ARE VULNERABILITY SCANS MAKING YOUR NETWORKS MORE VULNERABLE?

Does continuous vulnerability scanning actually create more risk?

GALACTIC ADVISORS

GALACTIC ADVISORS

WHO IS BRUCE MCCULLY

…and what the heck does he know about growing **M S P s**?

GALACTIC ADVISORS

GREW:

$8.5M

MSP

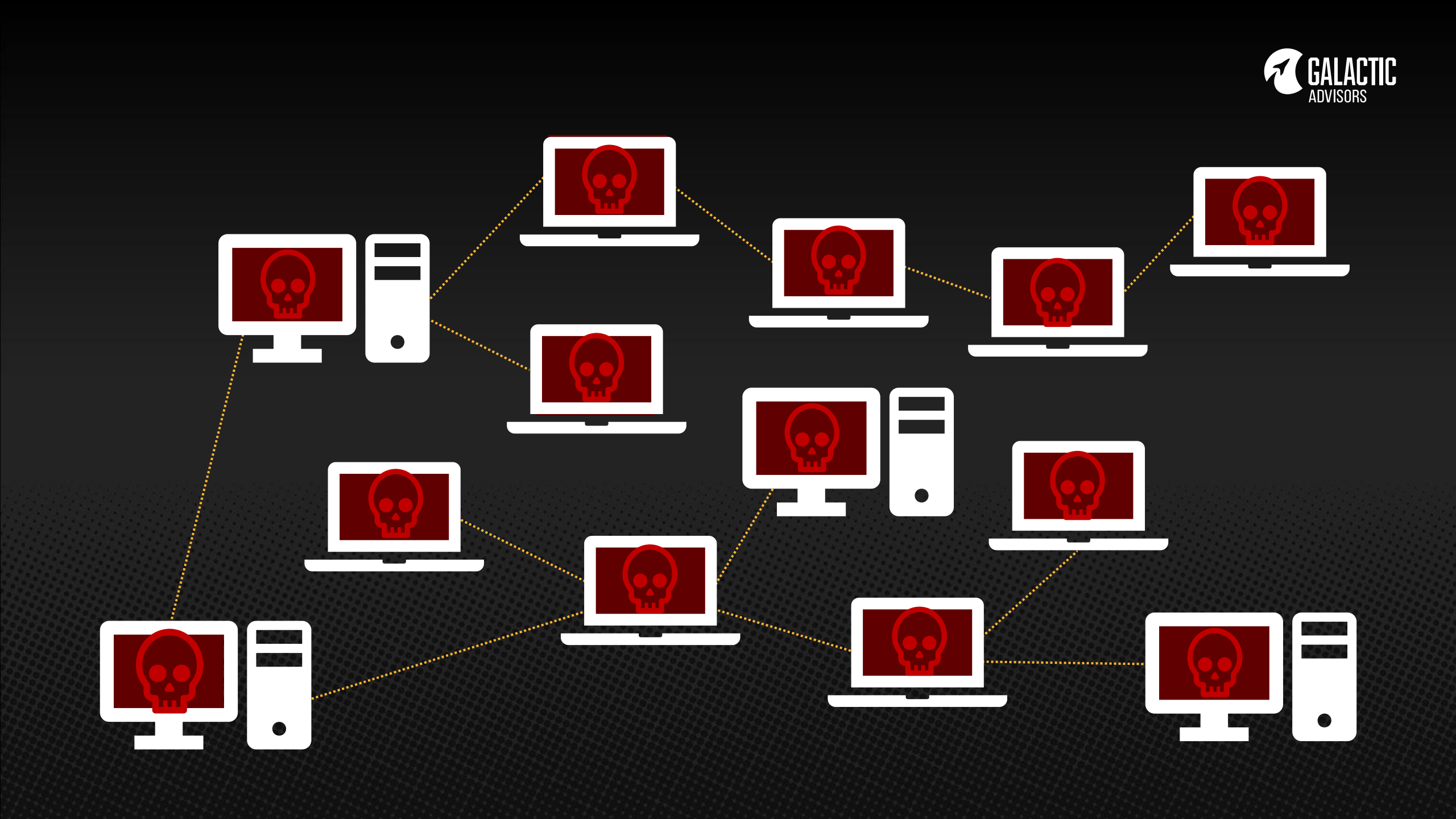
SOLD:

$1.3M

IN MRR IN 2019


NEW AT 6
MEDICAL RECORDS HELD HOSTAGE

GALACTIC
ADVISORS


GALACTIC
ADVISORS

GALACTIC ADVISORS

OUR COMMUNITY IS UNDER ATTACK

GALACTIC ADVISORS

1 MILLION

PEOPLE

GALACTIC ADVISORS

HOW WOULD YOU GET INTO A NETWORK?

GALACTIC ADVISORS

LINK

GALACTIC ADVISORS

80%

of the time hackers get administrator rights

GALACTIC ADVISORS

ARE THEY LANDING WITH ADMINISTRATOR RIGHTS?

GALACTIC
ADVISORS

NOPE.

GALACTIC ADVISORS

GROUP POLICY PREFERENCE XML-FILES

SERVICE ACCOUNT BACKDOORS

LOST AUTO LAUNCH

HOW DO YOU GET ADMIN RIGHTS?

FILE PERMISSION ERRORS

UNATTENDED INSTALLS

LEGACY PROTOCOL ACCESSIBILITY

GALACTIC ADVISORS

ARE THESE VULNERABILITIES?

GALACTIC ADVISORS

NOT TRADITIONAL

PERMISSIONS

CONFIGURATIONS

GALACTIC ADVISORS

50%

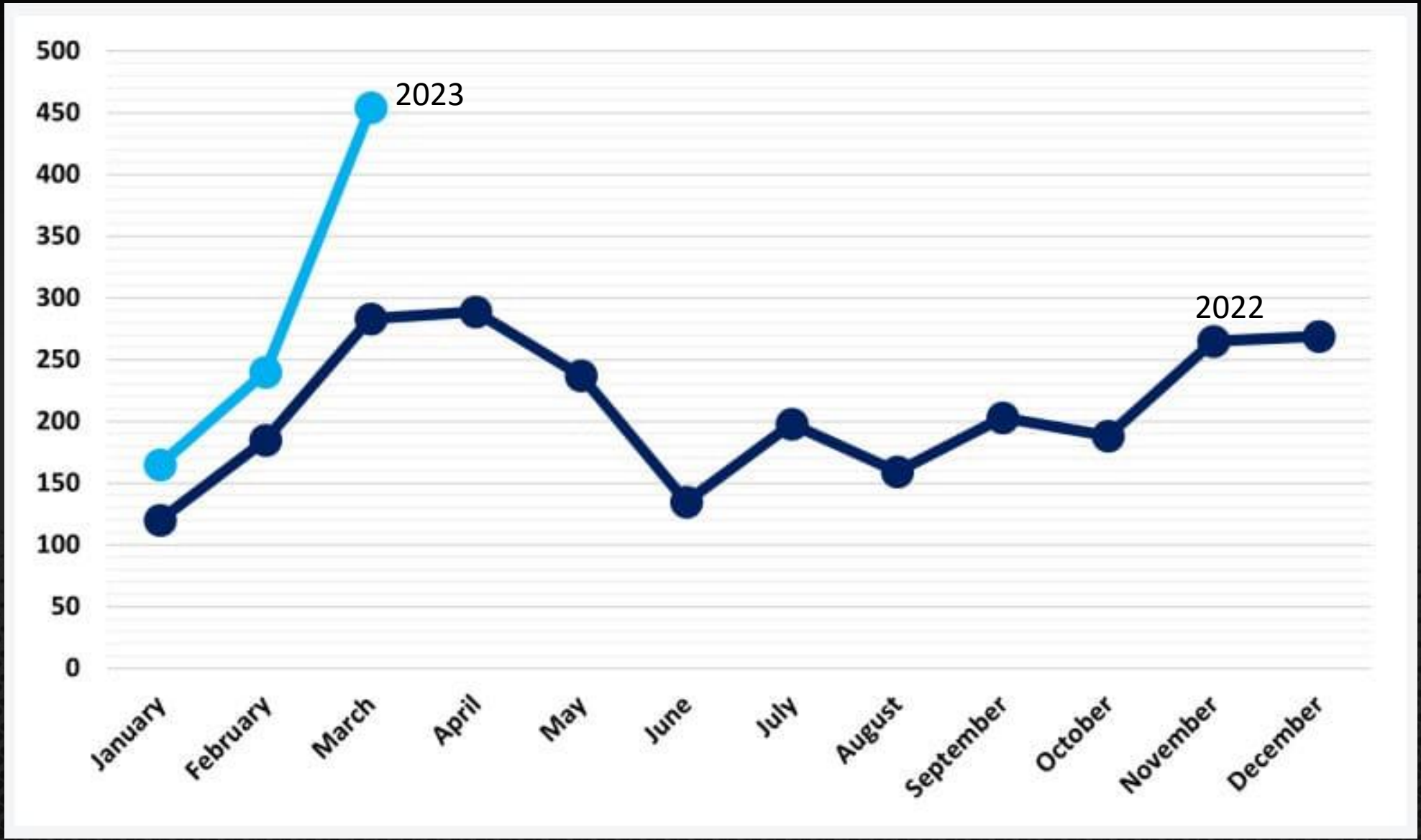
of organizations had a ransomware incident in 2022

