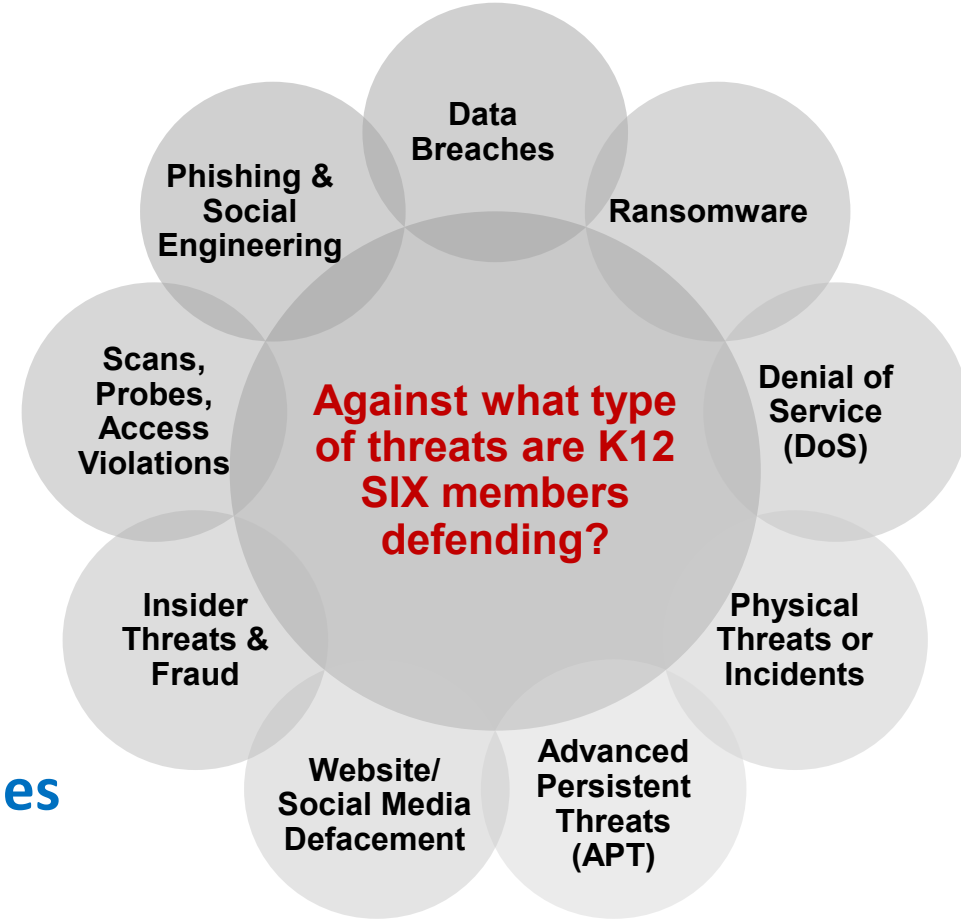
Leveraging AI to Uncover Hidden Cyber Risks at Your School

K12 SECURITY INFORMATION EXCHANGE (K12 SIX)

AUGUST 15, 2023

K12 Security Information eXchange (K12 SIX)

- A Global Resilience Federation (GRF) member community, K12 SIX is a real-time cyber threat intelligence sharing hub ***exclusively for schools***, to aid in preventing and mitigating cyber threats.
- This non-profit member community provides cost-effective collective defense by crowdsourcing security information among a vetted, trusted group of professionals with a common interest, using common technology and with supporting, independent analysis from the K12 SIX security team.



