Accelerating Business and Data Recovery After a Ransomware Attack

Surya Mukka
Cybersecurity Strategist and Practice Lead (Central US and APJ)

Oregon Cyber Resilience Summit

Dell Cyber Resiliency Video

DELL Technologies

October 13th , 2022

A Deeper Dive

It’s Saturday evening and you are at home with the family when you get the call that ransomware has taken down your network…what do you do next?

© Copyright 2020 Dell Inc.


CHEATER v3.5
CHEATER
The important files on your computer have been encrypted with military grade AES-256 bit encryption.
Your documents, videos, images and other forms of data are now inaccessible, and cannot be unlocked without the decryption key. This key is currently being stored on a remote server.
To acquire this key, you have to transfer a Bitcoin Fee (300$ in Bitcoin) to the specified wallet address that you find on the bottom - Or you can contact us by email and I will give you a specific wallet address. Email: alphateam56@protonmail.com
After you made the payment, I will give you the key to restore your files
If you don't contact us/make the payment before the
TIME REMAINING
23:55:35
bitcoin
ACCEPTED HERE
WALLET ADDRESS:
bc1qkgdzagcs7l49hjfaq2k2ue2gff9r4fp9rgd0ql
BITCOIN FEE:
0.0051
View Encrypted Files
Enter Decryption Key
PCrisk.com

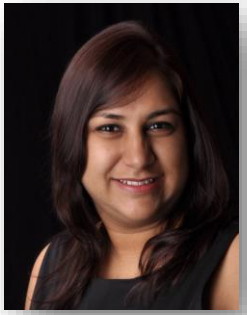
Surya Mukka

Cybersecurity Strategist and Practice Lead (US Central & APJ)

Focus | Proactive Cybersecurity, Incident Recovery and Response, Enterprise Architecture, Application Integration

Awards | Dell Services President's Award for Incident Recovery, Dell Services President's Award for Workforce Transformation, Global Innovation Challenge

Certifications | CISM (Ongoing), Become a Senior Manager, Dev Ops Certified Site Reliability Engineer, Microsoft Certified Technology Specialist, VMWare Certified Professional



Microsoft CERTIFIED Professional

vmware CERTIFIED PROFESSIONAL 5

DevOps Institute SRE Foundation CERTIFIED

Industry Experience and Key Skills

- 17+ years of IT experience in the field of Cybersecurity, Incident Response and Recovery, End User Computing and Workforce Transformation
- Global and regional enablement of Cybersecurity services.
- Digital Forensics, Domain and Identity Administration, Server and Applications Recovery, Cloud Technologies, Databases, Storage and Backup, Network, Client Deployment etc.
- Customer business prioritization mapping and defining service outcomes
- Designing delivery processes using next gen technologies
- Client advisor for new technology and digital platform implementation
- Strategic Thinker, Results-Oriented, People person, and a natural leader

Previous Roles

- Principal Engineer - Delivery Lead for Cybersecurity, Incident Response Recovery, Application Mgmt., Virtualization, Migrations, Modern Provisioning & Digital Workspace
- Systems Integration Sr. Advisor - Managing large Windows Migration readiness projects. Enabling best shoring efforts.
- Dell ABU Consultant - Virtual Data Center implementation to enable App Services Delivery in factory model. Application Packaging and Virtualization, Browser and Desktop Migration
- Software Engineer, HSBC Bank & Patni Computer Systems - Web and Client-Server Java Application Dev, OOP, DBMS, Web development, Unix and Shell Scripting
- Network Engineer, Zain Information Systems, Internship - VLAN Implementation and Simulation

Experience

- Solutioning and managing technical delivery of Dell's Proactive Cybersecurity Services Customers
- Practice Lead for 18 Countries
- Incident Response and Recovery Lead and Enterprise Architect
- Application portfolio unification and readiness for customers going through migrations, mergers, separations and globalization.
- Assisted 150+ customers in their migration journey
- Single point of contact for Multi M$ accounts
- Expert in identifying opportunities and utilizing best shoring capabilities for delivery.
- Designing, Implementation and Operation of cloud-based Dell Factory. Enablement of HA and DRS for business continuity
- Process improvement, optimization and modernization initiatives leading to multiple awards
- Managing C-Level Executive Communication
- Training and mentoring team members to excel and exceed expectations.
- Languages: English, Hindi, Telugu, Urdu, Punjabi, Gujrati, Marathi, Bengali

