HYAS

CASE STUDY

FIRST WEST CREDIT UNION SPEEDS CYBER FRAUD INVESTIGATIONS WITH HYAS™ INSIGHT

COMPANY AT A GLANCE

First West Credit Union (www.firstwestcu.ca) was formed in 2010 with roots dating back to 1946 when its original credit union brands were established. First West provides full-service financial products and solutions, both online and from over 50 branches throughout British Columbia.

CHALLENGES

- Mitigating fraud and improving incident response
- Improving analyst investigation productivity
- Gaining credibility with law enforcements and internal constituents

RESULTS

- 3X increase in analyst productivity with rapid identification of adversary infrastructure
- Board visibility and enhanced relationship with law enforcement through improved fraud mitigation and comprehensive adversary information
- Proven effectiveness and resulting risk mitigation helped justify a 3x increase in fraud team headcount

> "Investigations can be complex as you poke through cyber attacker tradecraft. HYAS helps us to save valuable time in investigations and achieve attribution. We have seen a speedup of about 3X for analysts when doing investigations with HYAS Insight."

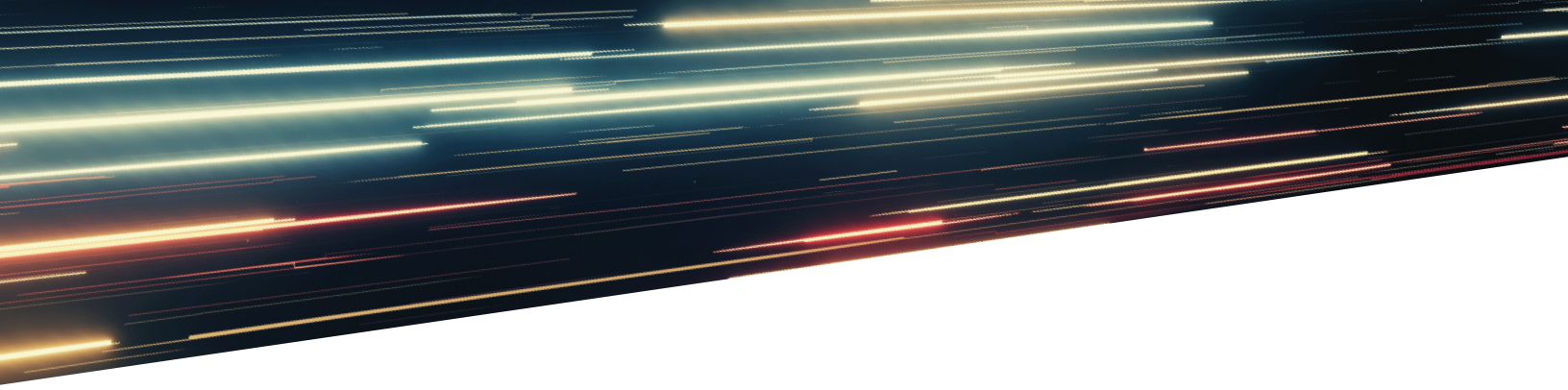
Ryan Smith
Manager of IT Security and Operations, First West Credit Union

SECURING MEMBER INFORMATION

First West Credit Union, headquartered in Langley, British Columbia, is one of Canada's leading financial cooperatives with 1,400 employees and over $11B CAD in assets. As a large financial institution, First West is under continual attack from adversaries attempting to make an illicit profit from the credit union and its members. The First West IT Security Operations team is tasked with countering the ongoing fraud attempts as well as incident response for issues affecting internal systems containing member information.

First West was re-evaluating its security threat intelligence toolset to address false positive "noise" when it came across HYAS. After seeing the quality and depth of the information HYAS Insight provided, First West realized that it also had an unsolved issue in understanding the credit union's cyber adversaries. Ryan Smith, First West's Manager for IT Security and Operations, explained, "As we evaluated our situation, we realized that we had a threat intelligence problem. We had used conventional threat intelligence for a number of years. When you use threat intelligence as much as we do, you realize that not all vendors provide trustworthy data. When it came to understanding our current threat actors, the threat intelligence platform we relied on before HYAS did not deliver adequate insights, detail, and attribution."