Collective defense | Best practices | Model policies
Professional development | Advocacy

https://www.k12six.org/member-benefits

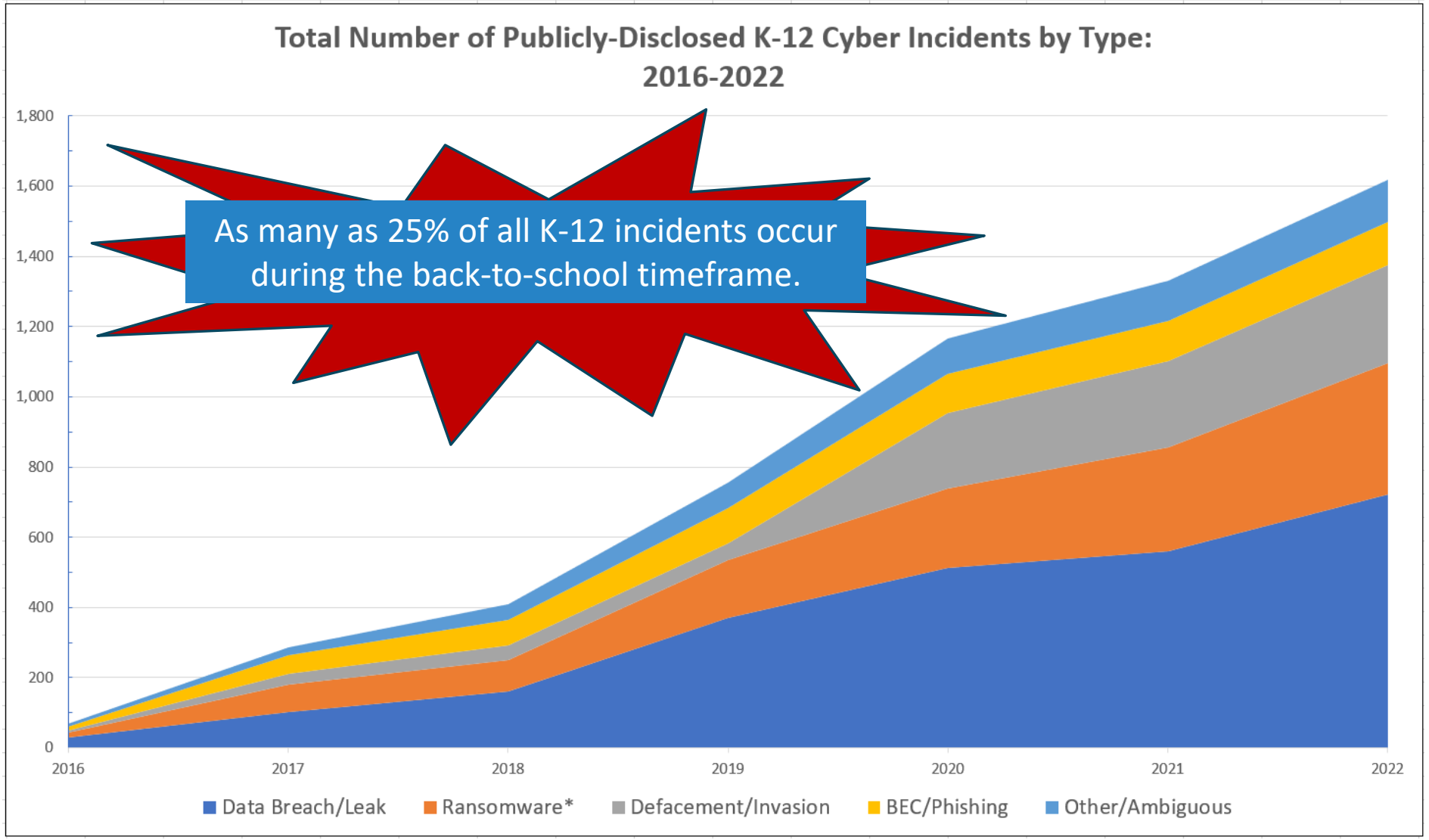
Today's Speaker

Microsoft

Corey Lee
Security CTO
US Education | Microsoft


Back
to
School

K-12 Cyber Incidents: Analysis and Trends



- Instigated by cyber criminals, students, teachers, administrators, and vendors.
- Affecting K-12 organizations of all sizes, types – in all 50 states

Source: K-12 Cyber Incident Map, K12 SIX https://www.k12six.org/map

Real-World Impacts

Case Study: Texas School District

Days before start of school, ransomware attack encrypted all of the data stored on school district servers, including multiple data backups and a few hundred district computers.

