Recorded Future®

CASE STUDY

Recorded Future® More Than Doubles the Power of Credit Union's Security Team

Real-time intelligence from multiple outside sources drives more informed business decisions and focused action

USE CASE

Uses intelligence to gain more accurate, widely sourced insights faster and empower its team to do more in less time.

CHALLENGE

Before using Recorded Future, critical business decisions and security actions were previously based on incomplete manual research, instinct, and trust.

SOLUTION

Recorded Future Intelligence Platform:

- Brand Intelligence
- SecOps Intelligence with SIEM Integration: IBM Security QRadar
- Third-Party Intelligence
- Vulnerability Intelligence
- Threat Intelligence
- Analyst on Demand (AOD) Services

OUTCOMES

- Significantly increases the capacity of the security team without adding headcount
- Accurately scores vendors and other third parties for true security risk
- Helps Hughes Federal Credit Union and partners/vendors patch vulnerabilities at high risk of exploitation
- Integrates with their SIEM, IBM Security QRadar, for prioritized triage, improved threat correlations, and enhanced investigations
- Helps protects the credit union's brand and reputation from misuse and copyright infringement
- Forms a strong foundation for a true security culture based on real-time, trusted data from multiple sources instead of security standing in the way of company objectives

Hughes Federal Credit Union

Overview

Originally formed in 1952 Hughes Federal Credit Union serves the community of Tucson, Arizona and now has more than 166,000 members and over $1.9 billion in assets.

Hughes has a relatively small security team consisting of Cybersecurity Manager Judy Mayoral, the vice-president of cybersecurity, and a security analyst. This means much of the hands-on work is performed by Mayoral and the analyst. The fast-paced growth of the organization pushed the security team to seek out a solution that would provide them with reliable security intelligence to help them prioritize what matters. The team turned to Recorded Future Intelligence Platform to more efficiently sift through the vast amount and variety of data that pours in on a daily basis.

Deploying the solution has been a great boon to the organization, as Mayoral points out: "Recorded Future is invaluable, as it helps us determine whether something is an active threat or a past threat, something to prioritize or not give as much importance. We also use it for research purposes, such as for vendor selection and management. As the company continues to expand quickly, we need to make sure that we're staying nimble and on top of things—and Recorded Future enables us to do so."

> Much of our time is spent making educated, risk-based decisions regarding vendor contracts. This is where we lean on Recorded Future."

Accurately Assessing Vendor Risk

Hughes Federal Credit Union has numerous vendor relationships. A core piece of the organization's business is working with auto dealerships that are looking to finance customer purchases through the credit union. In fact, this constitutes about 70% of their business. Apart from auto loan-related entities, Hughes partners with solution providers, vendor management software companies, and technical vendors such as Cisco and IBM. Additionally, the credit union also evaluates companies they are looking to merge with or acquire.

As Hughes identifies new vendors they want to work with, they strive to do appropriate due diligence. "Much of our time is spent making educated, risk-based decisions regarding vendor contracts." remarks Mayoral. "This is where we lean on Recorded Future."

Prior to Recorded Future, the vendor evaluation process was largely guided by gut instinct or trust. When a vendor approached Hughes, the credit union would get to know them, get a feel for their business, and look at their security operations center (SOC) documentation or due diligence package. Based on that information, the credit union would make a decision about next steps which would include whether to escalate to a third party for a quantitative risk assessment, initiating the relationship, or opting not to pursue a business relationship.

"The piece that was missing for us in evaluating vendors was data on the stability of the company and the risk that they had out in the world. When we really started to leverage Recorded Future, we found that some vendors we conducted business with historically were high risk and compromised. For example, we discovered that their information was on the dark web. We wouldn't have known that without insights from Recorded Future. Now we can identify whether the vendor had any security problems that were publicly disclosed or revealed on the dark web," she says.

The Recorded Future Third-Party Module assigns vendors, partners, and other third parties with a numerical cyber-risk score, which eliminates the guesswork. Mayoral continuously keeps a vigilant eye on the vendors Hughes does business with, checking for breaches, potential vulnerabilities, ransomware, credential compromise, and other security challenges.

For core vendors or service providers that have direct access to the Hughes environment and would pose a risk to the business if compromised, Mayoral uses Recorded Future to track their usernames. If her team sees those usernames on the dark web, they then notify the vendors so they can conduct further investigations and remediations.

"When Recorded Future flags us that there's a problem, that's usually an indicator that we shouldn't be doing business with the vendor or that we need to exercise extra precautions when working with them," she asserts.

> Recorded Future provides us with substantial reporting and tools to see if anybody we do business with is vulnerable to Log4j attacks. Additionally, they help us to discover other indicators of compromise (IoCs) and determine whether adversaries are targeting us or attacking us."

