ALTA
American Land Title Association

ALTA inSIGHTS

REAL TIME | ON-DEMAND

A Practical Cybersecurity Roadmap for Title Agents

July 10, 2024

Today's ALTA Insights Featured Sponsor

Stavvy

Speakers

- Genady Vishnevetsky| CISO| Stewart Title
- Shawn Fox| Chief Revenue Officer| Premier One

The basics are still a MUST

- **Basic security hygiene**
  - Full inventory
  - Standardization and hardening
  - Patching
  - Standard user
- **Password hygiene**
- **Multifactor Authentication is not an option**
- **Know your surface (datacenter vs. office vs. cloud vs. SaaS)**
- **Invest in endpoints (computers) you can control**
- **Mobile device hygiene**

The Real Threat – focus on it

Unknown

Known

Modern attack vectors

- **Social engineering – your data is everywhere (no illusions)**
- **Credential attacks – password spraying**
- **Phishing and impersonation – check for email rules (frequently)**
- **Support scams – Remote Access Trojan**
- **Password reset attacks – social engineering service desk**
- **MFA attacks**
  - MFA token harvesting
  - MFA fatigue – strive for “phish-resistant” options
  - SIM swapping – (not that) new
- **Browser-based attacks**
  - Malicious browser add-ons
  - Infostealers

2024 “must have’s” on a cheap

- Assess where you are today
- Create a budget and use what you already pay for
- Designate a cybersecurity monitor/manager
- Follow a specific cybersecurity standard
  - CIS, NIST, SOC2
  - ALTA Best Practices is a good starting pointing
- Security education and awareness – supplement with phishing simulation
- MFA – NOT AN OPTION (phish-resistant)

2024 “must have’s” on a cheap

- Web proxies
- Email proxies and enhanced security tools
- Contain privileged access - password managers
- Work as a standard user
- Employee clean-up
  - Active directory
  - Dormant users
  - Role based access
- Incident response preparation and plan
- Know where to get help

2024 “must have’s” on a cheap

- Antivirus is dead, it’s your basic security
- EDR – Endpoint Detection and Response
- MDR – Managed Detection and Response
- Educate yourself and spend wisely
- TEST YOUR BACKUPS
- Hold your MSP and IT Manager accountable

19 Devices

SECURITY ANALYSIS: **SUMMARY**

Reporting Period		12 Month Service History
4,384,274	**ANALYZE** System- and User-produced metadata collected from endpoints and servers through the SNAP-Defense agent, as well as audit log data collected from Microsoft 365 through Cloud Response.	4,883,318
80,749	**DETECT** System- and User-produced metadata collected for analysis is processed and matched to threat rules to produce events, assign an event risk score, and attribute it to a threat tactic and technique.	179,500
2	**HUNT** Detected events that produce an event risk score high enough to trigger threat hunting conducted by the SOC. For example, the analyst would review and begin a full investigation.	3 Past 90 Days
0	**RESPOND** The analyst's review and investigation would lead to a response, stopping a cyberattack.	2

33	7	4,912	1,226	85	61,703
Rule Detections	Threat Techniques	Privileged Remote Activity Events	Cloud Response Events	Antivirus Events	MITRE ATT&CK® Framework Events

June 2024

Bonus

2024 – "Security on a Budget" supplement

Security Awareness

- SANS - https://www.sans.org/newsletters/ (OUCH and NewsBites)
- SANS Security Blogs (pick your interest) - https://www.sans.org/blog/
- CISA Cyber Training - https://www.cisa.gov/cybersecurity-training-exercises
- MIST Training Resources - https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content
- Amazon Learning - https://learnsecurity.amazon.com/en/index.html
- Cyber101 - https://www.cyber101.com/
- Cyber Readiness - https://cyberreadinessinstitute.org/
- Udemy - https://www.udemy.com/
- Cybrary - https://www.cybrary.it/
- eDX - https://www.edx.org/
- LinkedIn Learning - https://www.linkedin.com/learning/

Essential Security Tools

Endpoint Detection and Response (EDR) tools

- Crowdstrike Falcon Go ($4.99/device/month [min of 5 with 1Y contract]) - https://www.crowdstrike.com/products/
- Crowdstrike Falcon Pro ($8.33/device/month [min of 5 with 1Y contract])
- SentinelOne Singularity Core ($69.99/device/year [min of 5] - https://www.sentinelone.com/platform-packages/ EPP
- SentinelOne Singularity Control ($79.99/device/year [min of 5]) - EDR
- SentinelOne Singularity Complete ($159.99/device/year [min of 5]) – XDR incl [managed services]
- Huntress MDR - https://www.huntress.com/platform/managed-edr

Email Security Tools

- Sublime Email Security (free option available) - https://sublime.security/
- Abnormal Security - https://abnormalsecurity.com/products/inbound-email-security
- Huntress MDR for Microsoft 365 - https://www.huntress.com/platform/managed-detection-and-response-for-microsoft365
- Check your existing email security - https://checkcybersecurity.service.ncsc.gov.uk/email-security-check

Email Encryption Tools

- Bracket (no MX record change) by Mailprotector - https://www.mailprotector.com/encryption
- SecureMyEmail (fee/low cost) - https://www.securemyemail.com/
- ZixMail - https://zix.com/products/email-encryption

Web Security Tools

- Cloudflare SSE & SASE Platform (free version is available for up to 50 users) - https://www.cloudflare.com/zero-trust/products/#overview

- Dashlane (starts at $60/year) - https://www.dashlane.com/
- 1Password (starts at $36/year) - https://1password.com/

MFA Apps

- Authy (free) - https://authy.com/ [most universal, cloud backup]
- Google Authenticator (free) – download from Apple or Google store
- Microsoft Authenticator (free) - download from Apple or Google store

Security Keys

- Yubikey (keys start at $50 one-time fee) - https://www.yubico.com/
- Feitian (keys start at $25 one-time fee) - https://www.ftsafe.com/Products/FIDO

Logs Aggregation (SIEM)

- CISA Logging Made Easy - https://github.com/cisagov/LME

Security Subscriptions and Resources

- CISA Alerts and Advisories (subscribe) - https://www.cisa.gov/news-events/cybersecurity-advisories {subscribe for automated delivery - https://www.cisa.gov/about/contact-us/subscribe-updates-cisa}
- CISA Cyber Guidance for Small Businesses - https://www.cisa.gov/cyber-guidance-small-businesses
- CISA Free Cybersecurity Services and Tools - https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools
- CISA Shields Up - https://www.cisa.gov/shields-up

Incident Response

- CISA Incident response Training - https://www.cisa.gov/resources-tools/programs/Incident-Response-Training
- Huntress Managed Security Platform (Managed EDR, MDR for M365, Security Awareness_ - https://www.huntress.com/platform
-

Q&A

ALTA
American Land Title Association

Contact Us

American Land Title Association
Protect your property rights

- **Shawn Fox | shawnf@premier-one.com**
- **Genady Vishnevetsky | genady.vishnevetsky@stewart.com**