Key services inaccessible: student registration/schedules/grades/assignments (SiS), teacher communication tools, etc.

- Impacts
  - 1 week delay to school opening; community upheaval
  - 100% data loss on teacher workstations
  - Working with insurance company, paid extortion demand to restore data, re-open schools

Case Study: Connecticut School District

Saturday before a Tuesday school start, local government offices attacked by ransomware gang, affecting multiple agencies (300 servers, 3,500 computers). District did not discover issue until day of school start.

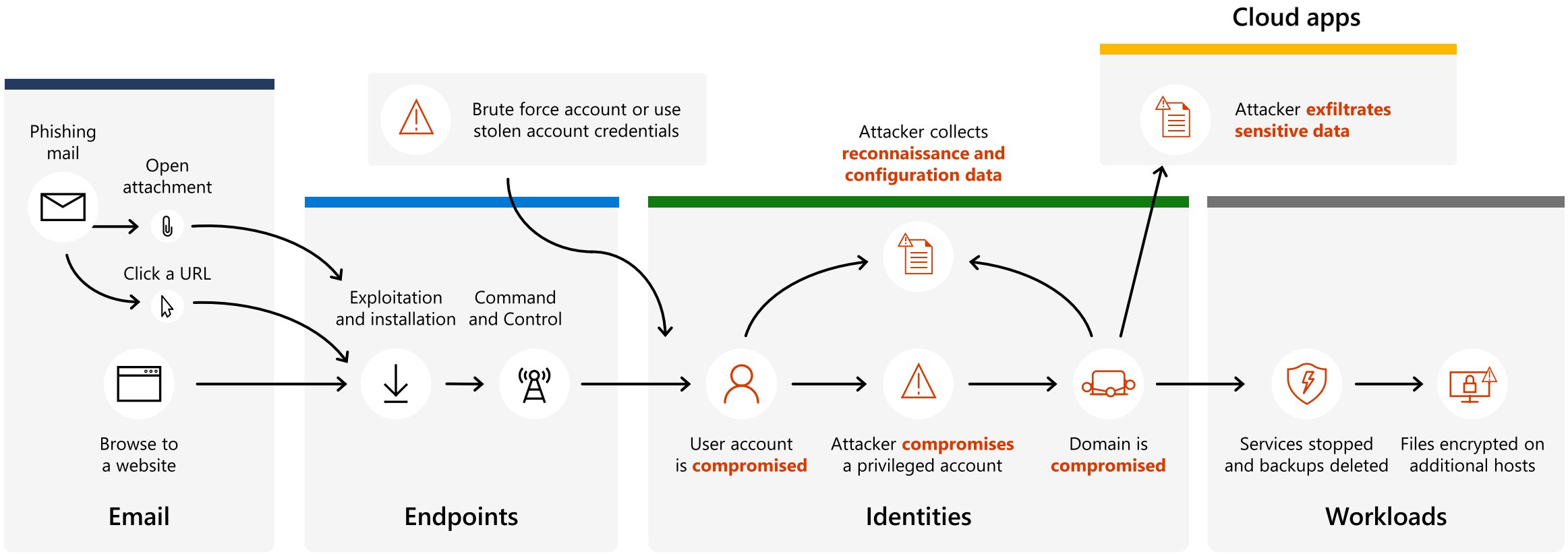
Key services inaccessible: school transportation system responsible for communicating real-time transportation routes to the district's bus company

