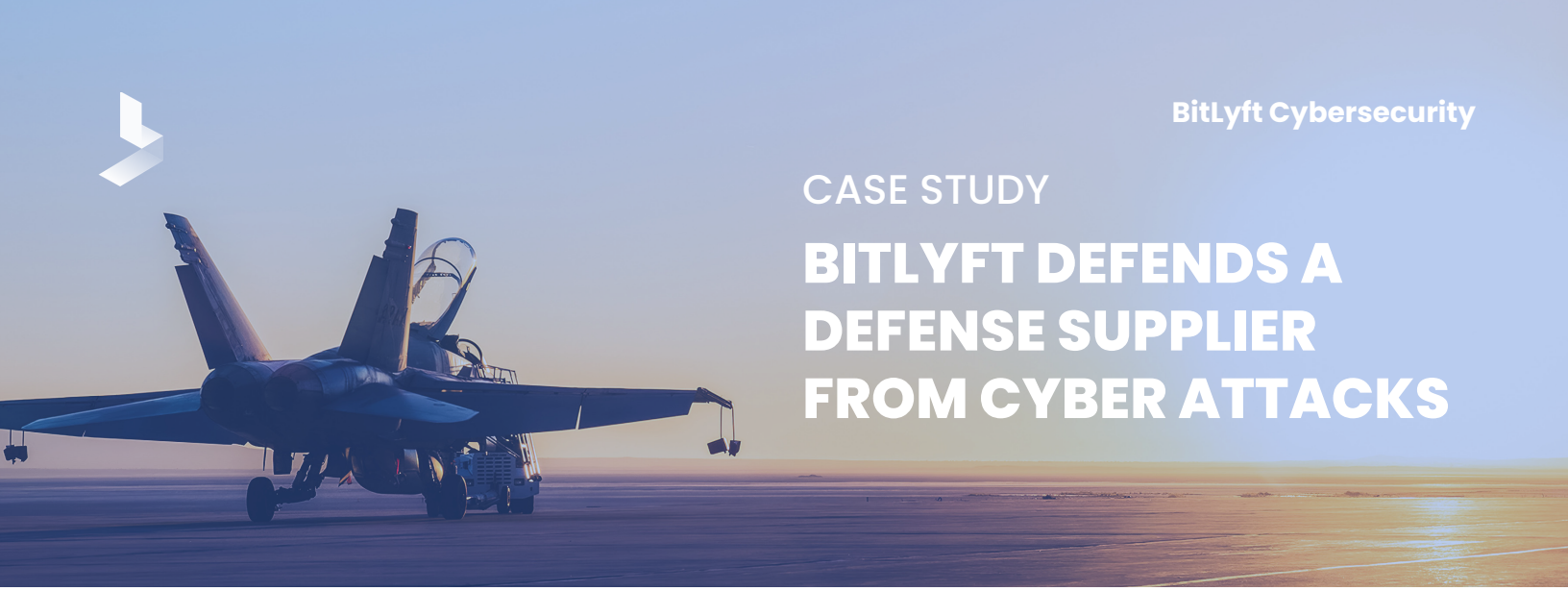

BitLyft Cybersecurity

CASE STUDY

BITLYFT DEFENDS A DEFENSE SUPPLIER FROM CYBER ATTACKS

AT A GLANCE

Challenges

- Implementing technologies to automate work
- Strengthening existing infrastructure
- Creating plans to identify security issues
- Positioning people and creating policies in case a breach ever were to occur

Outcomes

- Identified log sources and locations
- Detected and remediated unwarranted access in the network
- Fixed misconfigurations in existing security stack
- Created future security protocols and practices

"We know BitLyft is in the background watching and waiting, monitoring threats."

Kyle Smith, General Manager
UMBRAGROUP

THE SITUATION

Protecting an organization from a cyber attack is an important objective for businesses of any size and industry. But when your primary functions include manufacturing parts to keep the country safe and handling controlled, unclassified information—suddenly the weight of responsibility takes on a whole new level.

This level of liability was true for UMBRAGROUP, the world's leading manufacturer and supplier of ball screws for the Department of Defense. With plants located in Italy, Germany and the United States, this manufacturing corporation for the aeronautics sector knew it needed to find an innovative solution to protect its state of the art operations and equipment.

"MEN AND WOMEN THAT DEFEND OUR COUNTRY RELY ON OUR PRODUCTS TO WORK," SAID WENDY CUNNINGHAM, TRADE COMPLIANCE OFFICER AT UMBRAGROUP.

Despite the weight of these responsibilities and tremendous workload, UMBRAGROUP only had a small security team to achieve their extensive goals. Some of their immediate objectives included:

- Implementing technologies to automate their work,
- making sure their infrastructure was strong enough,
- Creating a plan to identify security issues, and
- Making sure they had the right people in place in case a breach ever were to occur.

(MORE)

THE SOLUTION

With these responsibilities in mind, UMBRAGROUP decided to bring on BitLyft as another asset to help strengthen and protect their growing infrastructure.

"Being a Michigan company was one of the first advantages of partnering with BitLyft," said Joe Sheridan, US Director of IT at UMBRAGROUP. "We'd be giving back to Michigan."

Once on board, BitLyft's team of cybersecurity consultants went to work by completing its onboarding process which includes a kickoff call and implementation of tasks outlined by BitLyft's security team.

"One of the first items we tackle in our onboarding process is to identify the location of a company's log sources," said Mike Skeith, Director of SOC at BitLyft. "UMBRAGROUP had not yet identified all the locations of its logs, and this was causing a critical lack of visibility within the network."

After this initial finding, BitLyft continued to scour the company's network for other areas needing improvement. Another item flagged by BitLyft's security team was several misconfigurations within the company's Microsoft Office 365's security settings.

"O365 has numerous known security vulnerabilities," said Skeith. "Our team has a firm grasp on these issues and was able to quickly identify and iron out those configuration mishaps."

The onboarding phase is one of the most critical components of BitLyft's work with its clients, but the relationship doesn't stop there. BitLyft's Next-Gen Extended Detection and Response (XDR) technology monitors network traffic 24/7, provides updated threat intel and provides the lightning fast speed that can only come from automation.

> "One of the most beneficial aspects about working with BitLyft is having access to our engineers. We're not just analysts who watch logs all day. We are engineers who are able to build, develop and manage ongoing software enhancements for our clients."
>
> **Mike Skeith, Director of SOC, BitLyft**

In addition, its security staff are trained to easily identify malicious behavior and are available to assist clients whenever needed.

"On one particular occasion our team identified successful logins from an inactive account," explained Noah Hoag, SOC Team Lead at BitLyft."We immediately alerted UMBRAGROUP once we discovered this unwarranted access. Without us monitoring their environment, this activity very easily could have turned malicious."

BitLyft not only worked with UMBRAGROUP to rectify the situation and remove the compromised account, but they also continue to work with the team to create future security protocols like resetting computers upon the departure of employees.

"One of the most beneficial aspects about working with BitLyft is having access to our engineers," said Skeith. "We're not just analysts who watch logs all day. We are engineers who are able to build, develop and manage ongoing software enhancements for our clients."

"We know BitLyft is in the background watching and waiting, monitoring threats," said Kyle Smith, General Manager at UMBRAGROUP. "They let our team know as soon as they detect any threats and are able to shut it down."