



# Fortifying the Grid: Incident Response and Advanced Threat Detection

Exploring incident response, resilience planning, and emerging threats in the energy sector.



Presented by Clayton Dillard, CEO | Legion Cyberworks LLC

# Our Agenda Today!

## Speaker's BIO

Who is this guy?

1

2

## About Legion Cyberworks

Discover Legion Cyberworks' mission, services, and expertise in protecting organizations against cyber-attacks.

## Significant Cyber Threat Stories

Explore three real-world cyberattacks that resulted in substantial impacts to the victims, including energy providers.

3

4

## Challenges You Face

Understand the unique cybersecurity challenges that cooperative utilities face, including evolving threats, resource constraints, and reliance on interconnected systems.

## Planning and Preparation for an Attack

Learn about essential steps in developing an incident response plan, including identifying key vulnerabilities and establishing clear communication protocols.

5

6

## Prevention, Detection, and Response

Dive into strategies for preventing cyberattacks, detecting suspicious activity, and responding effectively to incidents.

## The Wrap-Up

Explore the benefits of proactive cybersecurity measures and the long-term impact of securing critical infrastructure.

7

# About the Speaker

- 1996: Started IT career as a Desktop Support Technician at Eaton Powerware
- 1998: Took a role at a Raleigh-based consulting firm providing support and working infrastructure projects at Rex Hospital (now UNC Health Rex)
- 1999: I left Alphanumeric Systems for a full-time role with a start-up eCommerce company in RTP
- 2001: Transitioned to full-time InfoSec role at ABB, Inc. as a professional penetration tester and consultant
- 2007: Worked for OpsWare (purchased by HP) as a Sysadmin
- 2009: Served as Director of Technology and Security at a New York-based FinTech firm, Mediant Communications for 13 years, where I managed a team in our North Carolina offices.
- 2016: Launched **Legion Cyberworks**, driven by my passions for technology, cybersecurity, and helping people.





# Emerging Threats in the Energy Sector



## Ransomware

Malicious software encrypting critical data for ransom demands.



## Supply Chain Attacks

Compromising trusted vendors to infiltrate utility networks.



## Advanced Persistent Threats (APTs)

Sophisticated, long-term intrusions targeting sensitive information and laying the groundwork for disruptive and destructive actions.

# The NotPetya Attack: A Case Study in Global Disruption

The NotPetya attack, launched in June 2017, was a global ransomware attack that caused widespread disruption. Disguised as a legitimate software update, it quickly spread, exploiting a vulnerability in the Windows operating system. The attack caused billions of dollars in damage, significantly impacting the global economy.

NotPetya is widely considered one of history's most damaging cyberattacks, highlighting the critical need for robust cybersecurity measures.





# The NotPetya Attack Timeline

## 1 June 27, 2017: The Start

The NotPetya ransomware attack began with the compromise of a Ukrainian accounting software company, M.E.Doc. The malware was distributed through a malicious update, initially affecting Ukrainian businesses and government agencies, including critical infrastructure operators like energy companies.

One of the first companies to be affected was a Ukrainian utility company, which suffered a major disruption to its operations, highlighting the immediate impact of the attack on critical infrastructure.

## 3 Billions in Damages

The attack caused billions of dollars in damages, affecting numerous businesses worldwide. NotPetya's impact extended beyond financial losses, disrupting supply chains, halting production, and hindering critical services. In the energy sector, the attack significantly impacted production and distribution of energy, leading to shortages and economic losses.

1

2

## 2 Global Spread and Impact

NotPetya quickly spread globally, targeting organizations in various sectors, including energy, finance, and transportation. The attack crippled systems, encrypted data, and caused significant disruption to operations. For example, in the energy sector, several power grids were disrupted, leading to temporary blackouts and operational challenges.

The attack also had a major impact on the shipping giant Maersk, causing widespread disruption to its global operations. Several other multinational corporations, including pharmaceutical companies, food producers, and automotive manufacturers, were also affected, demonstrating the broad reach and devastating consequences of the NotPetya attack.