Who We Are and Our Approach

Product Agnostic Security Practitioners following Framework-Driven Methodology focusing on Resiliency

- North America DoD Clearance
- Bench of Industry-Certified Experts
  - Military/gov, law enforcement, energy industry backgrounds
- Security Certifications
  - CISSP, CISM, Certified Ethical Hacker (CEH), GIAC SANS (GNFA, GCFA, GCIA, GCWN, GCIH, GSNA, GSEC), OSCE, OSCP, CompTIA CSA+, CompTIA CASP+, CSFPC, Cisco Specialist, Cisco CyberOps, SAFe
- Product Certifications
  - MCSE, VMWare VCP, SecureWorks XDR & VDR, Carbon Black, Cylance, Arcsight, Juniper, McAfee, CSM, Splunk, Citrix, AWS, Microsoft Security, DevOps SRE

© Copyright 2020 Dell Inc.

Today's Protection Needs

The threat landscape is challenging and requires
many skilled peoples, tools and solutions.

Very high complexity , getting more difficult every day

Securing a modern environment requires a new approach

DELL Technologies

Cyber threats 2021: The Facts

Every 11 seconds

A cyber or ransomware attack occurs[1]

$6T

Total global impact of cyber crime in 2021[2]

$13M

Average cost of cybercrime for an organization[3]

Banking	$18.4M
Utilities	$17.8M
Software	$16.0M
Automotive	$15.8M
Insurance	$15.8M
High Tech	$14.7M
Capital Markets	$13.9M
Energy	$13.8M
US Federal	$13.7M
Consumer Goods	$11.9M
Health	$11.9M
Retail	$11.4M
Life Sciences	$10.9M
Media	$9.2M
Travel	$8.2M
Public Sector	$7.9M

*[1]Cybersecurity Ventures: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021
https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021
[2]Cybersecurity Ventures: *https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021*
[3]Accenture Insights, Ninth Annual Cost of Cyber crime Study March , 2019 - https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

