CUSTOMER CASE STUDY:

Educational Institution Schools Threats with Anomali

ANOMALI

CHALLENGE

To defend against cyberattacks, this public university deployed dozens of disparate software and hardware technologies ranging from basic firewalls to honeypots. Included in the mix are education and awareness programs along with IT and staff support augmentation. It soon became evident to the cybersecurity operations team that it needed to massively improve its ability to access and operationalize threat intelligence from outside the organization, as it had no way of knowing if it was detecting and blocking all of the threats it faced.

SOLUTION

Anomali ThreatStream, the market-leading threat intelligence platform (TIP), serves as the foundation of the school's threat intelligence program. The university also relies on multiple integrations with leading malware sandboxes, endpoint protection solutions, and other controls to accelerate investigations and response. The public university is especially impressed with Anomali dashboard features, which allow it to see specifically what intelligence it is ingesting and integrating across its security infrastructure.

RESULTS

- Faster, more accurate threat detection and alerting
- Reduced malware infections
- Successful blocking and detection of ransomware
- No data breaches, to date
- 200+ Point BITSIGHT rating increase
- 50% reduction in cybersecurity insurance costs
- Complete visibility over all threat intelligence

> *"Within the existing system we'd set up, we had no control over the intelligence that was in use. Without 100 percent visibility over our intel, we had no way of knowing whether or not we were missing the worst threats coming at us. We needed to find a way to improve detection, response, and alerting without having to invest in expensive upgrades across our security stack. We saw Anomali as a way to achieve these goals," said the institutions CISO.*

OVERVIEW

The university is a master's-level institution with a spirited community of over 8,200 students and 1,000 faculty. It has a rich American Indian history and is one of the safest campuses in the educational system. With small class sizes, a low student-faculty ratio, and one of the most diverse campuses in the nation, it's a growing university that empowers students to live vibrant, fulfilling lives. With threat actors always looking for ways to monetize ransomware, stolen data, and fraud, the organization's security team is acutely aware that its vast and diverse community combined with the new remote work and learning reality fits the profile of a cybercrime target. With only a small cybersecurity team overseeing the institution, the university recognized that it needed to augment its talent and expertise with advanced cybersecurity solutions and effective processes.

UNIVERSITY CHALLENGE

The University experiences an average of 730,000 cyber intrusion attempts and several hundred thousand inbound emails daily. To defend against attacks, it had built a security stack made up of dozens of disparate software and hardware technologies ranging from basic firewalls to deployed honeypots. Included in the mix of threat mitigation and detection tools were education and awareness programs along with IT and staff augmentation.

It soon became evident to the cybersecurity operations team that it needed to massively improve its ability to access and operationalize threat intelligence across its security infrastructure, as it had no way of knowing if it was detecting and blocking the relevant threats it faced.

THE ANOMALI SOLUTION

The University turned to Anomali ThreatStream, the market-leading threat intelligence platform (TIP), which integrates and manages commercial, open-source, and ISAC feeds, to serve as the foundation of its threat intelligence program. It also relies on multiple integrations with leading malware sandboxes, endpoint protection solutions, and other controls to accelerate investigations and response. The University is especially impressed with ThreatStream dashboard features, which allow security operations workers to see specifically what intelligence it is ingesting and integrating across its infrastructure.

With Anomali, the company was able to start executing quickly. TIP deployment was fast, threat feed aggregation was easy, and IOC collection began almost immediately. The University found that it was conducting faster investigations and creating threat intelligence that could be operationalized into existing security controls for automated and immediate detection and blocking across its environment.

Within the education sector, some threats and processes are more relevant than others. Of extreme concern is the prospect of not being able to respond quickly to ransomware campaigns and phishing attacks, not having the ability to build and block a list of malicious IP addresses, or of being delayed during an investigation.

THE ANOMALI IMPACT

Prior to Anomali, the university's cybersecurity operations team had no way of knowing if it was receiving and integrating relevant threat intelligence needed to detect and block threats it was facing. With ThreatStream, the university has been able to expand the universe of IOCs it has access to, aggregate them into a single platform, and then operationalize them to conduct faster and more accurate investigations and to increase its security controls' detection and blocking capabilities.

With Anomali, the university has achieved numerous, measurable results. It has increased its BITSIGHT security rating by more than 200 points, managed to avoid being breached, successfully detected and blocked ransomware attacks, lowered help desk costs by reducing its malware infection rate, and cut its cybersecurity insurance premiums in half.

"The overall improvement we've experienced has been the result of all of our efforts, programs, and tools in use. Anomali has helped us to super charge our operations to not only speed how quickly we can identify and respond to threats but also to optimize the value of existing security investments. We've been extremely pleased with the results we are getting from Anomali, the performance we've received from the solution combined with excellent customer support has given us reason to be confident in our ability to defend the university against current and future threats," concluded the CISO.

> *"We are responsible for the cybersecurity of 10,000 on-campus users, 30,000 alumni, 70,000 digital records, and more than 60,000 connected devices. With Anomali, we can see and control available IOCs, which helps us to ingest and operationalize key threat intelligence that helps to address priorities," stated the CISO.*

ABOUT ANOMALI

Anomali is the leader in intelligence-driven extended detection and response (XDR) cybersecurity solutions. Anchored by big data management and refined by artificial intelligence, the Anomali XDR platform delivers proprietary capabilities that correlate the largest repository of global intelligence with telemetry from customer-deployed security solutions, empowering security operations teams to detect threats with precision, optimize response, achieve resiliency, and stop attackers and breaches. Our SaaS-based solutions easily integrate into existing security tech stacks through native cloud, multi-cloud, on-premises, and hybrid deployments. Founded in 2013, Anomali serves public and private sector organizations, ISACs, MSSPs, and Global 1000 customers around the world in every major industry. Leading venture firms including General Catalyst, Google Ventures, and IVP back Anomali. Learn more at www.anomali.com.