- Impacts
  - Very late notification of school closure; community upheaval


Notes

Attacks are crossing modalities

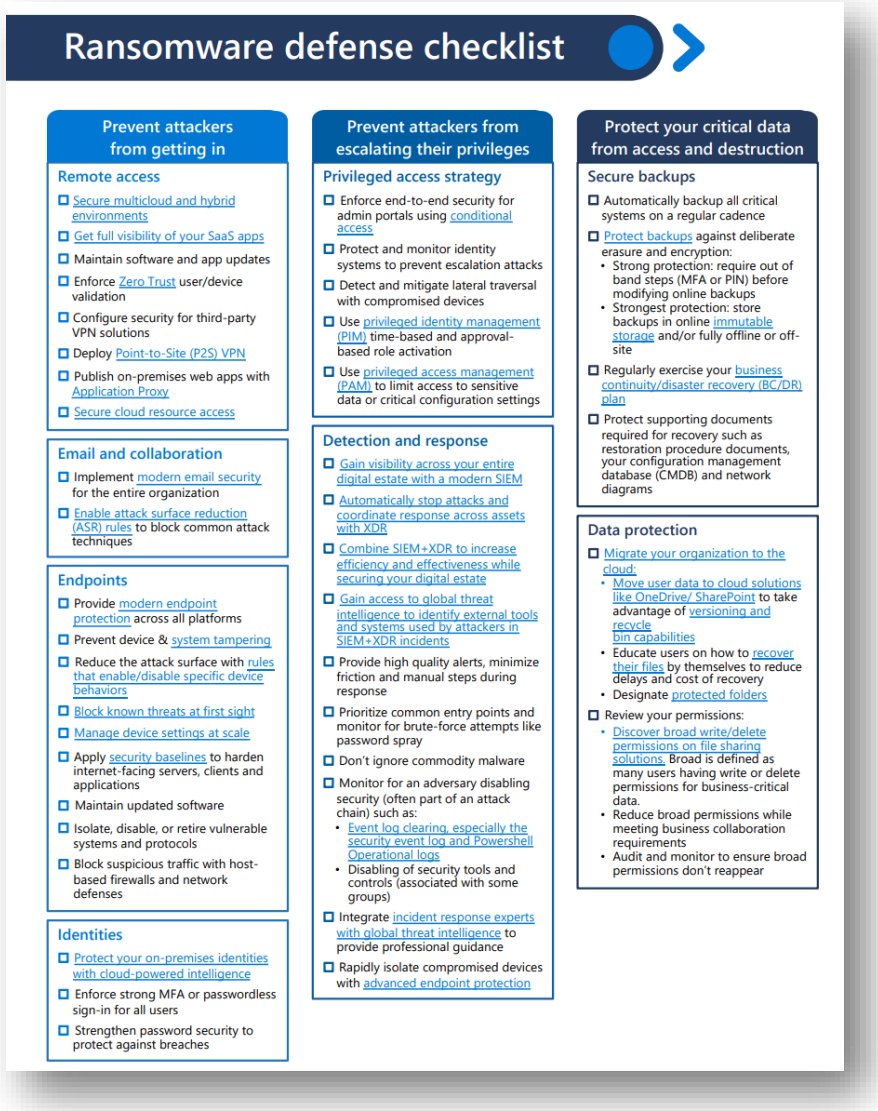
Typical human-operated ransomware campaign



AI Detection for Hidden Risks

Top 5 AI-Powered Detections

1. Credential Theft – Anomalous Tokens / Leaked Credential
2. Suspicious Identity Activity – Lateral Movement Paths
3. Suspicious Device Behavior – Disabled AV / RDP Bruteforce
4. Suspicious Application Behavior – Malicious OAuth app
5. Suspicious Data Transfer/Deletion – Ransomware Activity



Ransomware defense checklist

Prevent attackers from getting in

Remote access

- ☐ Secure multicloud and hybrid environments
- ☐ Get full visibility of your SaaS apps
- ☐ Maintain software and app updates
- ☐ Enforce Zero Trust user/device validation
- ☐ Configure security for third-party VPN solutions
- ☐ Deploy Point-to-Site (P2S) VPN
- ☐ Publish on-premises web apps with Application Proxy
- ☐ Secure cloud resource access

Email and collaboration

- ☐ Implement modern email security for the entire organization
- ☐ Enable attack surface reduction (ASR) rules to block common attack techniques