DELL Technologies

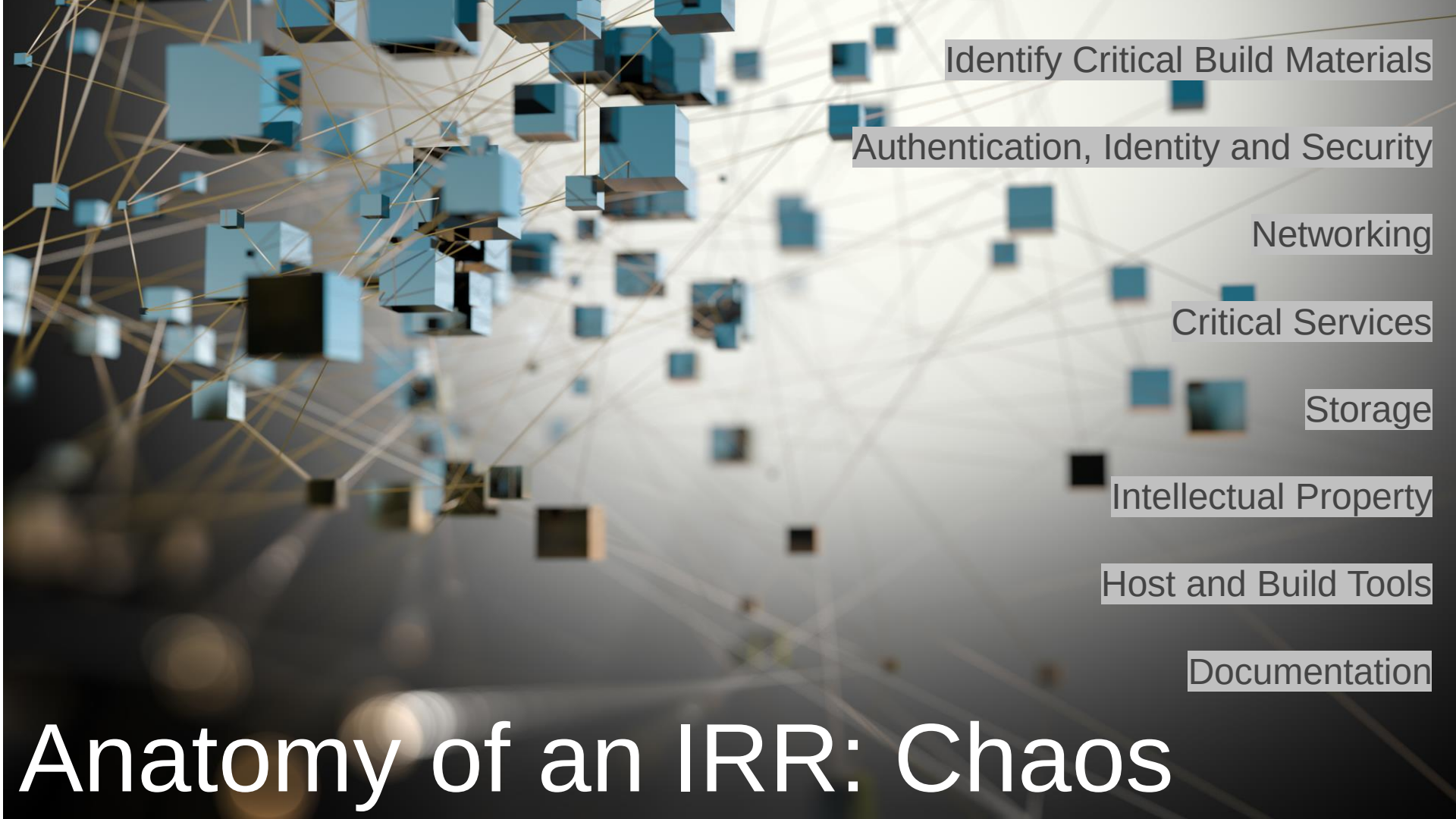
Evolution of Cyber Threat Actors

Different Motivations, Techniques, & Goals

CRIME	INSIDER	ESPIONAGE	HACKTIVISM	TERRORISM	WARFARE
					
Theft & extortion for financial gain	Trusted insiders steal or extort for personal, financial, & ideological reasons. Increasingly targeted because of privileged access to systems	Corporate or Nation-state actors steal valuable data	Advance political or social causes	Sabotage & destruction to instill fear	Nation-state actors with destructive cyber weapons (Not Petya)

© Copyright 2020 Dell Inc.

PREPARE!!!

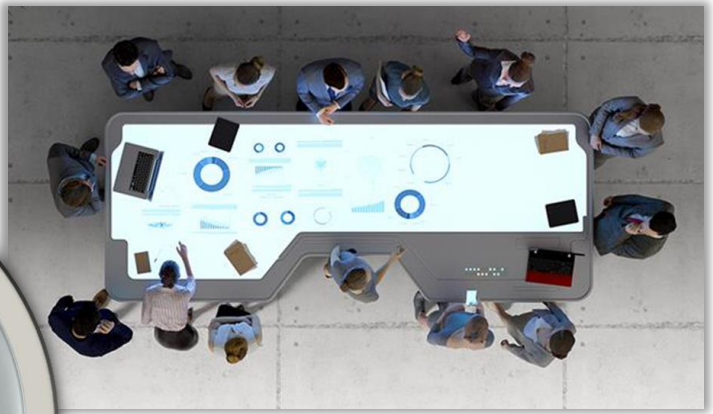


Anatomy of an IRR: Chaos

How to Recover Faster?

