioritised internally for remediation.

Severity levels assigned by vulnerability scanners don't always reflect the true risk presented by security weaknesses. An administrative panel being exposed to the internet could be considered a low or medium risk. Perhaps the admin uses weak credentials to login, which can be easily guessed by an attacker. This was the case for one Vanguard client, and it meant that IP-camera footage from inside an industrial warehouse was in effect openly accessible to the internet. In this case, the severity of the issue in the client's scan results was increased to reflect the ease of exploitation, and the client was notified.

Chained Exploitation

Intruder's penetration testers are encouraged to proactively seek out weaknesses within the assets under the protection of **Vanguard**. These highly skilled testers have a knack for discerning small vulnerabilities in scan reports which in combination are greater than the sum of their parts.

Here is an example found for a client in the eCommerce sector, which involved combining four issues that were reported by our vulnerability scanner.



In this example, no single finding would be rated a critical severity, however when combined, the threat posed comfortably met that criteria.

Ad-Hoc Requests

We frequently take requests and odd jobs to help clients improve their security. Here are some examples –

A leading multinational construction company was concerned about the security of some of their **Remote Desktop Services** (RDS). Our testers gave them a thorough review and successfully gained remote access to a domain system.

This system was connected to a wide network, in which an attacker could try to compromise further machines, exfiltrate sensitive information or deploy ransomware.

The client took immediate steps to remediate. When the time came to roll out a new RDS platform, Intruder also assessed this for security weaknesses.

The Head of IT Security at a client's organisation requested **issue severity increases**, to account for internal context and organisation-specific sensitivity. The team adjusted the issue severities, which were reflected in the client's reporting.

Validation of **bug bounty reports** from third-party security researchers or bug bounty schemes.

Customising scanning, for example by delivering ad-hoc scans, scans specifically targeting a particular weakness, and scan results in particular formats.

Summary

Intruder's **Vanguard** service delivers a hybrid approach of vulnerability scanning in conjunction with manual auditing by penetration testers. The security team behind Vanguard are all CREST or Offsec certified and have years of penetration testing experience.

To learn more about how **Vanguard** works, and how we can help solve your security problems, please reach out to us at contact@intruder.io.