

# Incident Response Team

We know how stressful it can be to field an alert about a potential security incident. **We're here to help.**

**The Varonis Incident Response Team** is a group of in-house cybersecurity analysts that can assist in responding to incidents reported by Varonis alerts.



Available on-demand to customers and trial users  
**at no cost**



Most cases are seen by a security analyst  
**within 24 hours**



Globally distributed team of **20+ experts**

## What can the team help me with?



Forensics analysis



Containment, eradication, and recovery



Making recommendations to improve future detection & response

## What types of attacks can the team help with?



Brute-force attacks and account compromise



APT intrusions, malware, ransomware



Insider threats, suspicious data access, exfiltration

## How do I request help from the IR team?

Contact your Varonis account team directly to request help from the IR team. If you need urgent assistance, you can **contact our support team at [varonis.com/support](https://varonis.com/support)**.

# About the Team



## MATT RADOLEC

Security Architecture  
& Incident Response

Matt Radolec and the Varonis Incident Response Team are called in to respond to **hundreds** of new and nefarious attacks for clients and trial users every year.

From thwarting ransomware to catching rogue insiders red-handed, these world-class experts are trusted by the biggest brands on the planet to identify, investigate, and stop attacks before they become crisis situations.

The security research team at Varonis has been recognized for investigations leading to the discovery of APTs and new strains of malware such as [Qbot](#) and [Norman](#).

“Varonis showed us the full extent of the problem and played a big role in helping us eliminate it.”

“Varonis’ team didn’t offer any kneejerk solutions—they listened, took notes, did some homework, and came back with informed suggestions that actually helped us solve our problem.”

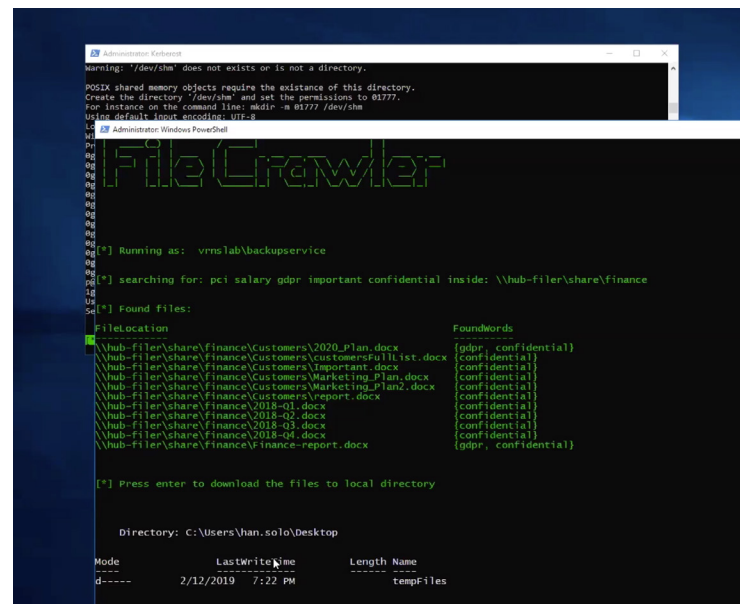
[Read a case study: varon.is/alertwin](https://varon.is/alertwin)

## Watch the IR Team in Action

Join our weekly cyber attack lab demos to get a live look at how popular attacks are executed, explore indicators of compromise, and learn how to detect and respond with Varonis.

The team runs **multiple live sessions per week**, webinar-style, on Zoom. After the attack simulation, you’re invited to stick around for Q&A.

Pick a time: [varonis.com/cyber-workshop](https://varonis.com/cyber-workshop)



```
Warning: '/dev/shm' does not exist or is not a directory.
POSIX shared memory objects require the existence of this directory.
Create the directory '/dev/shm' and set the permissions to 01777.
For instance on the command line: mkdir -m 01777 /dev/shm
ls: can't default font encoding: error

Administrator: Windows PowerShell

FileCrawler
[*] Running as: vrnslab\backupservice
[*] searching for: pci salary gdpr important confidential inside: \\hub-filer\share\finance
[*] Found files:
FileLocation                                     FoundWords
-----
\\hub-filer\share\finance\Customers\2020_Plan.docx (gdpr, confidential)
\\hub-filer\share\finance\Customers\CustomersFullList.docx (confidential)
\\hub-filer\share\finance\Customers\Important.docx (confidential)
\\hub-filer\share\finance\Customers\Marketing_Plan.docx (confidential)
\\hub-filer\share\finance\Customers\Marketing_Plan2.docx (confidential)
\\hub-filer\share\finance\Customers\report.docx (confidential)
\\hub-filer\share\finance\2018-01.docx (confidential)
\\hub-filer\share\finance\2018-02.docx (confidential)
\\hub-filer\share\finance\2018-03.docx (confidential)
\\hub-filer\share\finance\2018-04.docx (confidential)
\\hub-filer\share\finance\finance-report.docx (gdpr, confidential)

[*] Press enter to download the files to local directory

Directory: c:\Users\han.solo\Desktop
Mode                LastWriteTime         Length Name
----                -
d-----           2/12/2019   7:22 PM          tempFiles

[*] Finished
```