Incident Response and Recovery Retainer

Intelligent Cyber Resilient Technologies

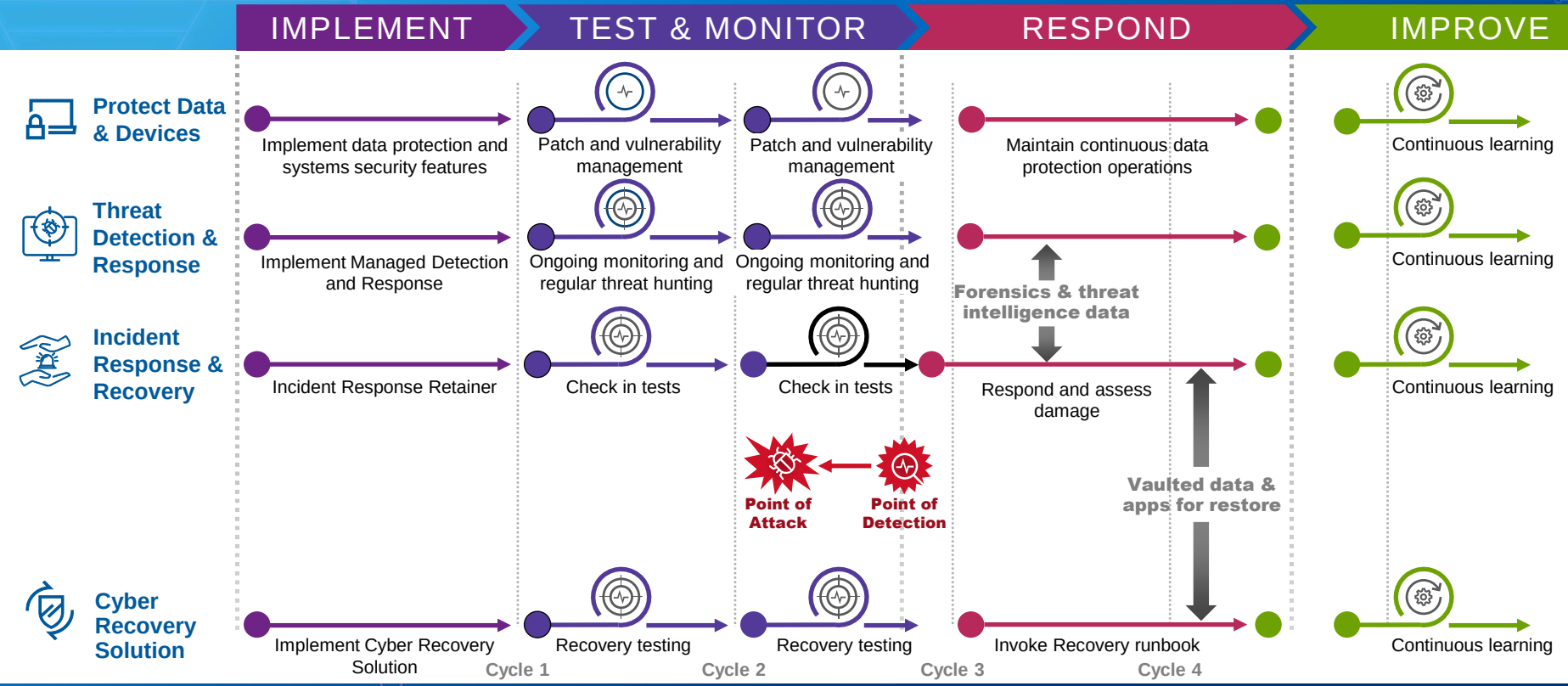


Tabletop Exercises

DELL Technologies

Connecting protection, detection, response and recovery

Tie together key capabilities to reduce recovery and keep the business up and running



Copyright © Dell Inc. All Rights Reserved.

Key Considerations for Incident Response

- CYA = **C**all **Y**our **A**ttorney
  - Disclosure requirements
  - Liability concerns
  - Evidence handling requirements
- Partnerships Matter!
  - Media relations
  - Partner / suppliers *(response help)*
  - Supply chain / service providers *(can't recover on your own)*
  - Legal advisors
  - Insurance company
  - FBI local agent
- Communications Management

- Cyber Recovery ≠ Disaster Recovery
  - Geography doesn't provide protection
  - Restoration must remove vulnerabilities

© Copyright 2020 Dell Inc.