Endpoints

- ☐ Provide modern endpoint protection across all platforms
- ☐ Prevent device & system tampering
- ☐ Reduce the attack surface with rules that enable/disable specific device behaviors
- ☐ Block known threats at first sight
- ☐ Manage device settings at scale
- ☐ Apply security baselines to harden internet-facing servers, clients and applications
- ☐ Maintain updated software
- ☐ Isolate, disable, or retire vulnerable systems and protocols
- ☐ Block suspicious traffic with host-based firewalls and network defenses

Identities

- ☐ Protect your on-premises identities with cloud-powered intelligence
- ☐ Enforce strong MFA or passwordless sign-in for all users
- ☐ Strengthen password security to protect against breaches

Prevent attackers from escalating their privileges

Privileged access strategy

- ☐ Enforce end-to-end security for admin portals using conditional access
- ☐ Protect and monitor identity systems to prevent escalation attacks
- ☐ Detect and mitigate lateral traversal with compromised devices
- ☐ Use privileged identity management (PIM) time-based and approval-based role activation
- ☐ Use privileged access management (PAM) to limit access to sensitive data or critical configuration settings

Detection and response

- ☐ Gain visibility across your entire digital estate with a modern SIEM
- ☐ Automatically stop attacks and coordinate response across assets with XDR
- ☐ Combine SIEM+XDR to increase efficiency and effectiveness while securing your digital estate
- ☐ Gain access to global threat intelligence to identify external tools and systems used by attackers in SIEM+XDR incidents
- ☐ Provide high quality alerts, minimize friction and manual steps during response
- ☐ Prioritize common entry points and monitor for brute-force attempts like password spray
- ☐ Don't ignore commodity malware
- ☐ Monitor for an adversary disabling security (often part of an attack chain) such as:
  - Event log clearing, especially the security event log and Powershell Operational logs
  - Disabling of security tools and controls (associated with some groups)
- ☐ Integrate incident response experts with global threat intelligence to provide professional guidance
- ☐ Rapidly isolate compromised devices with advanced endpoint protection

Protect your critical data from access and destruction

Secure backups

- ☐ Automatically backup all critical systems on a regular cadence
- ☐ Protect backups against deliberate erasure and encryption:
  - Strong protection: require out of band steps (MFA or PIN) before modifying online backups
  - Strongest protection: store backups in online immutable storage and/or fully offline or off-site
- ☐ Regularly exercise your business continuity/disaster recovery (BC/DR) plan
- ☐ Protect supporting documents required for recovery such as restoration procedure documents, your configuration management database (CMDB) and network diagrams