3

4

## 4 The Russian Origin of NotPetya

NotPetya was a deliberate act of cyberwarfare, launched by the Russian government against Ukraine. The attack demonstrated the Russian government's willingness to use cyberweapons to disrupt critical infrastructure and destabilize its adversaries.



# Indestroyer2 - Russian Malware Attack on Ukraine

In April of 2022, a variant of the Industroyer malware (initially used in 2016) was deployed in an attack targeting high-voltage electrical substations. Fortunately, the attack was detected and mitigated before it could cause a blackout.

This attack demonstrated the persistent threat posed by state-sponsored actors to critical infrastructure (Source: IronNet)



# The Indestroyer2 Attack Timeline

**April 2022**

**1**

Indestroyer2 malware targeted Ukrainian electrical substations, attempting to disrupt power distribution.

**2**

## Target

The attackers focused on high-voltage electrical substations, aiming to cause a widespread blackout in Ukraine.

## Malware

**3**

The malware was a variant of Industroyer, previously used in a 2016 attack on the Ukrainian power grid. It used custom tools and exploits to target specific industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems.

**4**

## Exploit

The attackers exploited vulnerabilities in the substation's control systems to gain unauthorized access and potentially take control of critical infrastructure.

The attack specifically targeted vulnerabilities in Schneider Electric programmable logic controllers (PLCs), a common component in industrial automation systems.

**5**

## Detection

The attack was detected and prevented by Ukrainian security forces and international partners who worked together to identify and mitigate the threat.

These vulnerabilities allowed the attackers to gain control of the PLCs and potentially manipulate critical operations.

**6**

## Outcome

This incident demonstrated the growing threat posed by cyberattacks to critical infrastructure and underscored the importance of robust cybersecurity measures. It highlighted the need for proactive security measures, including advanced threat detection, vulnerability management, and incident response capabilities, to protect against such attacks.

# The SolarWinds Security Breach



## Compromised Software

SolarWinds Orion software, a widely used network management tool, was compromised by a sophisticated malware campaign.



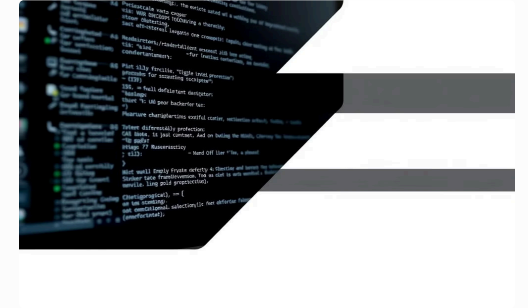
## Widespread Impact

The breach affected thousands of organizations, including government agencies, utilities, and Fortune 500 companies.