K-12 Organization

DELL Technologies

Reacting to a Ransomware Virus

Timeline:

- 5:00am servers were offline and encrypted. Ransom note sent for payment of $1.5M
- 7:30am client contacted Dell Incident Response Team
- Dell Team engaged immediately; Dell resources traveled to site by 5pm
- 3-month engagement (non-IR Retainer customer)

Investigation:

- Identified security tools to assist with identification and containment of threat actor
- Leveraged security tools to identify patient zero
- Eradicated threat actor
- Investigate for signs of data exfiltration
- Review dark web for exfiltrated data

Results:

- HVAC system down
- Security camera systems down
- Underlying hardware for datacenter non-recoverable (200+ virtual servers)
- Determined that of 5,500 endpoints (servers and workstations), 93% were infected / encrypted
- Conducted data sanitization, networking and server recovery
- Deployed EDR solution and integrated 24x7 monitoring

Incident Response & Recovery | Country: USA

Rebuild / Restore / Re-Deploy

Provide expert guidance on IT and Security topics during the recovery effort

Customer Success Stories

1 Large Packaging Company

- Global packaging company
- Ransomware attack
- Ramped to 130 resources in < 7 days (180 at peak)
- Data sanitization, networking and server recovery
- Stood up 24x7 service desk in 24hrs to support 9 languages

2 Services Provider

- Service Provider (Large Global OEMs)
- Ransomware & Extortion
- Damaged entire IT environment
- 45-day recovery
- 24x7 delivery with over 150+ resources

3 International Government Agency

- International Government Agency
- State-sponsored ransomware attack
- Stole IP and sensitive government PII
- 30-day effort, recovered vital server infrastructure
- Data sanitization, networking and server recovery
- 24x7 delivery with 15 resources

4 Retail

- Retail chain with 58 stores
- Ransomware attack
- Damaged entire IT environment
- 90-day recovery with 24x7 delivery
- Data sanitization, networking and server recovery
- Microsoft 365 Defender Suite monitoring

DELL Technologies

© Copyright 2020 Dell Inc.

Final Words

Have a Plan

Know the Plan

Practice the Plan

© Copyright 2020 Dell Inc.

Questions?

Cyber Resiliency Health Check

Incident Response Recovery

Managed Detection & Response

DELL Technologies

Contact info

Surya Mukka, MCP, VCP, CRE
Cybersecurity Strategist & Practice Lead (US Central & APJ) – Global Proactive Cybersecurity Services
Dell Technologies | Global Professional Services
Mobile: (732) 318-0452
Surya.Mukka@Dell.com

Backup Slides

© Copyright 2020 Dell Inc.

WDATPaaS Customer Story

Higher Education | United States

Quacks like a Keyboard

Austin Peay State University (APSU) was attacked with a Rubber Ducky hacking device, an innocuous looking USB flash drive specially developed to emulate a keyboard Human Interface Device (HID) so that upon insertion, Windows promptly installs the appropriate HID drivers to allow for system input like any other keyboard. What makes this device and "hack" so dangerous is that once the Ducky is installed, it spews keyboard input in the form of command shell prompted commands and scripts at a rate of 1000's of characters per second. Within several moments, any number of attack payloads are executed on the victim machine. The favorites? Keystroke logger and a backdoor communication channel to send all legitimate typed characters back to the attacker… usernames, passwords, sensitive documents or emails… all of it gets transmitted!

How we helped

APSU was immediately engaged via incident response protocols and real-time coordination that enabled resolution in under 3 hours. As the device was plugged in from machine to machine across the campus, Dell EMC Security Analysts provided real-time, actionable, location and user information that ultimately led to APSU staff pinpointing a group of students moving from classroom to classroom attacking machines. Undetected, these victim machines would have been attacked for stolen credentials and other potentially sensitive information. They could also have become the foothold into the university network leveraged by the attackers to move laterally and expand the breach to total domain compromise; which is the observed behavior in so many attacks today.

The Solution

Amid the rising volume and velocity of threats emerge a category of fileless attacks, like the Rubber Ducky, that don't touch the disk and are not detected by traditional anti-malware solutions. Having an advanced threat detection capability on your endpoints is of critical importance. Furthermore, you need a team of experts that can quickly investigate and respond to observed threats and provide the facts and guidance you need to prevent major breach damage.

Get ***your*** ducks all in a row with **Dell EMC's WDATPaaS**

"Working with the Dell EMC Cybersecurity Team has allowed the APSU IT Security "team" (1.25 people) to have expert resources assisting us in watching, detecting, and mitigating threats to the university network."

- Stephanie Taylor, Director of Information Security, APSU

© Copyright 2020 Dell Inc.