First West selected HYAS because of its high fidelity information that helps enable "to the doorstep" attribution, intuitive user interface, and partnerships with strategic partners like Microsoft that are significant to First West.



INVESTIGATING AND COUNTERING CYBER FRAUD

Online fraud against First West typically happens in waves with the IT Security Operations team observing clusters of events. The team makes some educated guesses about their cyber adversaries, but using HYAS Insight has enabled the team to dive deeper, faster, and achieve "to the doorstep" attribution. As Smith highlighted, "*The HYAS Insight intelligence allows us to act quickly to counter adversaries, so we typically see attacks for a relatively short period of time. Reducing the window of opportunity for threat actors reduces fraud losses.*"

Some fraud and cyber security incidents that HYAS has helped First West resolve include:

- **APT-C:** The team was able to locate an email address that was tracked back to an individual in Central America and profile the threat actor. The adversary, internally dubbed APT Carlos, established domains for phishing attacks. The adversary typically took two weeks between establishing the domains and employing them in an attack. **The advanced knowledge provided by HYAS Insight enabled First West to request the takedown of the domain for brand infringement before it was used in an attack, as well as locate and block other domains that were obviously nefarious.** "*If you have good intelligence and are able to quickly react, you can avoid significant financial damage. We had good intelligence with HYAS Insight and were able to react quickly to avoid a big fraud bill.*"

- **APT-P:** Financial institutions face adversaries that can be well-funded and sophisticated in their tactics, techniques and procedures (TTPs). First West recently encountered a growing fraud bill for reasons that could not be determined. The team puzzled over this until one day the team stumbled across a fake ad on Google Ads. The advertisement led to a compromised Wordpress site that redirected to a phishing site that mimicked the First West website. The adversaries had established their own hidden infrastructure that mimicked the First West website, and led consumers to the site through "trustworthy" Google ads. The fake phishing site was not indexed by search engines, so it was difficult to locate. "*The adversary was capturing credentials as users would click on what they thought was a legitimate ad that they could trust. They were paying for the ad clicks that led to their phishing site.* ***HYAS allowed us to investigate the phishing domains using WHOIS information and other data to identify the infrastructure and quickly shut it down.***"

The gang behind fraud was dubbed "APT-P" because it probably originated in Eastern Europe. Investigating each of the fraud incidents yielded IP address information that proved to be particularly interesting. The information provided by HYAS was able to geolocate what the First West team thought to be an open WiFi network used by APT-P. After identifying a number of potential locations apparently used by the attacker, the team identified a fraud incident originating with an isolated, rural house and visited the homeowner to ask if anybody suspicious had been lurking to use the WiFi. The WiFi network turned out to be locked, and the homeowner confirmed that the WiFi was closed and had seen no suspicious activity. After realizing that it was not open wireless, the team did some more digging and realized that the adversaries were using insecure and inexpensive DVR surveillance camera systems as a passthrough channel to attack traffic. The team was able to go to the corporate security team and block additional IPs that used the same DVR camera system. The team has subsequently identified fraud episodes that leveraged similar surveillance camera logins.

DIGITAL FORENSICS AND INCIDENT RESPONSE

The First West Security Operations team also investigates and resolves potential compromise within the credit union infrastructure. One credit union employee responded to a phishing attack and gave up their credentials. The threat actor attempted to log in from overseas using the credentials, and the user approved the two factor authentication request without much thought. This generated an alert in internal systems that locked the account. **The Security Operations team investigated the incident and was able to geolocate the adversary in Cyprus and rule out a potential false positive alert.** Commented Smith, "HYAS Insight precise geolocation enables us to distinguish between traveling employees and potential bad actors."