Vulnerability Management Adds Richness to Vendor Profiles

By using Vulnerability Intelligence from Recorded Future, Mayoral and her team can determine whether the credit union's vendors and partners are vulnerable to zero-day attacks or other threats. Leveraging machine learning, Recorded Future scores vulnerabilities on their likelihood of exploitation based on real-time data from open, dark web, and technical sources. This allows Mayoral and her team to prioritize and act on vulnerabilities days before they are published in the U.S. National Vulnerability Database (NVD).

The Apache Log4j flaw, which was discovered in December of 2021, is a clear example of a zero-day vulnerability that has impacted numerous businesses across multiple sectors. It gives remote attackers the ability to commandeer a system in order to install malware, execute payloads, steal data, or damage the system. Fortunately, Hughes was well-buffered against Log4j, so they did not take a hit like many other organizations did, but the credit union was concerned about third parties potentially being victimized.

"Recorded Future provides us with substantial reporting and tools to see if anybody we do business with is vulnerable to Log4j attacks. Additionally, they help us to discover other indicators of compromise (IoCs) and determine whether adversaries are targeting us or attacking us," she says.

SIEM Integration Enriches Context and Makes Information More Accessible

An important benefit of the Recorded Future SecOps Intelligence Module is that it integrates seamlessly with IBM's Security QRadar, a Security Information and Event Management (SIEM) solution implemented at Hughes. Recorded Future feeds real-time intelligence into QRadar, giving Mayoral and her analyst the information they need to make quick, confident decisions.

As Mayoral puts it, Recorded Future "sees the outside world," helping Hughes prepare for possible threats. By bringing QRadar and Recorded Future together, Mayoral and her team have been able to enrich the overall data set in the SIEM. The SecOps Intelligence integration with QRadar enriches SIEM data with risk scores that provide context for the actual risk associated with exploitation of each Common Vulnerabilities and Exposure (CVE). Recorded Future's risk scores supplement CVSS scores to help Mayoral and her team prioritize the security patches that matter most based on the likelihood that a vulnerability would be exploited.

Thanks to the integration, Mayoral and team can build customized alerts. "For example, if internal users are visiting websites that are allowed through our firewall, but Recorded Future indicates that these URLs have a high risk score, then we get notified. That way, we can see that there could be a problem with a website and fine-tune our alerting. This gives us a good perspective on what our employees are doing and what our applications are doing—and this helps us better protect both," Mayoral explains.

Employees outside of Mayoral's immediate security team benefit from the enrichment that Recorded Future provides, too. For example, the infrastructure team uses the guidance of Recorded Future data in QRadar when executing security patching.

"More people in the organization can be touched by or can get the benefit of the intelligence just by virtue of having this integration. This makes the data understandable to them. When they see a bright red score of 78 from Recorded Future, they know there's a problem, but if the score is zero, they don't have to be concerned," Mayoral observes.

Curtailing Brand Abuse and Impersonation

Non-technical teams—such as finance, operations, and marketing—regularly make use of the Recorded Future Brand Intelligence which collects information, such as domain registration data, social media profiles, and malicious websites from its many sources. This capability helps Mayoral and her team immediately find leaked credentials, typosquat domains, brand infringements, and other digital risks.

At one point, Mayoral received an alert from Recorded Future about suspicious Bank Identification Numbers (BINs), which indicate the first six digits of a credit number. She immediately involved the fraud operations team who determined that these credit cards were live cards that needed to be shut down. They took a deeper look at that intelligence and enriched it with their own knowledge and were able to determine that these credit cards were part of a larger breach and could be published on the dark web or used by fraudsters. By putting all the pieces together, the fraud operations team prevented the affected credit union members from having any fraud on their accounts.

Similarly, when Mayoral and her team spot an email address from an executive account that has been found on the dark web by Recorded Future, they can immediately have the holder of that email address change their passwords and credentials.

The marketing department at Hughes makes use of the Brand Intelligence Module in several ways, facilitating corrective action by the security team if necessary. For example, with Recorded Future Brand Intelligence, the marketing department can see where the brand is being used and how it's being used.

According to Mayoral, Brand Intelligence has been especially insightful for phishing pages. "We are able to predict and detect when a phishing site is being spun up, and when phishing emails are coming based on the notifications and alerts from Recorded Future," she affirms.

In addition, Mayoral and her team can see whether the credit union's website code has been copied by unauthorized individuals to PasteBin, a hosting site where users can store text online for a set period of time and share with anyone and everyone. Again, if this does occur, they can decide on how to address the situation.

