VULCAN.

MANDIANT CASE STUDY

How Mandiant Uses Vulcan cyber for intelligent vulnerability remediation

The Mandiant Challenge

- Development teams too busy with product releases
- Too much vulnerability data
- Vulnerability prioritization not in business context

About Mandiant

Mandiant is an industry-leading cybersecurity solutions provider. It has identified and prevented major cyber attacks, and its products enable major organisations to protect against malicious software, analyze IT security risks, and stay ahead of threats. Since being founded in 2004, and being acquired by FireEye in 2013, Mandiant now has more than 3,000 employees across 19 global offices.

Vulcan Cyber Benefits

- Risk-based prioritization
- Consolidated data
- Improved collaboration
- Faster and more complete remediation

THE SITUATION

1

Development teams are busy releasing new features and are reluctant to focus on *theoretical* vulnerabilities that will never be exploited by a threat actor.

2

Huge amount of data from security tools. Thousands of vulnerabilities are detected, but many are not relevant based on Mandiant's risk profile.

3

Prioritizing these vulnerabilities is a manual and time-consuming process.

4

Meanwhile, zero day vulnerabilities are on the rise.

THE PROCESS

Vulcan asset management organizes data into business groups.

Risk-based prioritization identifies relevant candidates for remediation.

Collaboration and communication with dev teams via their tools, such as Jira.

Remediation campaigns activated for tracking remediation progress.

THE RESULTS

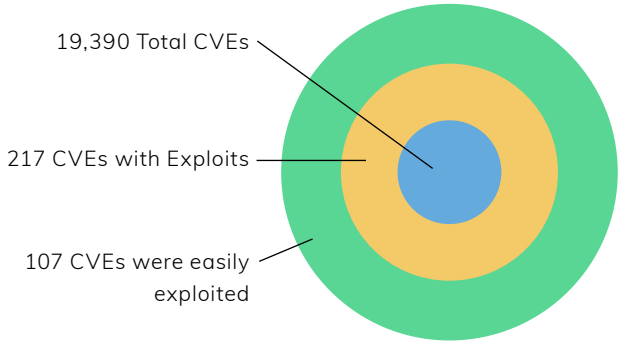
- Greater visibility of threats
- Increased collaboration
- Trackable progress
- Accelerated risk remediation

Challenge

Mandiant maintains its reputation as a cutting edge company through constantly introducing and implementing new features and capabilities into its products. In the view of DevOps and development teams, this progress can be held back by security professionals opening tickets for remediation of theoretical vulnerabilities, many of which will never have any real impact. Developers work hard and are reluctant or unavailable to address abstract security concerns.

For example, in 2021 so far, the security team uncovered over 19,000 CVEs. Of those 19,000, only 217 had real exploits attached to them. And less than half of those were easy to exploit.

2021 VULNERABILITIES



Exploit Rating	# of CVEs
Critical	1 (*)
High	31
Medium	57
Low	128

* CVE-2021-26855-Microsoft Exchange Server 2019 cumulative update 8 server-side request forgery vulnerabilty

Out of the 217 exploitable vulnerabilities, Mandiant had a human analyst assess the risk level and exploit difficulty of each vulnerability. Only 31 were “high risk” and only 1 was “critical”.

The traditional CVSS score method would have treated thousands of the CVEs as critical, but Mandiant’s risk profile is unique, as is every company’s. For Mandiant, certain assets are more significant than others, and vulnerabilities within those assets represent a greater potential risk than so-called “critical” vulnerabilities within assets less relevant to Mandiant’s business. The CVSS score takes an objective view of vulnerabilities’ criticality, and so carries limited usefulness when it comes to assessing risk.

Mandiant wanted a smart and efficient solution to consolidate their data and focus on the vulnerabilities that they believed to be critical.

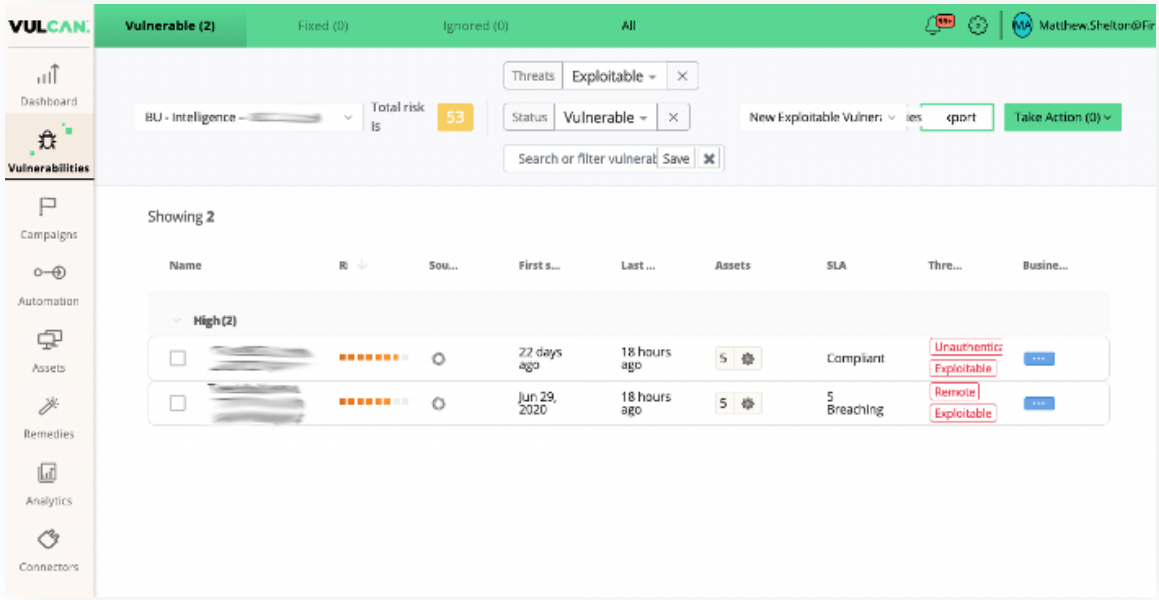
Not only that, but such an intelligence-led vulnerability management solution should also be centred around full remediation. This would help with cases like the PrintSpooler vulnerability, for which Microsoft announced a patch, but one which Mandiant discovered to be only sometimes effective.

