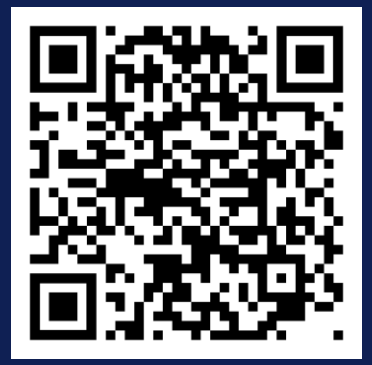
MassCyberCenter – Cybersecurity Call Incident Response and BC Lessons Learned

Augusto Alvarez
Solutions Principal – Dell Technologies Services
Augusto.Alvarez@Dell.com



DELL Technologies

Agenda

- Common Gaps Found in our Customers
- Preparing Yourself for a Cyber Incident Following NIST CSF 2.0
- Call to Action: Stay Engaged

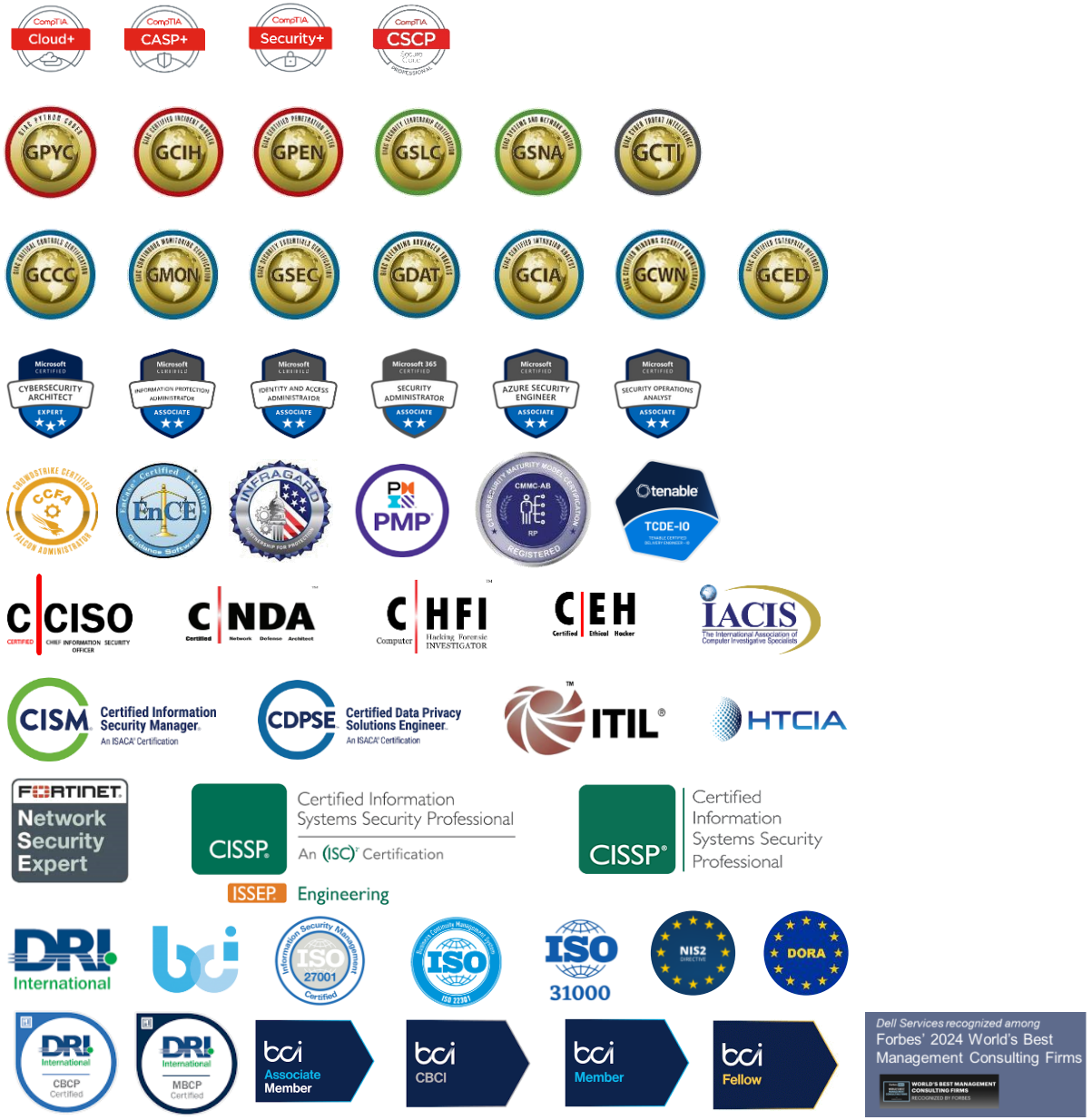
2 Copyright © Dell Inc. All Rights Reserved.