## Data Exfiltration

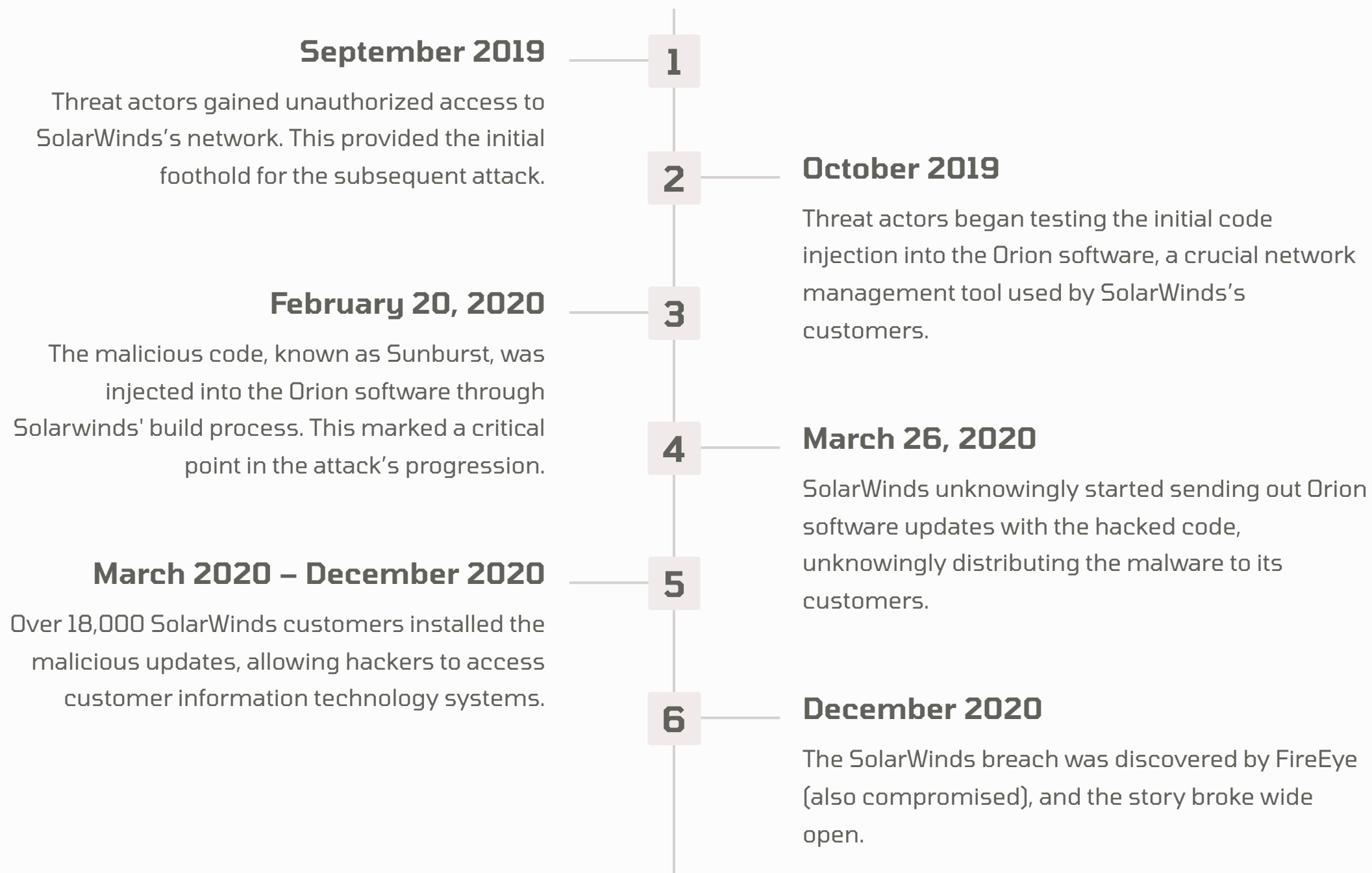
The attackers gained access to sensitive data and potentially compromised systems, impacting critical infrastructure and operations.



## Long-term Consequences

The SolarWinds breach raised concerns about supply chain security and highlighted the need for robust cybersecurity measures.

# The SolarWinds Attack Timeline



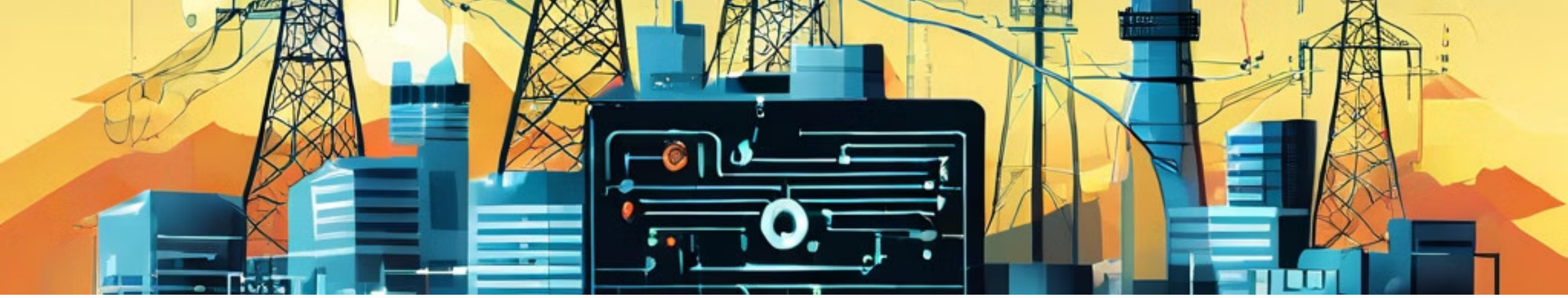
Some of the most notable victims of Sunburst include:

- Department of Energy
- National Nuclear Security Administration (maintains US nuclear weapons stockpile)
- NIH (National Institutes of Health)
- Dept. of Homeland Security
- Microsoft
- FireEye (A Tier 1 cybersecurity services firm)



# Ransomware and Other Threats to Energy Infrastructure

- **Growing Cybersecurity Risks:** Nearly 50% of critical infrastructure organizations in the energy sector are facing data breaches. **([Energy.gov, 2023](#))**
- **Vulnerable Systems:** Ransomware attacks exploit the industry's reliance on complex, often outdated systems. **([CISA, 2023](#))**
- **Planning to be Proactive:** Enhancing cybersecurity measures is crucial to safeguarding the power grid and ensuring operational resilience in the face of emerging threats. **([NCSLA, 2024](#))**



# The IT Department's Challenge

## Stretched Thin

As the IT Director of a small utilities corporation, you wear many hats, juggling critical infrastructure, cybersecurity, and supporting the organization's technology needs.

Limited resources strain your time and expertise.

## Overextended Operations

Maintaining the utility's mission-critical power grid assets demands specialized knowledge and constant vigilance.

You're often pulled in multiple directions, making it difficult to dedicate the necessary attention to these vital components.

## Cybersecurity Concerns

Defending against ever-evolving cyber threats is a top priority, but with a small team and limited budget, implementing robust security measures is an ongoing challenge.

Vulnerabilities in your systems could put your utility and its customers at risk.

## Constantly Juggling

The IT Director's role in a small utilities corporation is a delicate balancing act. You must juggle critical infrastructure, cybersecurity, and broader technology support - all while operating with limited resources. This scenario puts the utility's resilience and the community it serves at risk.



# Cyber Criminals Have the Advantage

- **Element of Surprise:** Cybercriminals often exploit vulnerabilities before they can be detected and patched, catching defenders off guard at a moment of weakness.
- **Opportunity to Strike Anytime:** Attacks can happen at any moment, day or night, when security teams are least prepared.
- **The Odds Favor Attackers:** With an exposed attack surface and limited resources, the cybersecurity challenge is an uphill battle for utility providers.

**The stakes are incredibly high for electric cooperatives and their customers, because a successful cyberattack could disrupt critical power infrastructure and cause widespread harm.**

# 2024 Incident Detection & Response Statistics

## Dwell Time

The average dwell time, the time between a compromise and detection, is alarming long.

Organizations are often unaware of breaches for **weeks, even months**, leaving them vulnerable to further attacks.

Source: **IBM Data Breach Report**

## Response Time

The average response time to cyber incidents is also concerning.

Organizations take **several hours, even days, to respond** and contain threats, impacting critical infrastructure and operations.

Source: **SANS Institute Report**

## Recovery Time

The average recovery time after a cyberattack can be **weeks, even months**. The complex process of restoring data, systems, and operations can be highly disruptive. This is on top of reputational damage that can take years to recover from.

Source: **Accenture Report**

# Impact on Cooperative Utilities

## Operational Disruption

Cyberattacks can cause power outages, affecting thousands of customers and first responders.

Critical infrastructure may be compromised, leading to safety concerns.

## Financial Consequences

Ransom payments and recovery costs can significantly strain budgets.

Potential legal liabilities and regulatory fines may arise from breaches.

## Reputational Damage

Loss of customer trust can have long-lasting effects on the cooperative.

Negative publicity may hinder future growth and partnerships.

**There is hope...**

# A Good MSP is a Force Multiplier

1

## Limited Resources

Electric grid cooperatives often face challenges with limited staff and budgets to manage infrastructure and ensure cybersecurity.