Incident Response & Recovery Phases

Dell Technologies' 3-Phased Recovery Approach for a Post Cyber-Event

DELL IRR

Initial Response & Triage

Phase 1

- Discovery
- Response
- Threat Hunting & Analysis
- Data Gathering & Forensics
- Introduce EDR, MDR, XDR, VDR
- Threat Mitigation
- Alternate Network & Services
- Map and Establish Core Business Dependencies & Functions

Restore Business Capacity & Conduct Network Rebuild

Phase 2

- Re-establish Core Business
- Redeploy PCs
- Rebuild & Redeploy Servers
- Rebuild & Harden OS Images
- Recover End User Data from Backup
- Network Security
- Decrypting & Sanitizing Drives
- Recovering Application Servers
- AD Stabilization
- Azure IaaS
- Implement Security Monitoring

Increase Business Velocity & Network Security Stabilization

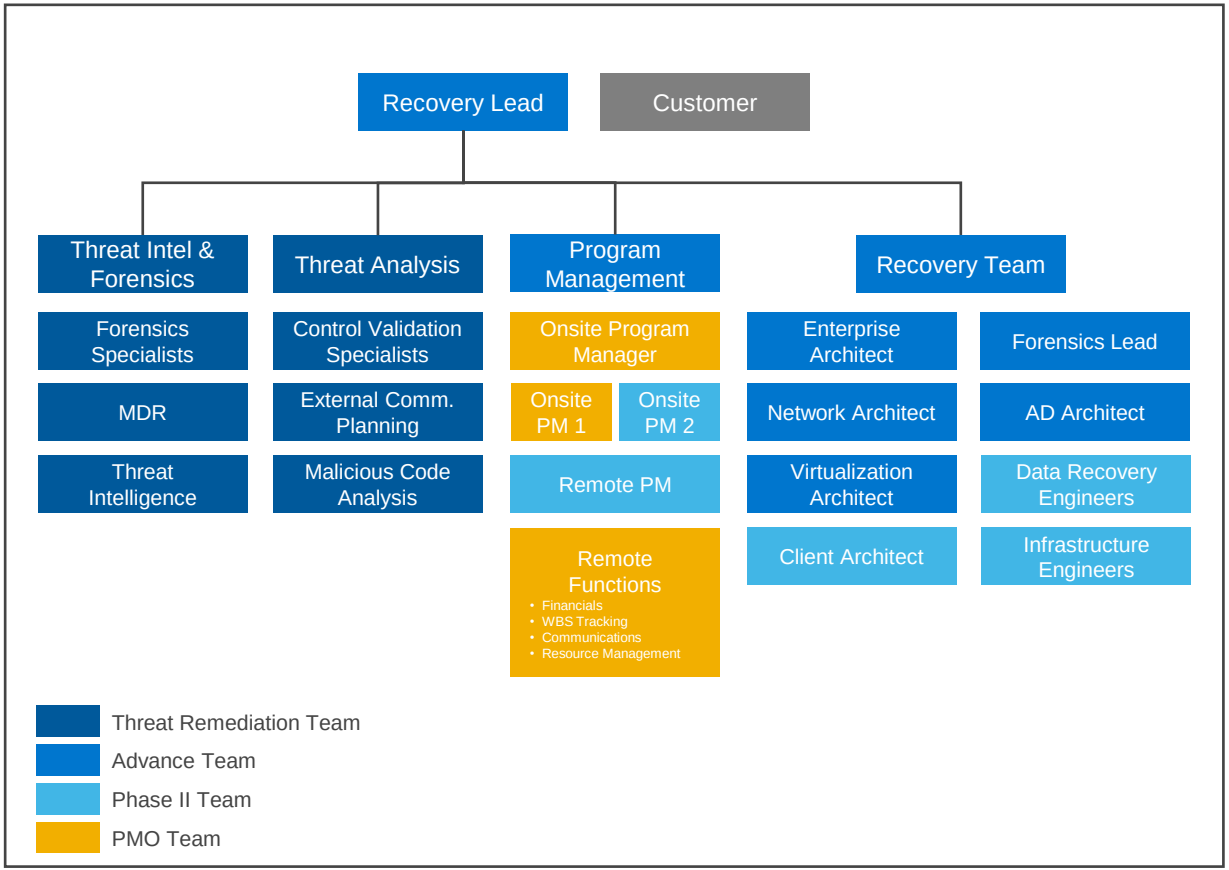
Phase 3

- Introduce vCISO Strategy & Vision
- System Management
- Extend EDR, MDR, XDR, VDR
- 24x7 Monitoring
- Routine Security Reviews
- System Management
- Network Monitoring / Clean Network
- Lift and Shift of Application Servers
- Transition to New Environment to IT Staff
- Knowledge Transfer