GALACTIC ADVISORS

2023 NOT LOOKING BETTER

GALACTIC ADVISORS

FIRST QUARTER NUMBERS SHOW RANSOMWARE IS ON THE RISE


500
450
400
350
300
250
200
150
100
50
0
2023
2022
January
February
March
April
May
June
July
August
September
October
November
December

GALACTIC ADVISORS

HOW DOES THIS HAPPEN?

GALACTIC ADVISORS

HUMAN ERROR

GALACTIC ADVISORS

1000%

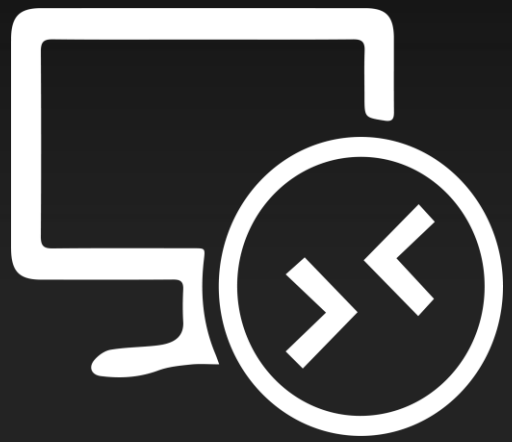
Of Ransomware Events Are Caused By Human Error

GALACTIC ADVISORS

HOW DOES HUMAN ERROR HAPPEN?

WHAT CAN YOU DO ABOUT IT?

GALACTIC ADVISORS



RDP

Rip-off

SQL Server Spanking

MFA

Misfiring

GALACTIC ADVISORS

A CALL FROM YOUR OUTSOURCED SECURITY OPERATIONS CENTER AT 12:31 AM SATURDAY MORNING

GALACTIC ADVISORS

SEEING A PROCESS THAT APPEARS TO BE ENCRYPTING FILES

GALACTIC ADVISORS

RUNNING ON MULTIPLE DEVICES

GALACTIC
ADVISORS

THE SOC HAS ALREADY KILLED IT

GALACTIC ADVISORS

NOTICING PASSWORD ATTEMPTS FROM WITHIN THE NETWORK

GALACTIC ADVISORS

LOOKS LIKE SOMEONE IS EXFILTRATING YOUR NT.DIT FILE

GALACTIC ADVISORS

13 DAYS LATER

REVIEWING FORENSIC RESULTS

GALACTIC ADVISORS

THE ATTACKERS ACCESSED THE SYSTEM USING AN OPEN RDP PORT

GALACTIC ADVISORS

REMEMBER WHEN WE USED TO SAY:

SHUT THE FRONT DOOR

GALACTIC ADVISORS

AN ENGINEER OPENED RDP DURING AN AZURE SERVER MIGRATION

GALACTIC ADVISORS

THIS WAS BAD

WHY DID IT HAPPEN?

GALACTIC ADVISORS

DID THIS ENGINEER KNOW IT WAS BAD?

GALACTIC ADVISORS

YES

HE PLANNED ON CLOSING IT UP LATER

GALACTIC ADVISORS

TOO MANY INTERRUPTIONS TO CLOSE IT UP LATER

GALACTIC ADVISORS

YOU ARE MAKING DINNER

BOILING SPAGHETTI

YOUR MOM IS RUSHED TO THE EMERGENCY ROOM

YOU RUN OUT THE DOOR TO HELP

WHAT HAPPENS TO THE BOILING SPAGHETTI?

GALACTIC ADVISORS

CONTROLS KEEP THIS FROM HAPPENING

APPLICATION WHITELISTING
(NOT SET UP YET)

GALACTIC ADVISORS

CONTINUOUS VULNERABILITY SCANS

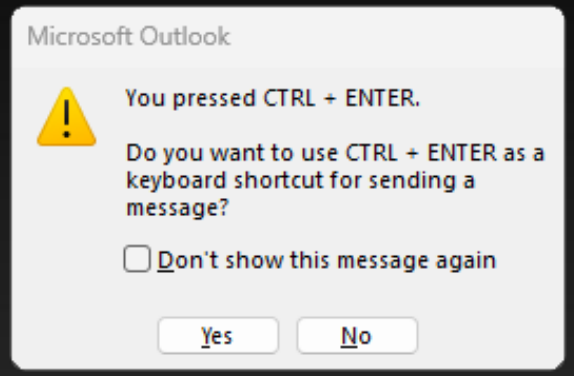
GALACTIC ADVISORS

ACKNOWLEDGED THE ALERT

GALACTIC ADVISORS

ALERTS!

GALACTIC ADVISORS



FAVORITE ALERT

GALACTIC ADVISORS

THIS MESSAGE POPS UP TO MAKE SURE YOU ARE SURE YOU WANT TO SEND

GALACTIC ADVISORS

CTRL + ENTER
ENTER


Annoying Confirmation
Are you sure?
Yes
No
Annoying Confirmation
Are you sure?
Yes
No
Annoying Confirmation
Are you sure?
Yes
No
Annoying Confirmation
Are you sure?
Yes
No
Annoying Confirmation
Are you sure?
Yes
No
Annoying Confirmation
Are you sure?
Yes
No
Annoying Confirmation
Are you sure?
Yes
No

GALACTIC ADVISORS

YES, I AM SURE

GALACTIC ADVISORS

NUISANCE ALERTS

REDUCE RESPONSE

GALACTIC ADVISORS

CREATE A RESPONSE PLAN FOR EACH TYPE OF ALERT

GALACTIC ADVISORS

BUILD OUT TOURS OF DUTY

GALACTIC ADVISORS

ONE PERSON RESPONSIBLE FOR APPLICATION APPROVAL

GALACTIC ADVISORS

WORK THAT TOUR OF DUTY FOR 90 DAYS

GALACTIC ADVISORS

ROTATE TO THE NEXT PERSON

GALACTIC ADVISORS

THEY OWN IT
FOR 90 DAYS

GALACTIC ADVISORS

WHY 90 DAYS?