Why Dell for cybersecurity?

Largest security company you've never heard of

1. Size / experience
2. Embedded security
3. Partnerships
4. Integration
5. Service / support

Guardians of the gateway



Dell Services recognized among Forbes' 2024 World's Best Management Consulting Firms

Common Gaps Found in our Customers

DELL Technologies

Reality Check

- We are fighting an asymmetric battle
- Bad guys are seeing the same efficiencies in AI as the good guys
- Attackers' business models are very efficient
  - Ransomware as a Service represents a minimal cost and effort. Ransomware provider can only get paid if attackers are successful.
- Low revenue / small companies are attackers low hanging fruits
- If you can't discern what normal looks like in your environment, you won't be able to detect what abnormal looks like.
- It is challenging to establish a common language between the business, IT, users, security, legal, risk and compliance.

 Copyright © Dell Inc. All Rights Reserved.

Dell Customer Communication - Confidential

Common “lessons learned” from cyberattacks

Lack an effective and tested IR plan

Lack an effective DR and BC plan

Poor communication across the business

Abandon potential recovery paths too quickly

Poor understanding of the perimeter to contain threats

Lack of recovery documentation for critical systems

Lack infrastructure to facilitate recovery

Not ready to scale with resources and partners

Lack current HW/SW support agreements

End of Life infrastructure requires specialist

DELL Technologies

Typical Lessons Learned - Areas of Exposure

1. Lack of Multi-factor Authentication
2. Weak Password Policies
3. Lack of privilege separation
4. Insufficient Protection of Backups (network segmentation, lack of immutability, shared/weak identity plane)
5. Inadequate EDR/SIEM configuration
6. Poor Perimeter device vulnerability management
7. Insufficient IT and Security staffing
8. Lack of Network Segmentation
9. Poor security architecture of remote access solutions (VPN, Citrix, VDI)
10. Poor hypervisor Infrastructure vulnerability management
11. Lack of Primary Storage availability configuration (snapshot policies)
12. End of Life Software and Hardware

Copyright © Dell Inc. All Rights Reserved.

Preparing Yourself for a Cyber Incident Following NIST CSF 2.0

 Copyright © Dell Inc. All Rights Reserved.

NIST CSF 2.0

Security Controls Alignment

IDENTIFY

- Asset Management (ID.AM)
- Risk Assessment (ID.RA)
- Improvement (ID.IM)

PROTECT

- Identity Management, Authentication, and Access Control (PR.AA)
- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Platform Security (PR.PS)
- Technology Infrastructure Resilience (PR.IR)

DETECT

- Continuous Monitoring (DE.CM)
- Adverse Event Analysis (DE.AE)

RESPOND

- Incident Management (RS.MA)
- Incident Analysis (RS.AN)
- Incident Response Reporting and Communication (RS.CO)
- Incident Mitigation (RS.MI)

RECOVER

- Incident Recovery Plan Execution (RC.RP)
- Incident Recovery Communication (RC.CO)

GOVERN

- Organizational Context (GV.OC)
- Risk Management Strategy (GV.RM)
- Roles, Responsibilities, and Authorities (GV.RR)
- Policy (GV.PO)
- Oversight (GV.OV)
- Cybersecurity Supply Chain Risk Management (GV.SC)

 Copyright © Dell Inc. All Rights Reserved.