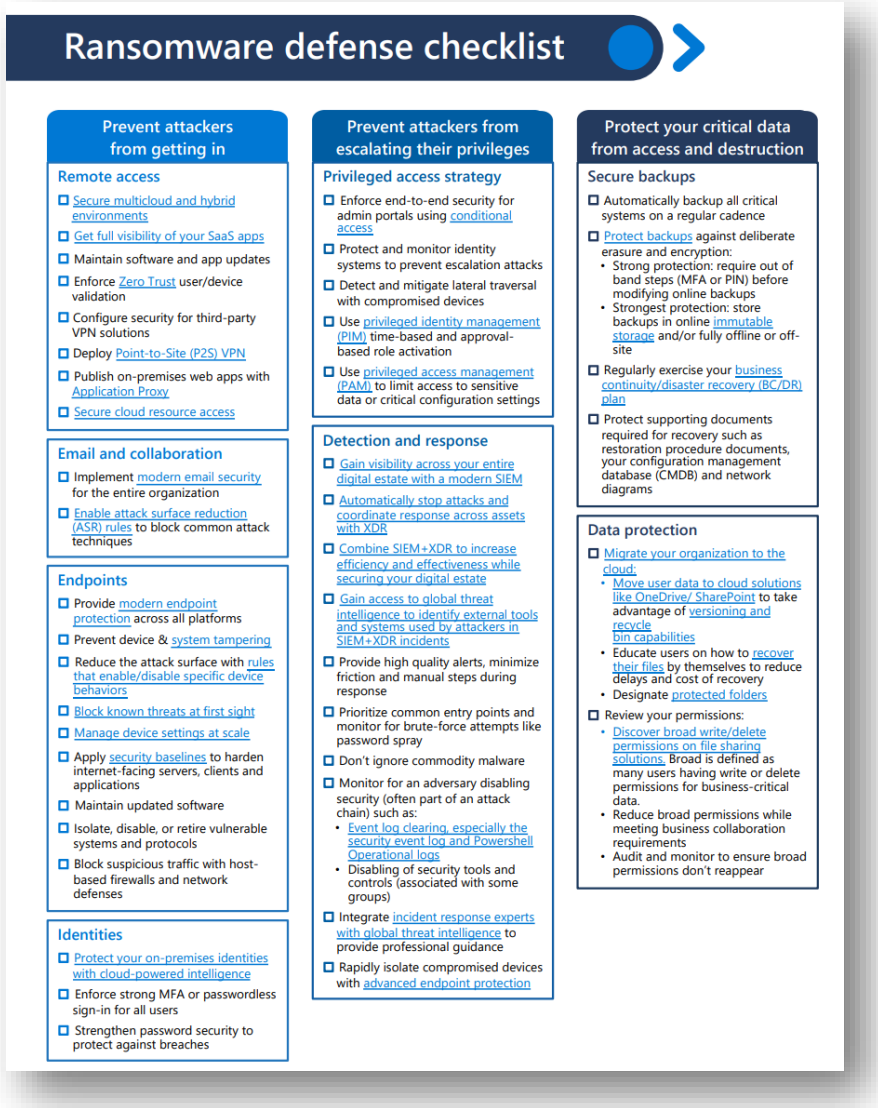
Data protection

- ☐ Migrate your organization to the cloud:
  - Move user data to cloud solutions like OneDrive/ SharePoint to take advantage of versioning and recycle bin capabilities
  - Educate users on how to recover their files by themselves to reduce delays and cost of recovery
  - Designate protected folders
- ☐ Review your permissions:
  - Discover broad write/delete permissions on file sharing solutions. Broad is defined as many users having write or delete permissions for business-critical data.
  - Reduce broad permissions while meeting business collaboration requirements
  - Audit and monitor to ensure broad permissions don't reappear

Easy Button AI Response Automations

Top 5 AI-Powered Response Actions

1. Identity Protection – Block User / Reset Password
2. Attack Disruption – Disable User
3. Attack Disruption – Device Contain
4. App Governance – Block Risky Application
5. Adaptive Protection – Dynamic Data Protection



Ransomware defense checklist

Prevent attackers from getting in

Remote access

- ☐ Secure multicloud and hybrid environments
- ☐ Get full visibility of your SaaS apps
- ☐ Maintain software and app updates
- ☐ Enforce Zero Trust user/device validation
- ☐ Configure security for third-party VPN solutions
- ☐ Deploy Point-to-Site (P2S) VPN
- ☐ Publish on-premises web apps with Application Proxy
- ☐ Secure cloud resource access

Email and collaboration

- ☐ Implement modern email security for the entire organization
- ☐ Enable attack surface reduction (ASR) rules to block common attack techniques

Endpoints

- ☐ Provide modern endpoint protection across all platforms
- ☐ Prevent device & system tampering
- ☐ Reduce the attack surface with rules that enable/disable specific device behaviors
- ☐ Block known threats at first sight
- ☐ Manage device settings at scale
- ☐ Apply security baselines to harden internet-facing servers, clients and applications
- ☐ Maintain updated software
- ☐ Isolate, disable, or retire vulnerable systems and protocols
- ☐ Block suspicious traffic with host-based firewalls and network defenses

Identities

- ☐ Protect your on-premises identities with cloud-powered intelligence
- ☐ Enforce strong MFA or passwordless sign-in for all users
- ☐ Strengthen password security to protect against breaches