DELL Technologies

© Copyright 2020 Dell Inc.

Typical IR Team Composite

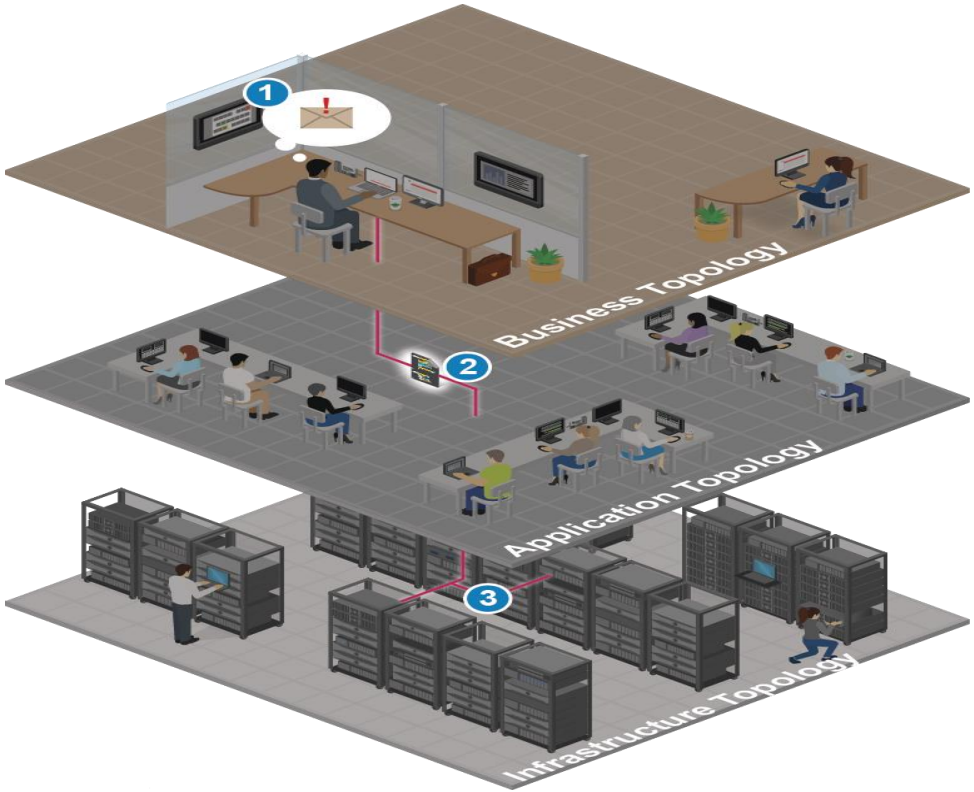


Solution Components

- IR Intake Lead receives the call
- Core team assembled
- Extended team staffed
- Solutioning
  - Price varies based on size of recovery effort and scope

© Copyright 2020 Dell Inc.

Identify Critical Systems and Map Dependencies



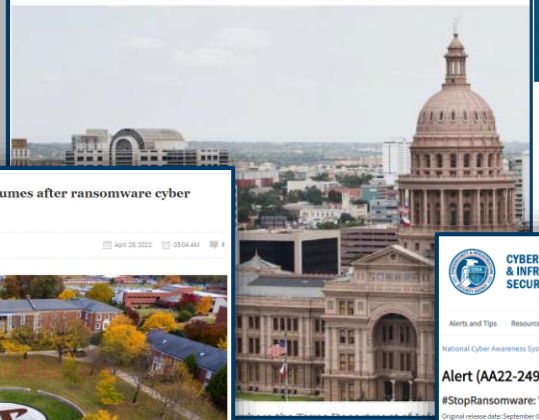
© Copyright 2020 Dell Inc.