CREATE COMPETENCY AFTER 2 WEEKS

GALACTIC ADVISORS

PART OF THE CAREER PATH INSIDE YOUR COMPANY

GALACTIC ADVISORS

CREATES REDUNDANCY AND ACCOUNTABILITY

GALACTIC ADVISORS

NEW PERSON IN A ROLE EVERY 90 DAYS

REQUIRES GREAT DOCUMENTATION

GALACTIC ADVISORS

PROTECTS YOU FROM TURNOVER

CREATE A SYSTEM

- **Batch work**
- **Get stuck?**
- **Get help** at 15 minutes
- **Ask for help**
- Update the **just-in-time documentation**

GALACTIC ADVISORS

GALACTIC ADVISORS

COMPETENCE ACHIEVED AT WEEK TWO

GALACTIC ADVISORS

HIGH PRODUCTION FOR 10 WEEKS

ROTATE TO THE NEXT DUTY

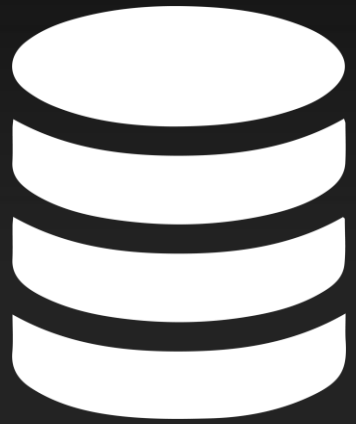
- Backups
- Patching
- Projects
- Alerts
- Evening

GALACTIC ADVISORS

GALACTIC ADVISORS

RDP

Rip-off



SQL Server Spanking

MFA

Misfiring

GALACTIC ADVISORS

HAVE YOU EVER HAD A CLIENT TELL YOU

NO?

GALACTIC ADVISORS

REFUSE TO DO THE RIGHT THING?

GALACTIC ADVISORS

“I NEED RDP OPEN IN ORDER TO WORK REMOTELY”

GALACTIC ADVISORS

WHAT ABOUT A VENDOR?

GALACTIC ADVISORS

KNOW IT ALL

BEEN DOING THIS FOR YEARS

NEVER HAD A PROBLEM

VENDOR?

GALACTIC ADVISORS

MICROSOFT SQL SERVER
PUBLICLY ASSESSABLE

VENDOR: WE NEED IT OPEN

GALACTIC ADVISORS

GALACTIC ADVISORS

MSP: NOT A GOOD IDEA

GALACTIC
ADVISORS

STOPPED THERE.

GALACTIC ADVISORS

HOW DOES THIS GO DOWN?

GALACTIC ADVISORS

WHAT HAPPENS WHEN AN ATTACKER GETS SQL ACCESS?

GALACTIC ADVISORS

THINK ABOUT THAT FOR A MINUTE

GALACTIC ADVISORS

DATA EXFILTRATION

GALACTIC ADVISORS

WHAT ELSE?

```
EXEC xp_cmdshell 'dir *.exe'; GO
```

GALACTIC ADVISORS

DATA EXFILTRATION

LATERAL SPREAD

RANSOMWARE

GALACTIC ADVISORS

CLIENT BLAMED THE MSP

GALACTIC ADVISORS

FIRE THE CLIENT?

GALACTIC ADVISORS

CHANGE THE CONVERSATION

GALACTIC ADVISORS

DO PEOPLE INVEST IN SECURITY TO DO THE RIGHT THING?

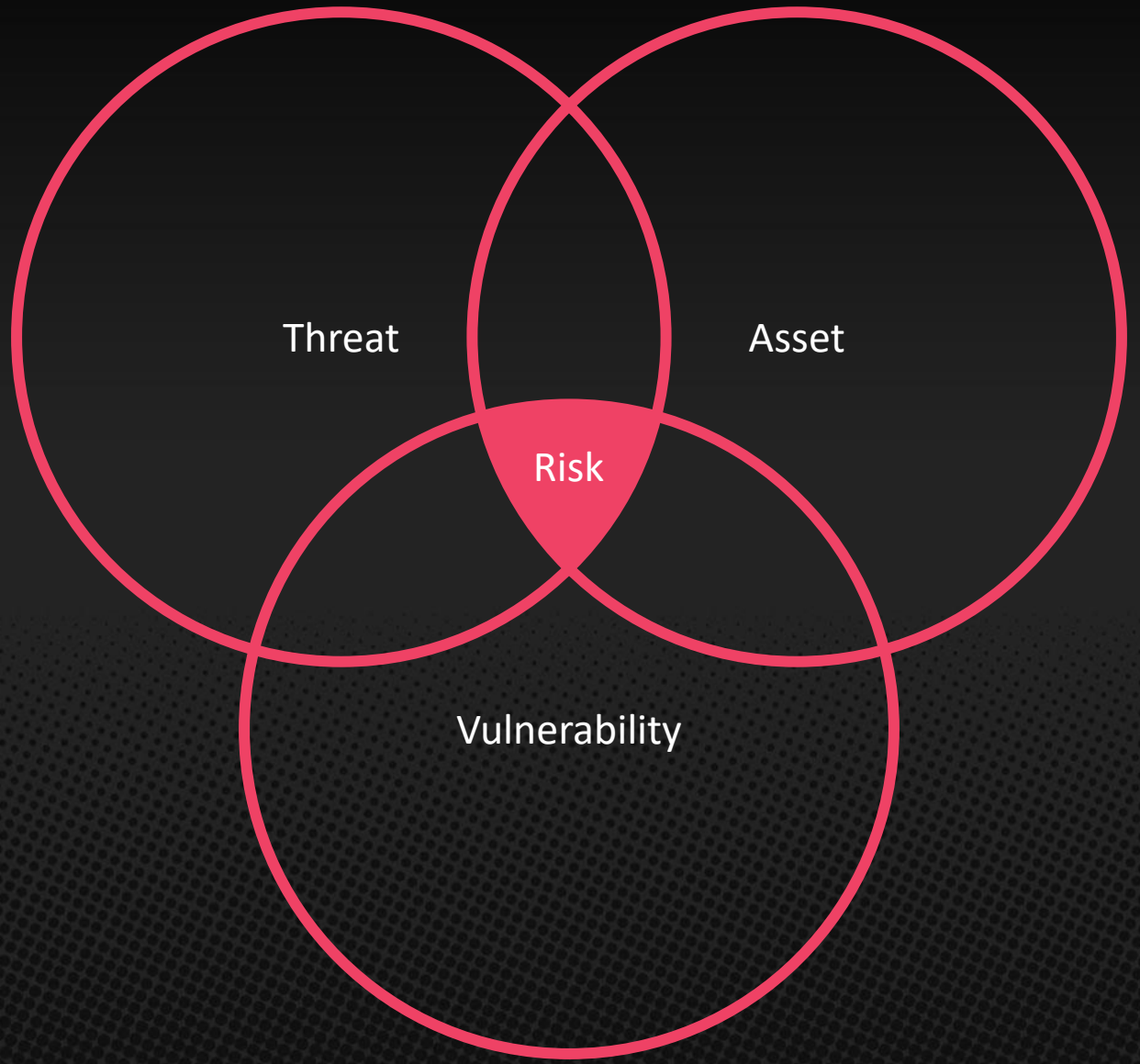
GALACTIC ADVISORS

ONE REASON: RISK

GALACTIC ADVISORS

WHAT IS RISK?

GALACTIC ADVISORS



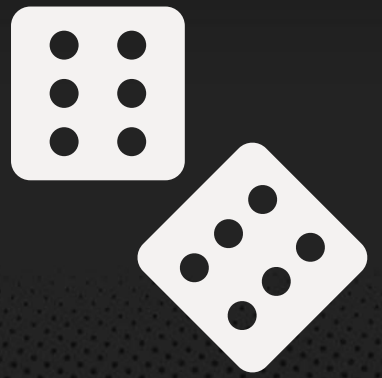
GALACTIC ADVISORS

HOW IS IT MEASURED?

GALACTIC ADVISORS

HOW IS RISK MEASURED?