2

## Augmenting Capabilities

Managed Service Providers (MSPs) can help cooperatives by supplementing their teams with additional expertise and advanced tooling.

3

## Reducing Technical Debt

MSPs can help cooperatives modernize systems and reduce technical debt, improving overall resilience.

## Advanced Security Monitoring

Continuous threat detection and proactive security posture assessment.

## Vulnerability Management

Regular penetration testing and vulnerability scans along with remediation guidance for identified weaknesses.

## Incident Response Services

Rapid response to security incidents, containment, and recovery efforts.

## Threat Intelligence

Access to real-time threat intelligence to stay ahead of emerging attacks.

## Security Awareness Training

Training for employees on cybersecurity best practices to reduce human error.

# The Cornerstone: Incident Response Planning

1

## Detection

Implement advanced monitoring tools to quickly identify potential threats.

2

## Containment

Isolate affected systems to prevent further spread of the incident.

3

## Eradication

Remove the threat and patch vulnerabilities to prevent reoccurrence.

4

## Recovery

Restore systems and data, ensuring operational continuity post-incident.



# Implementing Advanced Detection Strategies

1

## Assessment

Evaluate current security posture and identify gaps in detection capabilities.

2

## Tool Selection

Choose appropriate detection and prevention tools based on the cooperative's specific needs and infrastructure.

3

## Integration

Implement and integrate new tools with existing systems and processes for seamless and effective operation. Focus on eliminating blind spots in your technical controls and your workflows.

4

## Training

Educate staff on new security tools and incident response procedures, and integrate into SOC workflows

5

## Continuous Improvement

Regularly update and refine detection and prevention strategies based on emerging threats.

# Top 12 Tools for Security

## 1 Managed Detection and Response (MDR)

24/7 monitoring and rapid incident response by trusted cybersecurity experts. This "SOC in a Box" capability is easier to onboard than you may think.

## 2 Network Detection & Response

Old-school detection rules, machine learning algorithms, and heuristics identify unusual patterns and potential threats earlier in the attack chain. [Your NDR should pipe data into your XDR platform.](#)

## 3 Endpoint Protection Platforms

Comprehensive security solutions for all workstations and servers connected to the network, delivered via EDR software. [Your EDR should feed into your XDR platform.](#)

## 4 Security Information and Event Management (SIEM)

Centralized log analysis, event correlation, and threat intelligence for enhanced threat visibility.

## 5 Honeypots and Deception Technologies

Enable early detection and identification of insider threats and post compromise actions. [Integrate into your XDR platform.](#)

## 6 Intrusion Detection and Prevention Systems

Identify threats at key ingress and egress points, and on lateral traffic on the network.

## 7 Continuous Penetration Testing

Conduct frequent simulated attacks to identify and prioritize weaknesses, enable remediation, and test your security controls.

## 8 Patch Management

Every device within the environment must be patched and kept up to date to close out vulnerabilities and weaknesses that introduce risk.

## 9 Dark Web Monitoring

This is an extremely potent tool against cyber attacks because it provides a way to peer into the underground and gain insights into planned attacks against your organization, alerts you to stolen credentials, and provides actionable intelligence.

## 10 Segmentation

Properly segmenting your endpoints and networks delivers a powerful layer of security that helps slow down attackers and impede or prevent the spread of malware and other threats across network boundaries. VLANs are good but firewall segmentation and ZTNA are often better.

## 11 Disaster Recovery

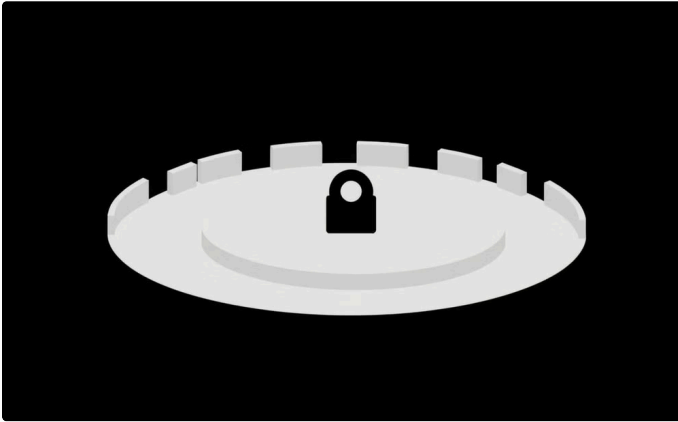
Regularly review, test, and validate your ability to recover critical systems, applications, and data.