Cyber News

Aug 2019

Ransomware Attack Hits 22 Texas Towns, Authorities Say

The state declined to say which towns were affected by the coordinated cyberattack. But one expert said it could signal more such attacks in the future.



Oct 2020

JOINT CYBERSECURITY ADVISORY

TLP:WHITE

APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations

SUMMARY

This joint cybersecurity advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor techniques.

Feb 2021

An official website of the United States government Here's how you know

rt (AA21-055A)

oitation of Accellion File Transfer Appliance

Release date: February 24, 2021

mary

int advisory is the result of a collaborative effort by the cybersecurity authorities of lia,[1] New Zealand,[2] Singapore,[3] the United Kingdom,[4] and the United States. These authorities are aware of cyber actors exploiting vulnerabilities in Accellion File er Appliance (FTA).[7] This activity has impacted organizations globally, including n Australia, New Zealand, Singapore, the United Kingdom, and the United States.

Dec 2020

CISA INSIGHTS

March 9, 2021

Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise: Risk Decisions for Leaders

Since December 2020, the Cybersecurity and Infrastructure Security Agency (CISA) has been responding to a significant cybersecurity incident. An advanced persistent threat (APT) actor added malicious code to multiple versions of the SolarWinds Orion

The threat actor only targeted a select group of organizations affected by the SolarWinds Orion

Austin Peay State University resumes after ransomware cyber attack

By Ax Sharma

Sep 8th , 2022

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources

National Cyber Awareness System > Alerts > #StopRansomware: Vice Society

Alert (AA22-249A)

#StopRansomware: Vice Society

Original release date: September 06, 2022 | Last revised: September 08, 2022

Summary

Note: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint CSA to disseminate IOCs and TTPs associated with Vice Society actors identified through FBI investigations as recently as September 2022. The FBI, CISA, and the MS-ISAC have recently observed Vice Society actors disproportionately targeting the education sector with ransomware attacks.

Over the past several years, the education sector, especially kindergarten through twelfth grade (K-12) institutions, have been a frequent target of ransomware attacks. Impacts from these attacks have ranged from restricted access to networks and data, delayed exams, canceled school days, and unauthorized access to and theft of personal information regarding students and staff. The FBI, CISA, and the MS-ISAC anticipate attacks may increase as the 2022/2023 school year begins and criminal ransomware groups perceive opportunities for successful attacks. School districts with limited cybersecurity capabilities and constrained resources are often the most vulnerable; however, the opportunistic targeting often seen with cyber criminals can still put school districts with robust cybersecurity programs at risk. K-12 institutions may be seen as particularly lucrative targets due to the amount of sensitive student data accessible through school systems or their managed service providers.

The FBI, CISA, and the MS-ISAC encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.

Actions to take today to mitigate cyber threats from ransomware:

- Prioritize and remediate known exploited vulnerabilities.
- Train users to recognize and report phishing attempts.
- Enable and enforce multifactor authentication.

Mar 2021

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:WHITE Product ID: AA21-069A

March 10, 2021

Compromise of Microsoft Exchange Server

This Joint Cybersecurity Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 8. See the ATT&CK for Enterprise framework for referenced threat actor techniques and for mitigations.

SUMMARY

This Advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) to highlight the cyber threat associated with active exploitation of vulnerabilities in Microsoft Exchange on-premises products. The FBI and CISA assess that nation-state actors and cyber criminals are likely among those exploiting these vulnerabilities. The exploitation of Microsoft Exchange on-premises products poses a serious risk to private companies. Successful exploitation of these Exchange Servers, enabling them to gain prise network. It has the potential to affect tens of rovides adversaries with access to networks nally identifiable information (PII), and other sensitive FBI and CISA assess that adversaries will continue ks and steal information, encrypt data for ransom, or ay also sell access to compromised networks on the

Apr 28, 2022

Dallas Business Journal

Tyler Technologies ransomware attack highlights what companies need to know - Dallas

Plano's Tyler Technologies was hit by an attack that's become increasingly common today. The software company, which assists local and state ...

4 weeks ago

© Copyright 2020 Dell Inc.

DELL Technologies