X



Impact

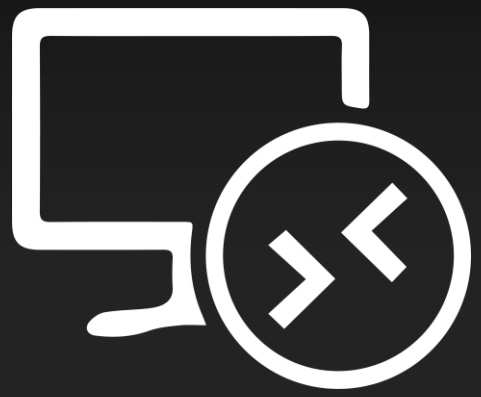
Likelihood

GALACTIC ADVISORS

HAVE YOUR CLIENT SIGN A "RISK ACCEPTANCE FORM"

bruce.mccully@galacticadvisors.com

GALACTIC ADVISORS



RDP

Rip-off

SQL Server Spanking

MFA

Misfiring

GALACTIC
ADVISORS

IMAGINE...

GALACTIC ADVISORS

YOU GET A HUGE OPPORTUNITY

SEND A LINK

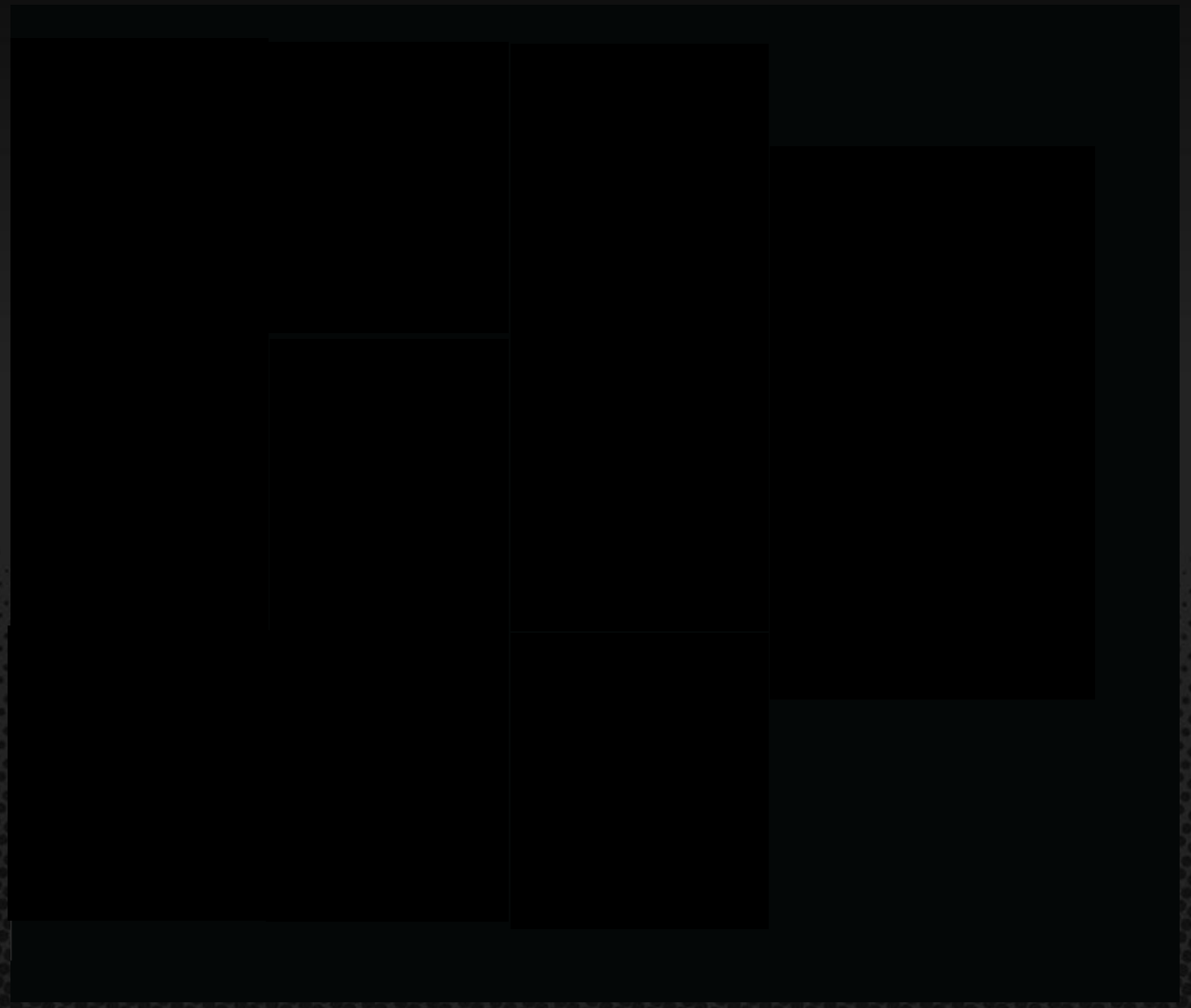
THEY CLICK THE LINK

WE ANALYZE THEIR SECURITY

YOU GET A REPORT IN UNDER TWO DAYS

GALACTIC ADVISORS

LET THE REPORT DO THE WORK



GALACTIC ADVISORS

SCORE CARD

METHODS

ACCOUNTS

M365

GALACTIC ADVISORS

GLOBAL ADMIN ACCOUNTS
HAVE ACCESS TO

ALL YOUR EXISTING DATA

GALACTIC ADVISORS

“I’ve seen enough. How much does it cost to work with you?”

GALACTIC
ADVISORS

YOU LEAVE

GALACTIC
ADVISORS

GALACTIC
ADVISORS

GALACTIC ADVISORS

“We fired our existing MSP. When can you start?”

GALACTIC ADVISORS

WHAT THE HECK HAPPENED HERE?

GALACTIC
ADVISORS

$24,000 PER MONTH DEAL

GALACTIC ADVISORS

CYBER INSURANCE RENEWAL

SELF ASSESSMENT QUESTIONNAIRE

GALACTIC ADVISORS

“Do you use MFA to protect all local and remote access to privileged user accounts?”

YES.

GALACTIC ADVISORS

“Does your organization enforce multifactor authentication (MFA) in order to access all cloud-based resources?”

YES.

GALACTIC ADVISORS

“Does your organization enforce multifactor authentication (MFA) in order to access or send email?”

YES.

GALACTIC ADVISORS

ALL THE ACCOUNT HAD MFA AS EXPECTED...