The mass of data and limited developer availability - together with incomplete remediation and the growing number of zero-day vulnerabilities - mean that the need for an intelligent risk-based solution becomes even more pronounced.

- Development teams too busy
- Vulnerability data unfiltered and not prioritized
- Current processes are manual and inefficient

Solution

Vulcan ingests Mandiant's existing data and filters everything according to stakeholders, specific systems and business units. Mandiant has a saved search for "exploitable" and "vulnerable" assets, focusing on "critical" and "high". They also group their "crown jewels" - or most important assets - into their own business unit.



From here, the Mandiant team easily identifies the candidates for remediation that require the most immediate attention.

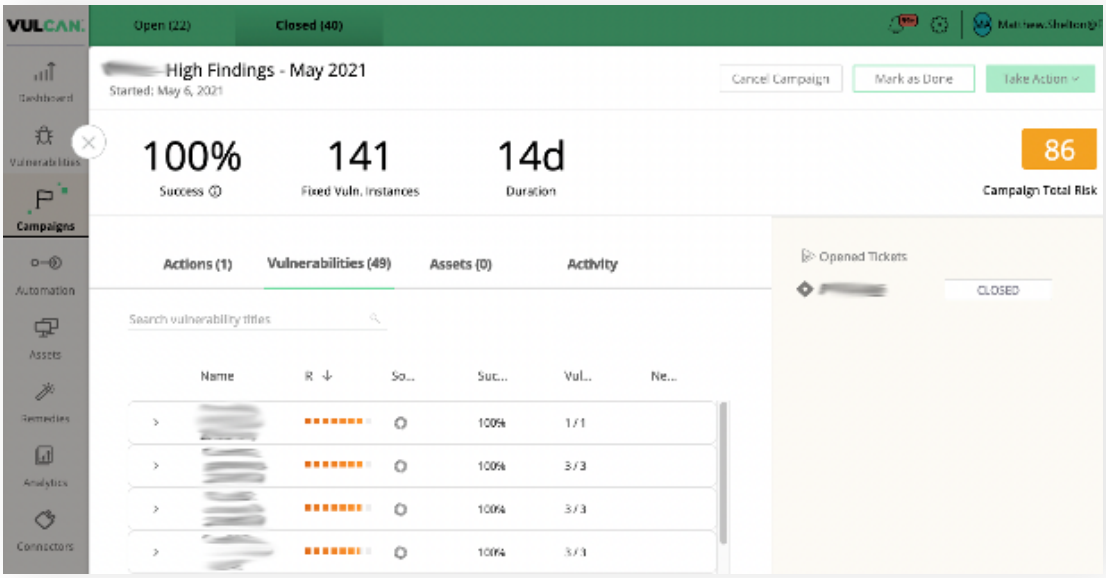
A remediation campaign is then created within the Vulcan platform that allows Mandiant to have full visibility of when each vulnerability is remediated across their environment. They can easily check the status of each vulnerability, and track the progress of the relevant people or teams in the remediation process.

Mandiant's engineering culture means they are heavily reliant on Jira - DevOps and development teams both expect their tasks to appear here. Vulcan lets Mandiant collaborate and communicate via Jira or any other tool they might use. This means that developers receive clear remediation instructions in a way that is clear to them, reducing any potential confusion at a critical part of the process.

- Better visibility and cyber asset management
- Risk-based prioritization
- Trackable remediation campaigns

Results

On this particular remediation campaign, Mandiant achieved 100% remediation within just 14 days:



Mandiant uses Vulcan to sift through the noise and find the signals they're looking for. Before Vulcan, they had several different repositories of information. Vulcan consolidated all this data and identified the most impactful vulnerabilities for Mandiant.

This works out for everyone. DevOps and development teams now receive only the most relevant, impactful vulnerabilities to work on. Meanwhile, the security teams know that the most impactful vulnerabilities are being remediated, and can see clearly what they need to focus on.

Intelligent risk-based remediation means that the right vulnerabilities get fixed for good, with trackable progress across every stage of the remediation lifecycle. This enables security teams to mitigate their risk, improve their processes and better protect their organizations against attackers.

- Minimal manual effort
- Increased productivity
- Remediation outcomes

Want to hear more about how Mandiant gets fix done with Vulcan?

See the Remediation Summit session from Matt Shelton, Director, Technology Risk and Threat Intelligence, here.