Prevent attackers from escalating their privileges

Privileged access strategy

- ☐ Enforce end-to-end security for admin portals using conditional access
- ☐ Protect and monitor identity systems to prevent escalation attacks
- ☐ Detect and mitigate lateral traversal with compromised devices
- ☐ Use privileged identity management (PIM) time-based and approval-based role activation
- ☐ Use privileged access management (PAM) to limit access to sensitive data or critical configuration settings

Detection and response

- ☐ Gain visibility across your entire digital estate with a modern SIEM
- ☐ Automatically stop attacks and coordinate response across assets with XDR
- ☐ Combine SIEM+XDR to increase efficiency and effectiveness while securing your digital estate
- ☐ Gain access to global threat intelligence to identify external tools and systems used by attackers in SIEM+XDR incidents
- ☐ Provide high quality alerts, minimize friction and manual steps during response
- ☐ Prioritize common entry points and monitor for brute-force attempts like password spray
- ☐ Don't ignore commodity malware
- ☐ Monitor for an adversary disabling security (often part of an attack chain) such as:
  - Event log clearing, especially the security event log and Powershell Operational logs
  - Disabling of security tools and controls (associated with some groups)
- ☐ Integrate incident response experts with global threat intelligence to provide professional guidance
- ☐ Rapidly isolate compromised devices with advanced endpoint protection

Protect your critical data from access and destruction

Secure backups

- ☐ Automatically backup all critical systems on a regular cadence
- ☐ Protect backups against deliberate erasure and encryption:
  - Strong protection: require out of band steps (MFA or PIN) before modifying online backups
  - Strongest protection: store backups in online immutable storage and/or fully offline or off-site
- ☐ Regularly exercise your business continuity/disaster recovery (BC/DR) plan
- ☐ Protect supporting documents required for recovery such as restoration procedure documents, your configuration management database (CMDB) and network diagrams