GALACTIC ADVISORS

EXCEPT THE ONES THE MSP USED TO MANAGE THEIR M365 TENANT

GLOBAL ADMIN ACCOUNTS HAVE ACCESS TO

ALL YOUR EXISTING DATA

GALACTIC
ADVISORS

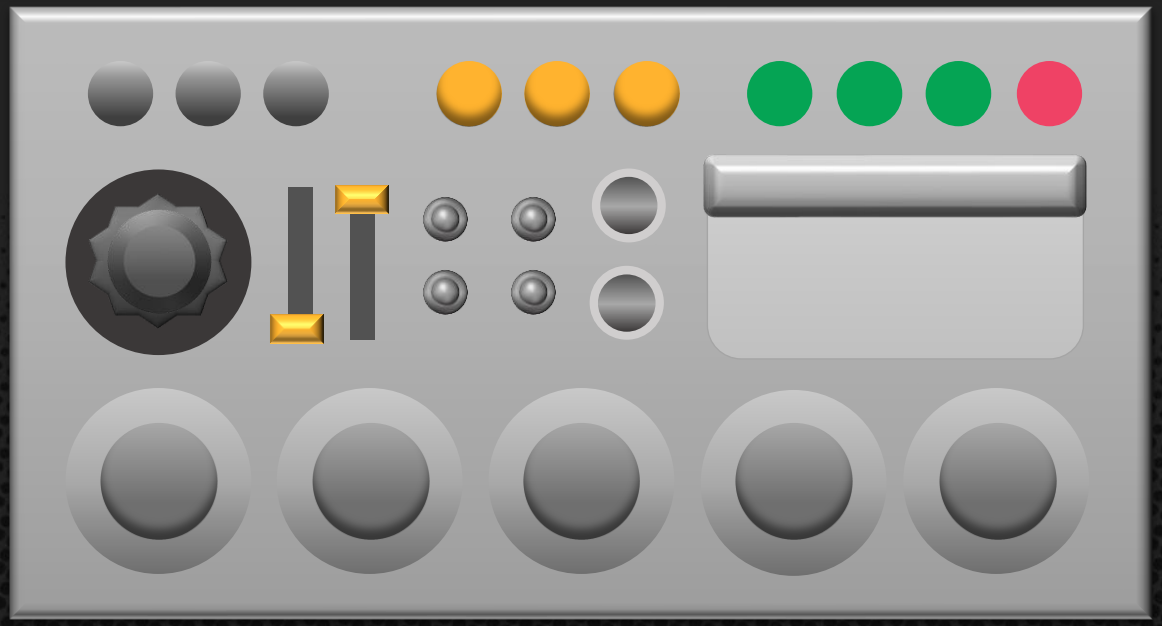
GALACTIC
ADVISORS

GALACTIC ADVISORS

HOW DID YOU GET HERE?

GALACTIC ADVISORS

MOVE THE CONVERSATION AWAY FROM INFORMATION TECHNOLOGY



GALACTIC ADVISORS

WHAT IF YOU WERE THE INCUMBENT MSP?

GALACTIC ADVISORS

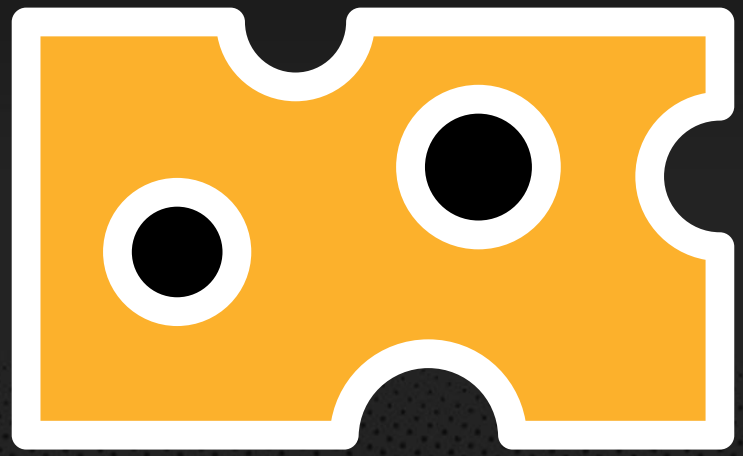
LOSING A 24,000 PER MONTH CLIENT?

GALACTIC ADVISORS

WHY DID THEY DO IT?

HABITUATION

GALACTIC
ADVISORS



GALACTIC
ADVISORS

GALACTIC
ADVISORS

GALACTIC ADVISORS

REDUCTION IN RESPONSE

GRADUAL DESENSITIZATION

COMPLACENCY

GALACTIC
ADVISORS

GALACTIC ADVISORS

WHAT CAN YOU DO?

GALACTIC ADVISORS

DO YOU HAVE CLIENTS THAT DO NOT WANT TO INVEST UNTIL THEY GET BURNT?

GALACTIC ADVISORS

CREATE AN EXPERIENCE

SEND A LINK

THEY CLICK THE LINK

WE ANALYZE THEIR SECURITY

YOU GET A REPORT IN UNDER TWO DAYS

GALACTIC ADVISORS

DEMONSTRATE THEIR RISKS

IMPACT ON YOUR ORGANIZATION:

GALACTIC ADVISORS

- **High Impact:** Will result in a **severe or catastrophic adverse effect of the system**. May cause damage to the reputation of system management, and/or notable loss of confidence in the system's recourses and services. It will require expenditure of significant resources to repair.

- **Medium Impact:** Will result in **a serious adverse effect on the system**. May cause tangible harm, perhaps only noted by a few individuals or agencies. May cause political embarrassment. Will require some expenditure of recourses to repair.

- **Low Impact:** Will have **some limited adverse effect on the system**. It will require minimal effort to repair or reconfigure the system.

LIKELIHOOD A BREACH EVENT WILL OCCUR:

- **High Likelihood:** Adversary is **highly likely to initiate the threat event**. Error, accident, or act of nature is highly likely to occur, or occurs between 10-100 times a year.

- **Moderate Likelihood:** Adversary is **somewhat likely to initiate the threat event**. Error, accident, or act of nature is somewhat likely to occur, or occurs between 1-10 times a year.

- **Low Likelihood:** Adversary is **unlikely to initiate the threat event**. Error, accident, or act of nature is unlikely to occur; or occur less than once a year, but more than once every 10 years.

CHART THE RISK:

GALACTIC ADVISORS

DATA!

GALACTIC ADVISORS

DATA IS NOT EMOTIONAL

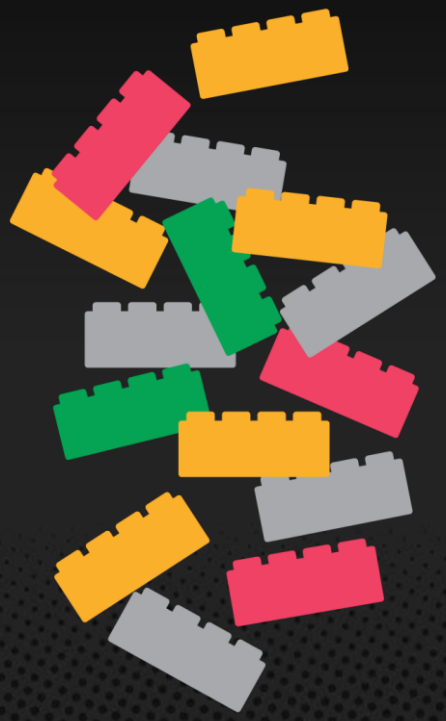
GALACTIC
ADVISORS

HOW DO WE MAKE IT EMOTIONAL?