Initiatives that need to be in place aligned with NIST CSF

IDENTIFY

- **Inventory of endpoints, servers, and critical assets, BIA and app dependencies.**
- **Identify high-value targets** (HVTs) such as file servers, domain controllers
- **Risk assessments and Ransomware TTX**
- **Classify data sensitivity and determine backup & recovery priorities**
- **Review attack vectors** (e.g., phishing, exposed RDP, unpatched software)
- **Map potential lateral movement paths** (e.g., SMB, RDP, WinRM, WMI)
- Monitor **third-party integrations** for vulnerabilities

PROTECT

- EDR/XDR
- **User awareness training program**
- **Backup environment isolated and immutable**
- **Mature vulnerability management program**
- App whitelisting
- **Restrict elevated permissions**
- **JIA (just in time) and JEA (just enough access) enabled**
- Least privilege & restrict local admin accounts
- Network segmentation and/or **microsegmentation** to prevent lateral movement
- Dynamic RBAC and ABAC

DETECT

- **Indicators of Compromise (IoC) and threat hunting**: File modification rate, unusual process execution, mass file encryption, abnormal outbound network traffic, user accessing systems they are not supposed to, hours of logins and access, etc.
- Detection sources: EDR/XDR, SIEM **correlation rules**, network IDS/IPS, evaluate logs in relevant platforms
- Monitoring for AD misconfigurations/changes
- **Monitoring backup and storage potential threats and/or changes**

RESPOND

- **Follow IRP with specific use case for ransomware**
- **Contextual actions automated based on IoCs**: MFA triggered, isolate user, isolate device, reset passwords, etc.
- **Determine lateral movement scope**
- **Forensics analysis** and threat hunting
- Triage and containment
- Evidence collection and preservation
- Block malicious hashes, domains, IPs at firewall & EDR
- Identify and remove backdoors, scheduled tasks, rogue accounts, data exfiltration, etc.

RECOVER

- **Follow “crown jewels” recovery plan**
- **Verify backup integrity**
- **Restore in airgapped environment** to execute proper validations
- **Enforce MFA**
- Deploy **verified gold images**
- Conduct root cause analysis to understand entry point
- Update incident response playbooks
- Update security rules
- Conduct new user training, update content and programs
- Share IoCs with threat intelligence platforms

Copyright © Dell Inc. All Rights Reserved.

Initiatives that need to be in place aligned with NIST CSF

GOVERN

- **Cybersecurity Program with clear roles and responsibilities**. RACI going across IT, security, business, risk and compliance.
- **Develop and communicate Cybersecurity policies**. Align regulations with legal and business requirements. Keep your users informed (who, what and WHY)
- **Risk management and oversight**. Integrate the cybersecurity risk management into the Enterprise Risk Management (ERM)
- **Build a strong 3rd party integration**. Ensure there is a proper 3rd party risk assessment in place. And some 4th party risk assessments when applicable.

 Copyright © Dell Inc. All Rights Reserved.

Dell Customer Communication - Confidential

Where to Start- Tier 0 Infrastructure and Services

Cyber Recovery Vault Recommendations

Authentication, Identity & Security

- **Active Directory / LDAP**
- **DNS dumps**
- Certificates
- Event logs (including SIEM data)

Intellectual Property

- **Source code**
- Proprietary algorithms
- Developer libraries

Networking

- **Switch / router configuration**
- **Firewall / load-balancer settings**
- IP Services design
- Access Control configuration
- Firmware / Microcode / Patches

Host and Build Tools

- **Physical/Virtual Platform Builds**
- Dev Ops tools & automation scripts
- Firmware / Microcode / Patches
- Vendor software
  - Binaries (golden images)
  - Configurations & settings

Storage

- **Backup Hardware configuration**
- SAN / Array configurations
- Storage Abstraction settings
- Firmware / Microcode / Patches

Documentation

- CMDB / asset **D/R and Cyber Recovery Run-books & Checklists**
- Management extracts
- HR Resources & Contacts Lists

Copyright © Dell Inc. All Rights Reserved.