Data protection

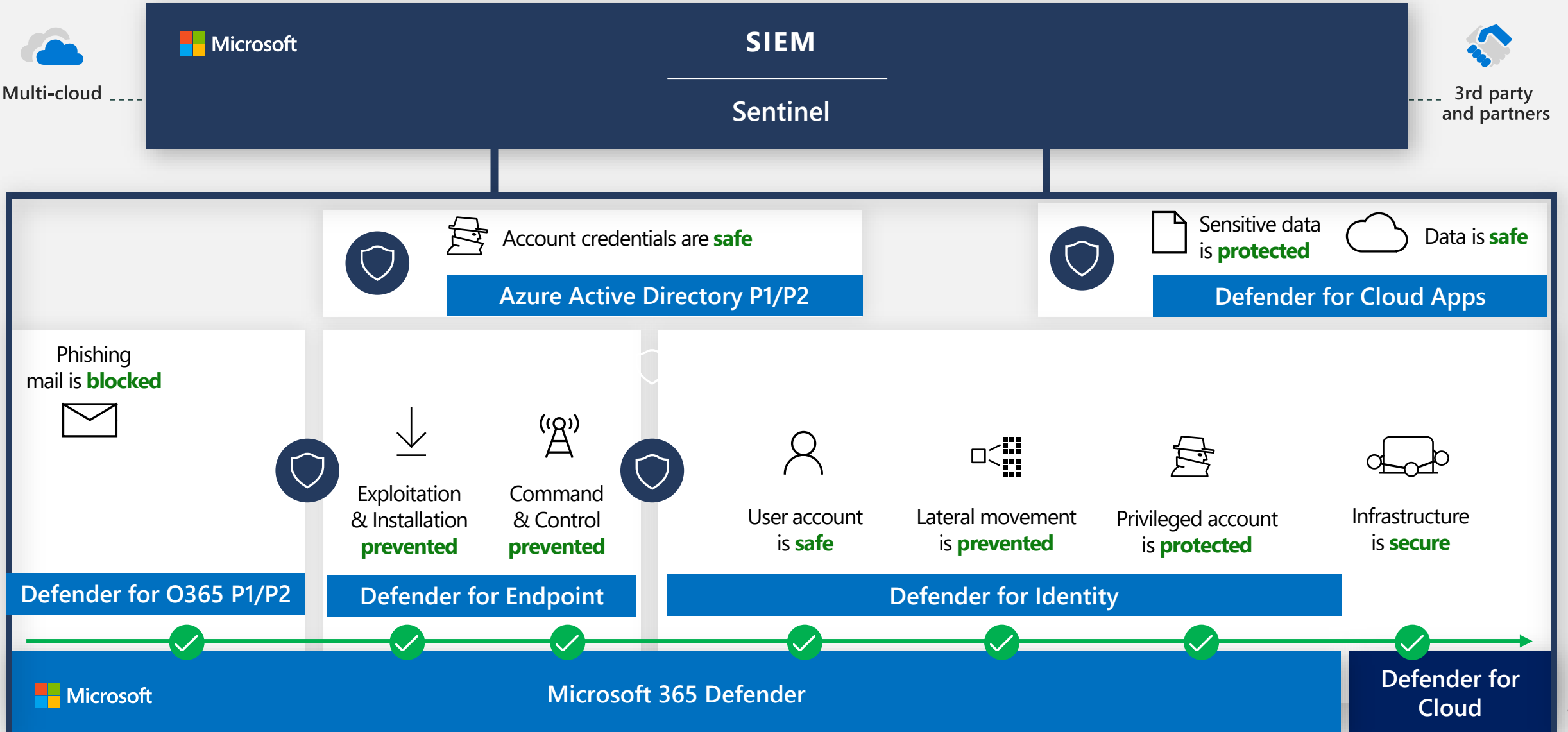
- ☐ Migrate your organization to the cloud:
  - Move user data to cloud solutions like OneDrive/ SharePoint to take advantage of versioning and recycle bin capabilities
  - Educate users on how to recover their files by themselves to reduce delays and cost of recovery
  - Designate protected folders
- ☐ Review your permissions:
  - Discover broad write/delete permissions on file sharing solutions. Broad is defined as many users having write or delete permissions for business-critical data.
  - Reduce broad permissions while meeting business collaboration requirements
  - Audit and monitor to ensure broad permissions don't reappear

Reduce cyber risk

Microsoft Security closes the gaps

Azure Services

M365 A5 Suite



Back to School Safely: Cybersecurity for K-12 Schools

Questions?

Microsoft Education Public Resources

- **K-12 Cybersecurity Awareness :** Keeping students safer with cybersecurity awareness | Microsoft EDU
- **K12 Cybersecurity Readiness:** Protect against cybersecurity risks with Microsoft 365 A5 security | Microsoft EDU
- **K12 Cybersecurity Solutions:** Digital Privacy and Cyber Security for Schools | Microsoft Education

Microsoft Security Public Resources

- Collaborate - Join the Microsoft Education Security Office Hours Community
- Protect - https://aka.ms/DisruptRansomwareNow
- Respond - Incident response playbooks | Microsoft Learn

K12 SIX Public Resources

- **The K-12 Cyber Incident Map:** https://www.k12six.org/map **and "State of K-12 Cybersecurity: Year in Review" report series** https://www.k12six.org/the-report

- **K12 SIX 'Essentials' Series:** https://www.k12six.org/essentials-series
  - Cybersecurity Frameworks: What K-12 Leaders Need to Know
  - K-12 Essential Cybersecurity Protections Series
  - K-12 Cyber Incident Response Runbook

- **2024 K12 SIX Annual Conference (Savannah, Feb 13-14, 2024)**

K12 SIX Public Resources

Webinar Series: https://www.k12six.org/webinars

- **8/29: Get to Know K12 SIX**
- **9/12: Leveraging AI to Defend Against Back to School Threats**

More TBA shortly…

- **Membership and partnership inquiries: info@k12six.org**