GALACTIC
ADVISORS

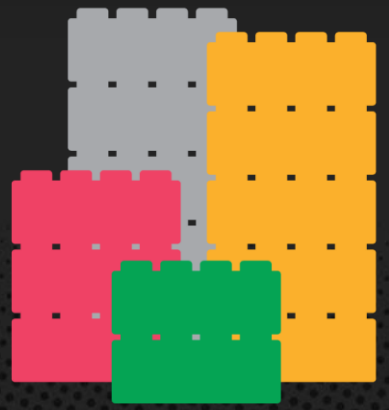
CONTEXT

GALACTIC ADVISORS

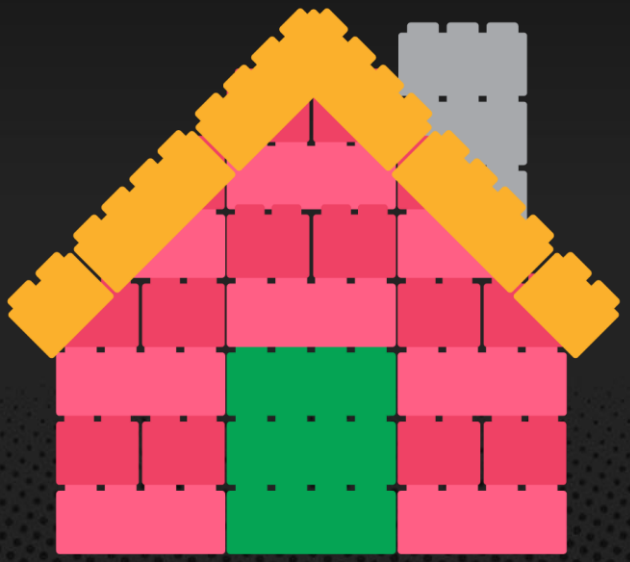


RAW DATA

SORTED DATA



REPORTED DATA



DATA EXPLAINED WITH STORY

PREPARATION

- Should have **at least 3 stories**
- How do you **create a good story?**

Transition
Who
Current state
What happened
Business outcome
Relate to finding

GALACTIC ADVISORS

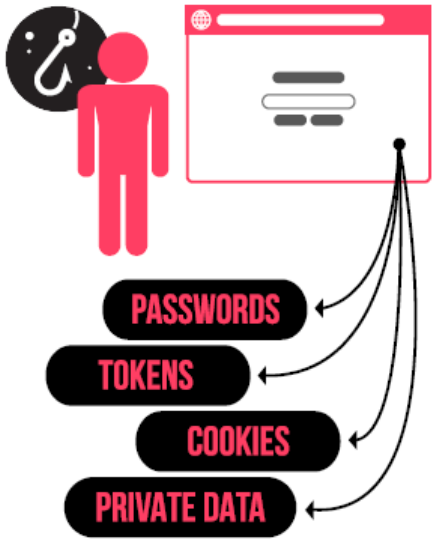
ACCOUNTS HIGH RISK ISSUES

PASSWORDS CRACKED

Passwords were cracked on computers within the environment. Hackers use tools like memory abuse, abusing user privilege, and ripping to obtain access to your passwords when you are phished. When this happens, these passwords are used to break into systems inside and even outside of the victimâ€™s environment. Below is a small sample of the passwords that were cracked. For a complete listing of passwords our team cracked by abusing user privilege refer to the detail report.

CODE	COMPUTER NAME	BROWSER	LOGIN NAME	PASSWORD	URL
8740	G*****9	Chrome	M*****m	1234****	https://l*****ogin

Remediation: Work with users and train them to never store their passwords inside browsers or other memory on the device. Review the passwords that were uncovered during this evaluation, consider additional training around password complexity. Implement password manager with multifactor authentication capabilities to make it difficult for the attacker to get to the memory storing the password set.



When a user is phished and clicks a link, there is one thing running EVERY SINGLE TIME: their web browser. Hackers quickly abuse the user's privileges, identify the cypher for the browser, and then use that cypher to access all passwords, tokens, cookies and private data that web browser has access to. The attacker takes this data set and uses it to access additional accounts to find out more about their victim or to identify a list of people who trust the victim. They use this list to then infect other unsuspecting organizations.

GALACTIC ADVISORS

“This reminds me…”

of a partner at an accounting firm
who thought they were safe
until hackers submitted 180 fraudulent tax refunds,
causing the IRS to suspend their ability to e-file,
and all they needed to get was a password.

GALACTIC ADVISORS

BACKUPS | ACCOUNTS | M365 | PATCHES | ANTIVIRUS | FIREWALLS | EDUCATION | ENCRYPTION | SURVEILLANCE

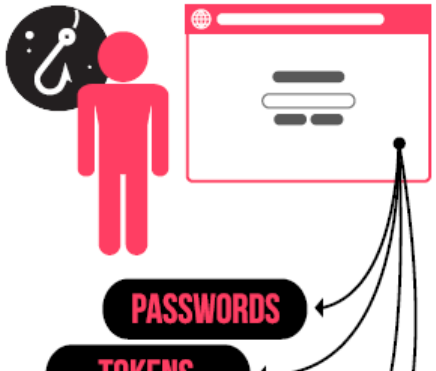
ACCOUNTS HIGH RISK ISSUES

Page 1/2

PASSWORDS CRACKED

Passwords were cracked on computers within the environment. Hackers use tools like memory abuse, abusing user privilege, and ripping to obtain access to your passwords when you are phished. When this happens, these passwords are used to break into systems inside and even outside of the victimâ€™s environment. Below is a small sample of the passwords that were cracked. For a complete listing of passwords our team cracked by abusing user privilege refer to the detail report.

CODE	COMPUTER NAME	BROWSER	LOGIN NAME	PASSWORD	URL
8740	G*****9	Chrome	M*****m	1234****	https://l*****ogin



GALACTIC ADVISORS

HOW ELSE?

GALACTIC ADVISORS

CVE-2023-23397

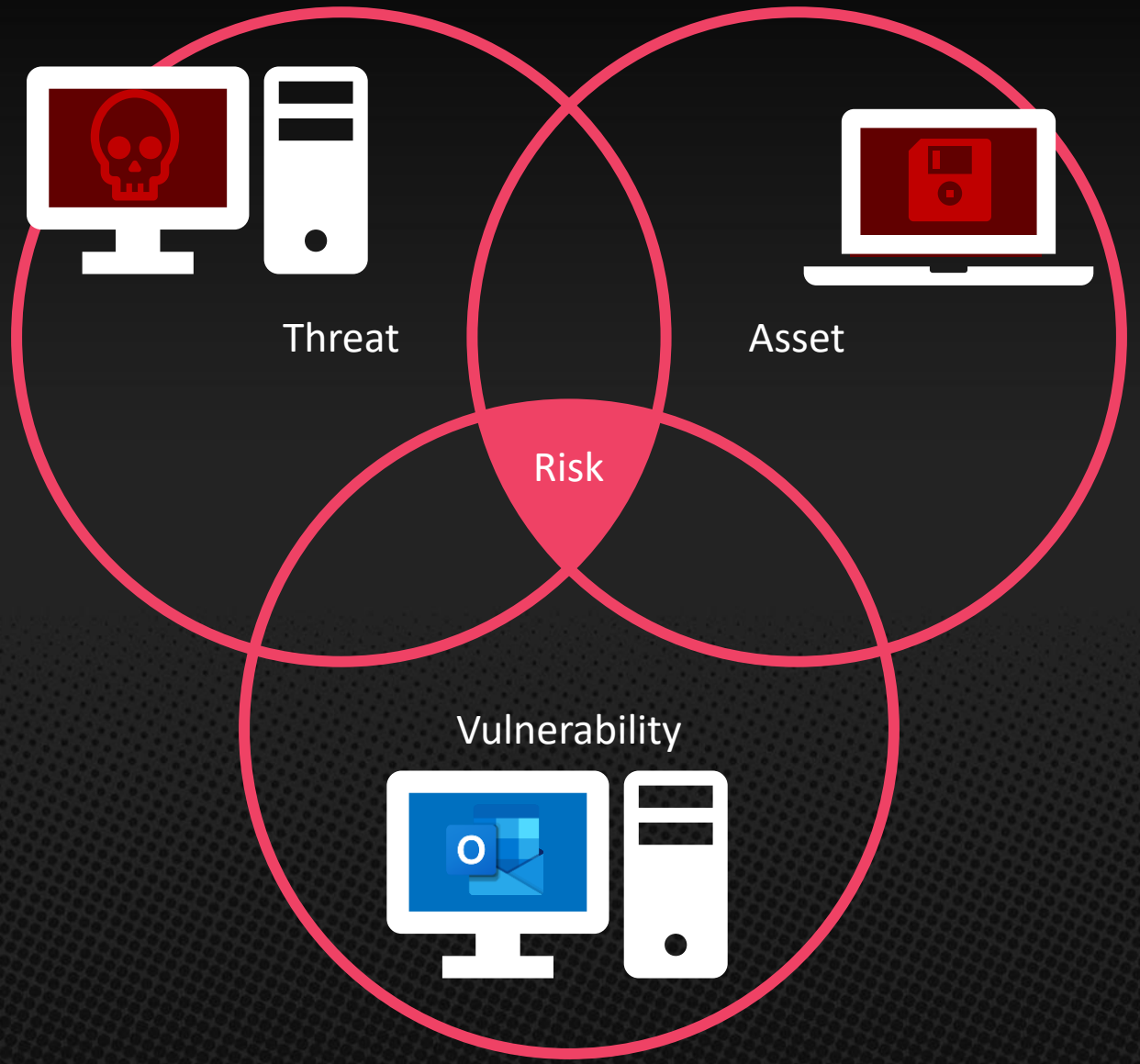
Microsoft Office Outlook Privilege Escalation Vulnerability

CVSS 9.8 CRITICAL

IMAGINE SOMEONE IN YOUR COMPANY

- Received an email
- They opened the email
- Using this **Microsoft Outlook** vulnerability
- **Hackers** accessed their computer
- The attackers took all **your data**

GALACTIC ADVISORS



GALACTIC ADVISORS

HOW DO YOU DO THIS?

