1. Welcome and Introductions (Jean Rikhof)
2. iUnite Security – Overview of Security Measures within iUnite (Ryan Ponto)
3. **Encryption and Database Security**
* encryption is a process that takes readable text and makes it unreadable as “cipher text”
* cipher text is sent to intended recipient (so not readable text)
* recipient has a “secret” encryption key used to interpret the cipher text

Types of encryption:

* Symmetric: when both sides use the same encryption method at the start and end
* Asyymetric: can be safer, starting encryption different from end encryption (both unique)
* Hashing: technically not encryption, a one-way transmission (hard to change cipher text back into readable data), often used for passwords (so “hashed” password is verified to be the same – but in other words the password is not known from our end)

This is what happens in our database:

* Data is encrypted as it is stored within the data (so that info pulled from a different database – not the same as where the platform information is stored)
* Data is only decrypted as there are authenticated requests
* We use these methods above to prevent physical data theft and digital data theft if the database is accessed outside of iUnite

Minimalistic Data Access:

* Database server is separate from the web server
* iUnite is granted access to the database with the fewest number of permissions possible.
* Database server can only be access with sources in the same account and region.
1. **Security Before Page Loads**

This is when you type in the URL and you hit enter, this is what happens:

**1st IP address check:** All traffic must come through the firewall. Attempts to access iUnite.ca by bypassing the firewall will get a 403 error. IP is checked against known problem, block listed and allow listed IP addresses. Anyone trying to access that does not have permission to will see, *“Forbidden. You don’t have permission to access this resource.”*

**2nd Web Application Firewall (WAF): Here** are the types of attacks it prevents.

 (1) DDos Protection – Dedicated Denial of Service attacks aim to overload a server or otherwise prevent normal function through traffic volume. (2) Bot Blocking – Known malicious or other suspicious bots attempting to access a website are blocked and denied all access. (3) Virtual Patching and Hardening – Attacks based on known exploits of outdated software on a server are prevented in transit to the server. (4) Geo blocking: Block or allow traffic based on its originated location. iUnite blocks all traffic outside Canada.

**Question:** What happens when the IP address at home is different than the IP address at work? Ryan: it is only checking if the IP address is a problem IP address.

1. **Securing During Page Loads**

Four layers of protection before actually accessing:

1. **Web Application Firewall (internal)**
2. **Automatic logout** – certain sensitive pages, will log out after a certain time (each login expires after a max of 48 hours, inactive for more than an hour logs you out)
3. **Access Permissions** – checking if you are allowed to access a page (user role checked, page/form access is checked, data access is checked before loading, DB Table access checked again before database tables are displayed)
4. **Automatic redirects** **–** are based on account permissions, if still logged in, redirect to login page, if logged out, redirect to login page.

**Question:** How often - after how many logins - does the system ask for a new password to be created? Ryan: This doesn’t happen only if you are locked out. But the system will not ask you to reset.

**Question:** Can you we use a different language word in a password? Ryan: yes.

1. **Login and Form Security**
2. **Passwords:** must be strong to be allowed, algorithm used looks for patterns, common groupings and minor modifications to words. It will consider passwords with recognizeable words make your password weak. *Note: it will take a bit of patience to create a password that the system will consider strong.*
3. **Login Obscurity:** shows the same error messages regardless if login attempt is a real account or not. Password reset does not confirm if an email was sent or not, to avoid confirming account emails or usernames. Makes it harder to hack a password if guessing at emails and usernames.

**Question:** How frequent are people trying to breach iUnite? Ryan: the occasional bot has tried.

**reCAPTHA:**

****

* Two types: invisible and checkbox
* Assesses how pieces of a website are regularly used to weed out suspicious users and bots
* Based on how user behaves on a website, a risk score between 0 (bad traffic) and 1 (good traffic) is created.
1. **Two-Factor Authentication (2FA)**
* Email code sent is unique for that account and time sensitive (5 minutes)
* To hack into an account, hacker would need to have a username or email, current password, and access to the email account.
* Future options: SMS/Text, time-based one-time password (TOTP), one touch sign-on, magic link, single sign-on (SSO)
1. **Nonces**
* A number used once to verify the form submission is from the same user that loaded the page.
* Nonces is a grouping of random characters randomly generated (i.e. 39a650fbec)
* Same nonce could possibly be used twice or more eventually but would not be the same for multiple accounts at the same time (holds for 12 hours)

**Question:** Does that mean that if I travel with my computer outside of it's usual area that I could get kicked out of iUnite? (Nonces) Ryan: By changing location it may just spit you out and ask you to relog in.

1. **Access Permissions** – checking if you are allowed to access a page (user role checked, page/form access is checked, data access is checked before loading, DB Table access checked again before database tables are displayed)
2. **Data Sanatization:** converts all submitted data to strings (text), checks for and removes code snippets (these are typically in the format of: <script>var code = something;</script>, files are scanned during upload for potential malicious code, suspicious file data, and file type mismatches (i.e. uploaded as a .pdf, but is really a .exe file).
3. **Scans, Alerts and Monitoring**
4. Three scans we have going on all the time ongoing: Malware and hack scanning, DNS Scanning, File integrity. If you have ever seen a site that suddenly redirects you or has a ton of adds, that is the type of hack that is often used to hurt companies and to try to send you to a phishing page. These scans prevent this from happening.
5. Alerts happen when: user account changes happen, website changes, security events (i.e. unauthorized form submissions) and these are monitored.
6. Monitoring: Blacklist monitoring, security logging – logins, failed login attempts, form submissions/actions taken, user account changes (add/edit/delete), password reset attempts.