CLOUD-NATIVE THREAT INTELLIGENCE THROUGH A GLOBAL PANDEMIC

When Covid-19 affected the world in early 2020, First West had to adapt some of its business practices. Employees that previously worked in an office were now working from home. The First West security operations team did not miss a beat with HYAS Insight. HYAS Insight's cloud-native design fit with First West's cloud-first strategy and continued delivering the access, scalability and availability needed by First West. It also avoided issues posed by on-premises security solutions. Commented Smith, "*Covid-19 affected a lot in our lives, but it did not affect our team's productivity. We've had someone in a trailer in the mountains fishing, and able to put down their rod and jump on an investigation.* ***It does not matter where our analysts are located, they are still able to get the same intelligence.***"

ENGAGING LAW ENFORCEMENT

Getting assistance from law enforcement to take action against cyber adversaries is a challenge. While a bank robber walking into a branch with a gun can elicit a prompt law enforcement response, a "low and slow" phishing campaign may not stimulate as much interest. In the jurisdiction in which First West operates, law enforcement staff are stretched thin and frequently do not have deep cyber threat knowledge. Commented Smith, "*We regularly need assistance from local law enforcement, and that requires proving to them that we have enough intelligence to reassure law enforcement that they have a viable case. We need a dossier of information to get attention and speed the law enforcement investigation. With our last investigation, we quickly got results with a local law enforcement agency) in part because we had all of the threat intelligence that they needed to engage.*"

"*When we are dealing with law enforcement in Canada or the United States and mention HYAS, a lightbulb goes off in their heads,*" Smith said. "***Knowledgeable law enforcement partners understand the quality and precision of HYAS threat intelligence. It helps us to build credibility with law enforcement.***"

RESULTS WITH HYAS INSIGHT

First West has utilized HYAS Insight for over a year, and the product and HYAS Intelligence Services have delivered results for internal and external constituents of the security operations team. **The fraud mitigation through precise threat attribution has established credibility for the Security Operations team with First West's Board of Directors and Executive Risk Committee.** As a result, the analyst team has tripled in size over the past year as First West Security Operations people, processes and technology have proved their worth.

HYAS Insight was added to a portfolio of technologies that First West uses for fraud investigations and incident response, but has become the first tool that the Security Operation team uses when fraud or indicators of compromise require investigation. Observed Smith, "***We have a threat intelligence platform, but have found it generates significant false positives and the interface is cumbersome to use. And open source threat feeds do not yield much.*** *Employing HYAS Insight has streamlined our investigations with an easy-to-use interface and needed contextual information. One pane of glass usually gives us what we need. HYAS Insight is typically our first pivot point on new investigations.*"

First West had worked with a number of security technologies and had mixed results. In reflecting on his experience with HYAS, Smith said, "*HYAS was with us from the start. They listened to what we needed to do and worked to ensure that we were successful. Some other vendors make promises and then are not responsive after closing the sale. HYAS has delivered on its commitments. When features are promised, HYAS has delivered and helped us achieve results.*"

Summarizing the HYAS relationship, Smith reflected, "HYAS has helped us to identify our adversaries and reduce fraud. Having precise, high-confidence threat intelligence has helped our members and improved the Security Operation team's credibility with the IT leadership team, the Board, and law enforcement partners."

FOR MORE INFORMATION OR TO SCHEDULE A DEMO, PLEASE CONTACT US AT:

Email: info@hyas.com Web: hyas.com/demo Phone: +1-888-610-4927

ABOUT HYAS™

Founded by a team of world-renowned security researchers, analysts and entrepreneurs, HYAS is a highly skilled information security firm developing the next generation of information security technology. HYAS enables enterprises to detect and mitigate cyber risks before attacks happen and identify the adversaries behind them. HYAS Insight is a threat intelligence and attribution platform that improves visibility and productivity for analysts, researchers and investigators while vastly increasing the accuracy of their findings. HYAS Insight enables analysts to connect specific attack instances and campaigns to billions of historical and real-time indicators of compromise faster than ever before, bringing invaluable new intelligence and visibility to security efforts. Threat and fraud response teams use HYAS Insight to hunt, find, and identify adversaries, often down to their physical doorsteps. To learn more about HYAS, please visit https://www.hyas.com.