GALACTIC ADVISORS

OFFER A PENETRATION TEST

Third-party analysis

3 available **THIS MONTH**

SCARCITY

URGENCY

GALACTIC ADVISORS

Google

ON AVERAGE, A HIGH QUALITY, PROFESSIONAL PEN TEST CAN COST

$10,000-$30,000

VALUE

GALACTIC ADVISORS

ITS DIFFICULT TO CREATE:

SCARCITY

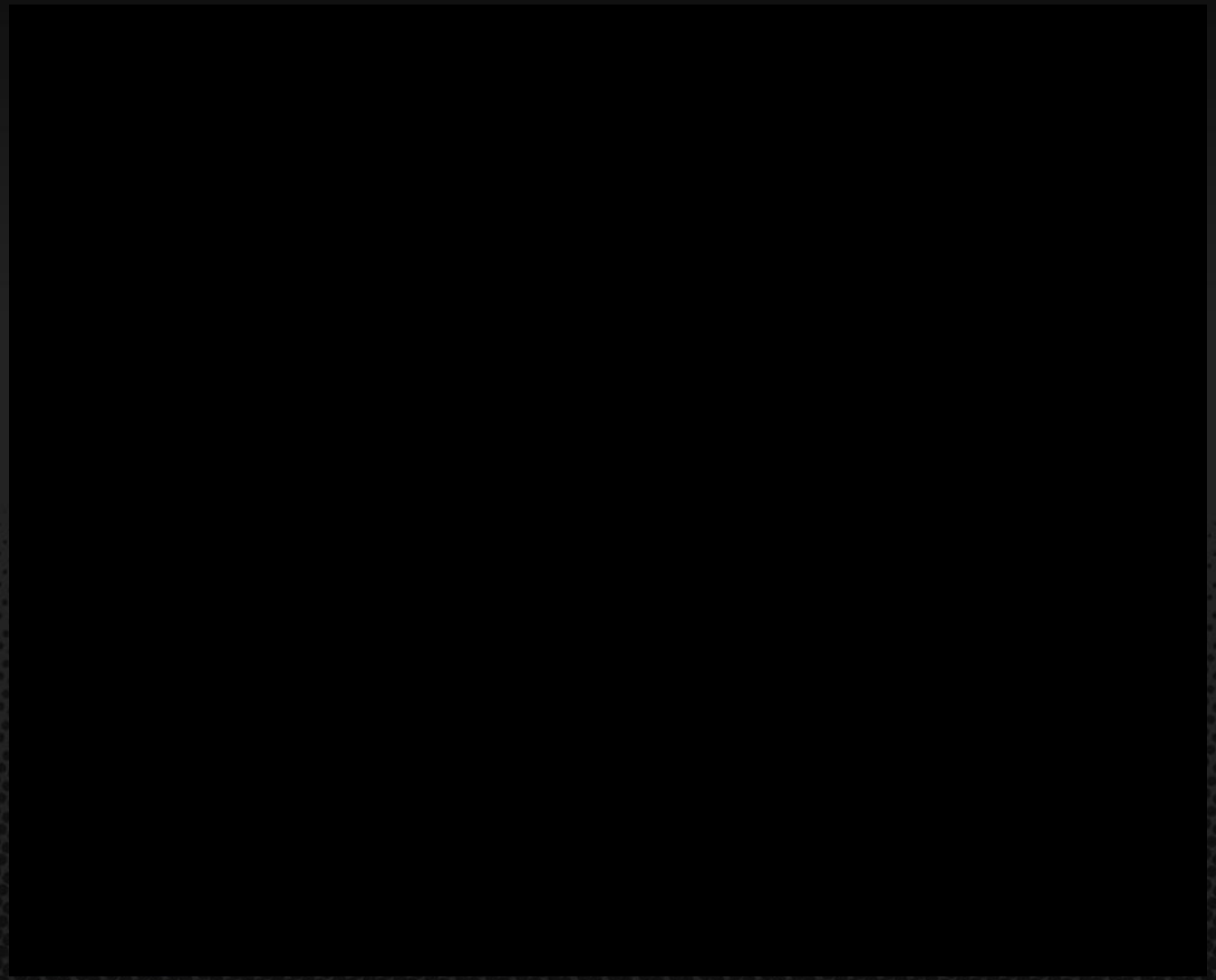
URGENCY

VALUE

ANALYZING YOUR OWN WORK

NO ONE CAN PROOFREAD THEIR OWN WORK

GALACTIC ADVISORS



GALACTIC ADVISORS

BRINGING A THIRD PARTY AS A RESOURCE

KEEPS YOU IN THE TRUSTED ADVISOR SEAT

GALACTIC ADVISORS

> This helped seal the deal on a $9,000 security project.

Jason Mance, CEO, Omega Tecks

GALACTIC ADVISORS

$9,000 Project Work

AND

298% MARGIN

Charging $897 Per Month

His Cost $220 Per Month

MISSION:

Protect your most profitable clients with recurring third-party security assessments and pen testing

Update your sales process to
hit these three critical areas

GALACTIC
ADVISORS

GALACTIC ADVISORS

BECOME IRREPLACEABLE

GALACTIC ADVISORS

vCSO

RECURRING THIRD-PARTY ASSESSMENTS

COMPLIANCE-AS-A SERVICE

BASIC IT

ADVANCED SECURITY

GALACTIC ADVISORS

CHIEF SECURITY OFFICER

YOU'LL HAVE T

- Build a vCSO Offerin
- vCSO Client Profiler
- Vendor Self-Assessme Questionnaire
- Risk Assessment Questionnaire
- Sales Process for vCSO
- Incident Response Proce
- Ransomware Tabletop
- Security Incident Log
- Critical Asset Evaluation Fo m
- Quarterly Privilege Review

NEW!