Key Takeaways

- **Failing to plan is planning to fail**
  - **Don’t boil the ocean, have a roadmap**. Fail early, fail fast.
- **Adopt a risk-based approach**. Prioritize security investments based on business risk.
- Make sure you are doing your **foundational initiatives first** (updated CMDB, frequent BIA, MFA enabled, network diagrams, vulnerability management, etc.)
- **Validate, validate, validate**. Test your cybersecurity and resiliency posture frequently.
- Build your **Cybersecurity culture**.
- **Don’t push automation to the end**.
- Follow the **Zero Trust principals**. Assume every system is potentially compromised
- Get your **Executive leaders and Board involved**. Cybersecurity should always be part of their agenda and priorities.

 Copyright © Dell Inc. All Rights Reserved.

Call to Action: Stay Engaged

 Copyright © Dell Inc. All Rights Reserved.

Dell Technologies Incident Response & Recovery

A Call for Action – 833-265-6167

Customer hits the panic button and asks for assistance in their most critical moment…

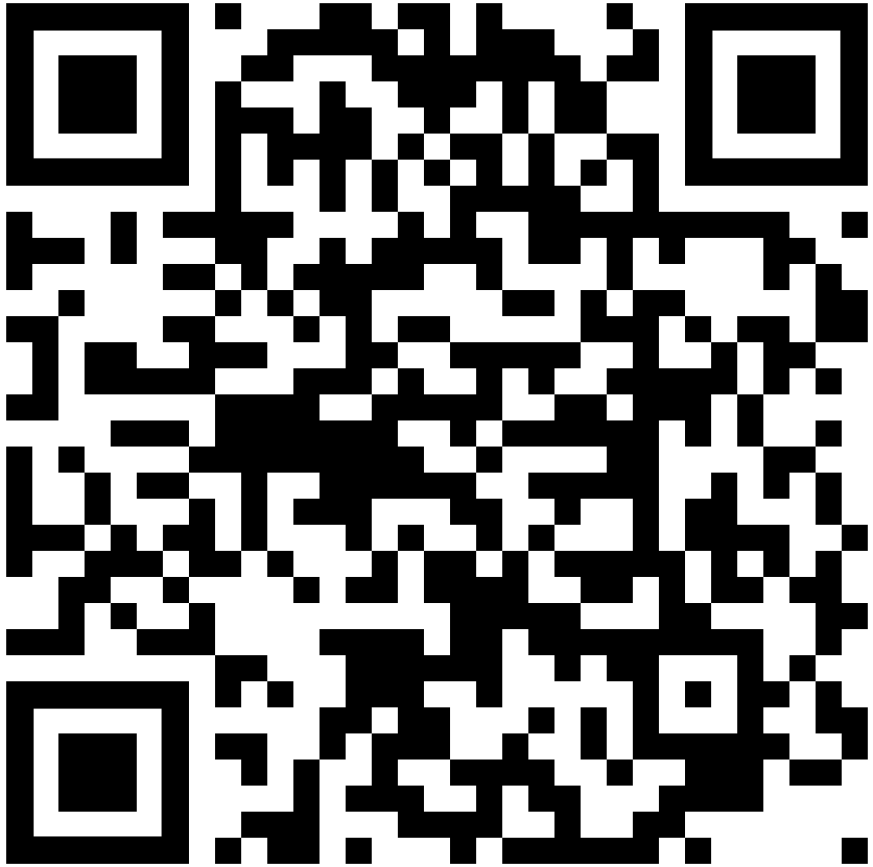
Dell IRR team will triage and solution efforts for recovery…

IRR Advanced Team is deployed to immediately begin recovery efforts…

Customer gets back to operational!

Have you been breached or have a Cyber-event? Contact → Incident.Recovery@dell.com

Stay in touch!



Augusto Alvarez
Solutions Principal - Cybersecurity & Resiliency at Dell Technologies

Augusto.Alvarez@Dell.com

16 Copyright © Dell Inc. All Rights Reserved.