"If it's a true typosquatting site, I take it down, or I work with our vendors to take it down, but, if it's just an innocent brand infringement, it allows us to reach out to the violator so they can handle it their way," says Mayoral. "Recorded Future Brand Intelligence also lets us know if somebody is talking about us on social media, because we get those alerts as well. We can then follow up on comments that may be negative or damaging to our reputation."

Prior to Recorded Future, the credit union had little to no visibility into typosquatting. "Having the ability to monitor for typosquat domains has protected us so much. We've had so many site impersonations that we had to act on. Recorded Future has enabled us to detect about six typosquatting domains per year—something we could never do before," notes Mayoral.

Expert Analysts from Recorded Future Expand and Complement the Security Team

To supplement the work done by her team, Mayoral regularly takes advantage of Recorded Future's Analyst on Demand (AOD) Service. Recorded Future's highly experienced intelligence analysts can take a deeper dive into alerts that appear in the credit union's environment and provide insights into threats that are targeting financial institutions of a similar size and scope, along with incident response guidance, on-demand flash requests for particular alerts, and regular reviews and reporting.

As part of her process of preparing high-level reports for the board and cybersecurity committee, Mayoral augments the AOD reports with other data she collects, such as results of phishing simulation tests. She presents this data to executive management in order to help them understand the organization's security posture and make informed decisions about budget and resource allocations.

"Recorded Future presents our actual risk, which can be compared to our acceptable risk. This helps us gain buy-in when we need to justify expenditure of funds for additional resources, such as headcount or new tools," asserts Mayoral.

Fostering a Security Mindset

Hughes is committed to expanding security awareness among all its employees, and Mayoral is a major influencer in that effort. She conducts annual training for all employees and is especially focused on new hires, ensuring that everyone understands how critical security is and how important it is to report anything suspicious. She enhances her training curriculum with Recorded Future's web content and webinars on ransomware and other threats.

On a day-to-day level, she offers practical information to employees on why a particular website is being blocked, backed up by risk scores from Recorded Future. Quite often, employees need to go to various websites to do research not just on dealerships but also on specific vehicle makes and models to ensure proper financing. At times, this results in a visit to a malicious site. Recorded Future comes in handy when this occurs, as it provides the security team with alerts, so they can block those URLs.

"When a website isn't accessible, I can show users that it has a high risk score of 79 out of 100, and it's been known to have phishing or malware associated with it. That way, I can offer justification for what we're doing. And we can do the same thing with vendors as well if a user is looking to establish a business relationship with a particular company," she relates.

She assists users with due diligence or vendor management program processes by using the Third-Party Intelligence Module to look up company risk scores.

Recorded Future has helped Mayoral and her team serve as trusted and helpful facilitators. They have been successful in their efforts to change the way employees view security at Hughes. Users have come to understand that her team is not letting security get in the way of processes. Mayoral has won the hearts and minds of employees to such an extent that they are now conscientious about reporting problems to her team, such as malicious sites or socially engineered phishing emails.

Automation Leads to Augmentation of Team Capabilities

As Mayoral states, “Recorded Future has more than doubled the capacity and effectiveness of my team.”

Recorded Future SecOps Intelligence provides ready-to-use, high-confidence threat data eliminating the need to perform manual research. Armed with real-time risk scores and indicators of compromise (IoCs), her team can quickly eliminate false positives, prioritize alerts, and do deeper investigations followed by triage where required.

Recorded Future Vulnerability Intelligence has also automated processes. In the past, reviewing vulnerability scans was an exceedingly time-consuming job. Mayoral’s team had to review every single CVE in conjunction with the critical asset scanned, such as firewalls and Microsoft Windows tools. Recorded Future pairs CVEs with their associated assets, so it’s easy to see which CVEs may be high risk for any given asset.

“Recorded Future does a lot of the work for us. I don't have to drill into each and every single CVE and determine its risk or likelihood of exploitation. And because it ties the CVE and risk level back to the asset, I can decide whether it’s necessary to take action or not. This keeps us from wasting time deciding whether a vulnerability is something we need to be paying attention to based on the asset it's coming from,” says Mayoral.

Additionally, the depth and breadth of intelligence in Recorded Future helps the team more quickly and easily pinpoint risky sites. Rather than manually filtering through dozens of websites, they simply enter the URL into Recorded Future and immediately get a risk score.

“When we do have an incident or need to research something, we're able to have one person handle the issue. And this individual doesn’t have to be skilled in multiple different systems. They only need to understand IBM Security QRadar, which gets all of the Recorded Future intelligence and delivers context and helps connect the dots. We can then make educated decisions as to whether something is actionable or a false positive—and that allows us to better prioritize our time.”