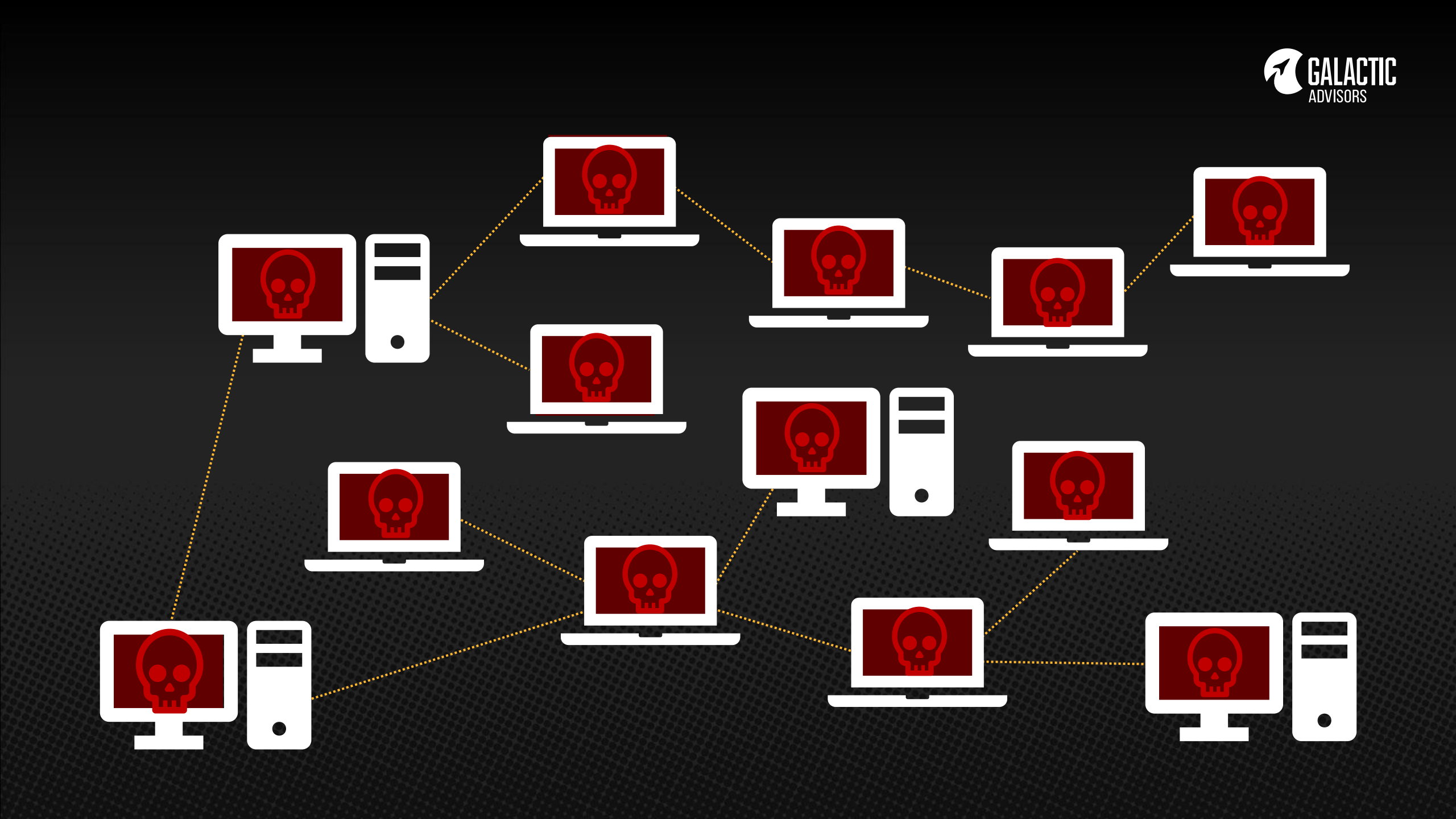
- Policy
- Security Prese

- Builder
- Defined
- ined Deliverables
- arketing Workflow and orksheet
- arketing Materials for vCSO isk Assessment, Campaign, mail/Phone Scripts
- Penetration testing
- Threat Intelligence

GALACTIC ADVISORS

GALACTIC ADVISORS

HOW DO YOU GET STARTED?


GALACTIC
ADVISORS

GALACTICSCAN

WOULD YOUR SECURITY SOLUTION DETECT OR STOP AN ATTACK?

GALACTICSCAN.COM/STACK

GALACTICSCAN

Here's what you can do:

GET A FREE ASSESSMENT OF YOUR CYBERSECURITY STACK

GALACTICSCAN.COM/STACK

GALACTICSCAN

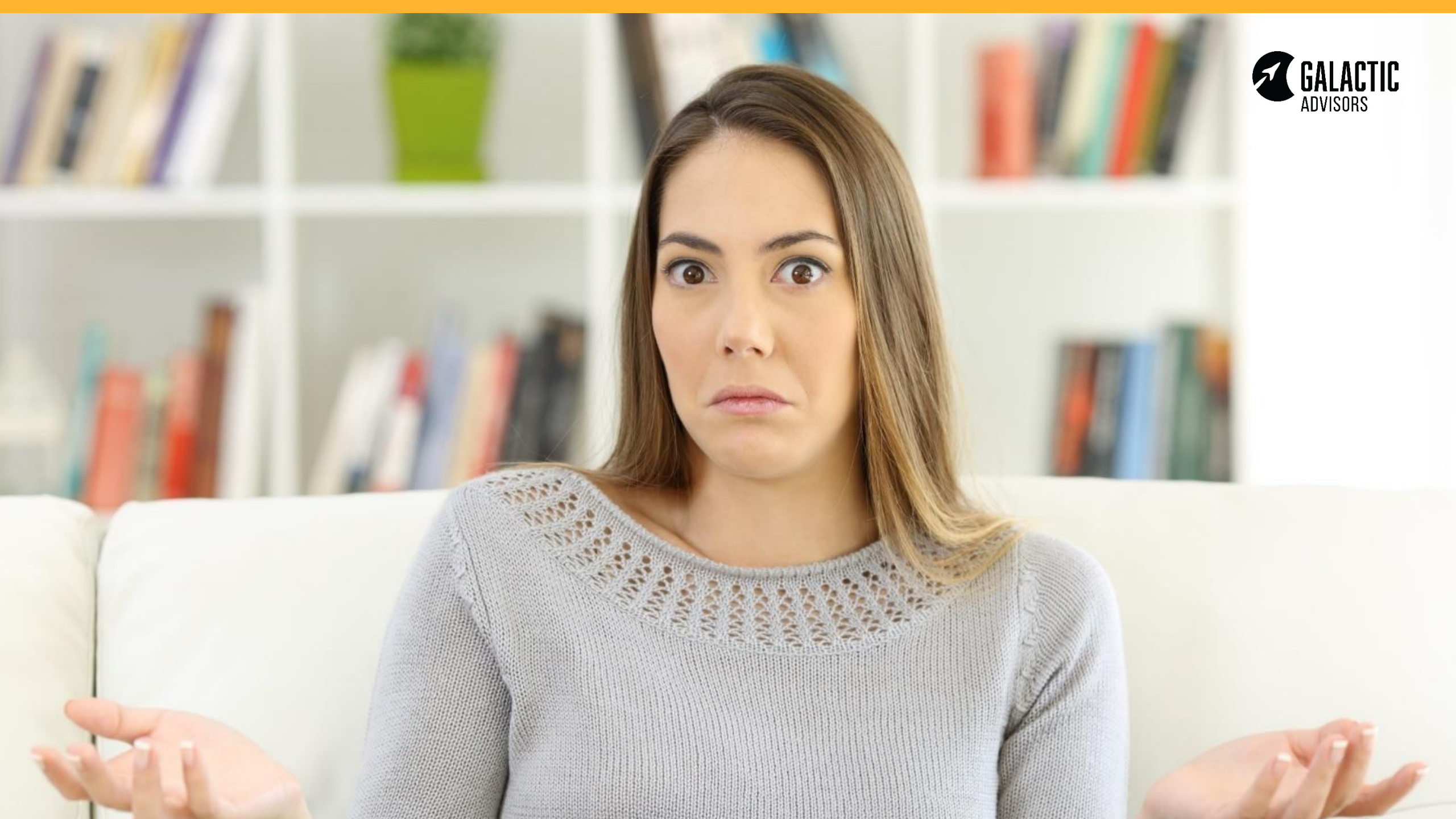
We will:

Analyze your security

Show how your tools respond

Give you steps you can take to protect yourself and your clients

GALACTICSCAN.COM/STACK


GALACTIC
ADVISORS

GALACTIC ADVISORS

1 MILLION

PEOPLE

GALACTICSCAN.COM/STACK

GALACTICSCAN

Here's what you can do:

GET A FREE ASSESSMENT OF YOUR CYBERSECURITY STACK

GALACTICSCAN.COM/STACK


GALACTIC
ADVISORS