Ensure that your backups are sufficiently protected against compromise and destruction.

## 12 Vendor Risk Management & Shadow IT

Develop processes, a short cadence, and employ tools like BlackKite, OneTrust, Nudge Security, spreadsheets and documents to frequently assess vendor related risks and the use of "Shadow IT" within your organization.

# Defense-in-Depth Strategy



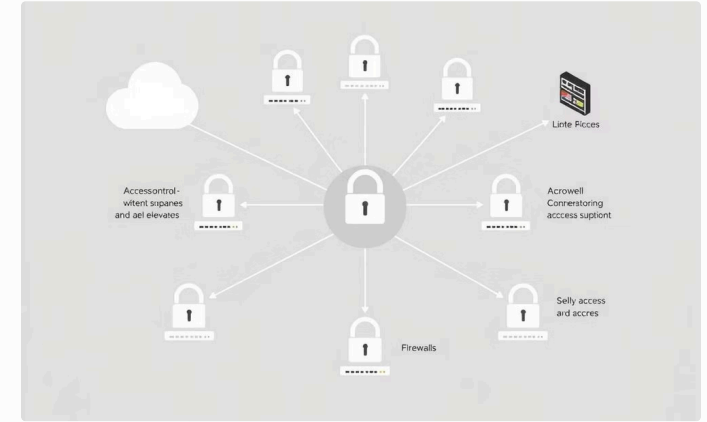
## Layered Protection

A defense-in-depth strategy requires multiple layers of security to protect your network from cyberattacks.



## Strong Prevention

Start with strong prevention measures including next-generation endpoint detection software, intrusion prevention systems, and robust training to help employees recognize and avoid phishing attacks.



## Hardened Defenses

Hardened authentication, network segmentation, and a zero-trust model further bolster your defenses.

# Building a Resilient Future

## Incident Response Plan

- Enables Response and Recovery
- This is your playbook when you need it most
- Vital element of your overall security posture
- **Moderate Implementation Difficulty**

## Segmentation

- Breach Containment
- Use firewalls for segmentation where possible / feasible
- Consider Zero Trust and/or micro-segmentation
- **High Implementation Difficulty**

## SIEM and Advanced Threat Detection

- Proactive Defense
- Enables detection and response
- Broad visibility, log retention, supports incident response
- **Moderate Implementation Difficulty**

## Workforce Training

- Human Firewall
- People are often the entry point to your organization
- Stolen accounts are better than a technical exploit
- **Low Implementation Difficulty**

## Continuous Improvement

- Evolve and adapt to changes to infrastructure, apps, services, and the threat landscape
- Protect your investment in security by avoiding rust and decay
- Forces attackers to constantly level up, and expend more resources
- **Moderate Implementation Difficulty**

## Dark Web Monitoring

- Gain intelligence covering adversarial activities pertaining to your organization
- Identify credentials that have been posted on the dark web
- Identify malware compromised machines
- Early warning gives you an edge against attackers
- **Low Implementation Difficulty**

# Questions & Answers

Let's open it up for any questions you may have. I'm happy to discuss any of the topics covered today, or any aspect of incident response and security.



# Thank You

We appreciate your attention and engagement throughout this presentation on enhancing incident response and advanced threat detection for energy cooperatives.

## Key Takeaways

- Cyber attacks can result in operational disruption, financial consequences, and reputational damage.
- Safety and reliability are paramount; disruptions in services can be life-threatening.
- Advanced prevention and detection tools and well designed strategies help to build a more resilient future for the electric cooperative members.

Contact us at 919-769-2916 or [info@legioncyber.com](mailto:info@legioncyber.com) for information on how we can partner with you.

We are at your service!

