opentext™ | Cybersecurity

Case Study

Bernicia Homes

ArcSight Intelligence for CrowdStrike provides deep cyber intelligence insight to proactively prevent attacks and educate users.

Who is Bernicia Homes?

Bernicia Homes has been providing quality homes and services to people in the Northeast of England for over 50 years, earning a reputation as one of the country's leading housing associations. Housing associations are not-for-profit landlords that provide homes and support for approximately six million people all around England.

Cybersecurity is a Top Priority for Bernicia

Managing sensitive data for over 60,000 customers means that cybersecurity is identified as a high risk for Bernicia. The process aims to collectively identify, analyze, and solve risks before they become problems. Adam Watson, Head of Security and Infrastructure at Bernicia, explains further: "Cybersecurity sits right at the top of our risk register. This shows how aware we are at all levels of the organization of the potential reputational damage that can result from a security breach of any kind. We have implemented a range of cybersecurity measures, but in recent years attacks have become so much more sophisticated. We felt we needed a proactive approach to prevent falling victim ourselves. We were particularly interested in raising the visibility in our environment so that we can detect lateral movement and potential suspicious behavior."

> "ArcSight Intelligence gives us the tools and the peace of mind to know we can protect our customers and employees against malicious intent."

Adam Watson
Head of Security and Infrastructure
Bernicia Homes

Adam explored the market and evaluated six potential solutions, including ArcSight Intelligence. ArcSight Intelligence provides advanced threat detection, supported by sophisticated AI and unsupervised machine learning. Through advanced baselining, ArcSight Intelligence builds risk profiles around each user, machine, URL, and entity, learning the organization's 'unique normal.' ArcSight Intelligence distills billions of security events into a few high-quality threat leads for further investigation.

ArcSight Intelligence Delivers Targeted Threat Leads

Bernicia runs a Virtual Desktop Infrastructure (VDI) within a private cloud environment. Adam particularly likes the fact that ArcSight Intelligence offers direct integration with CrowdStrike. He comments: "Our CrowdStrike Falcon platform provides rich security data, which ArcSight Intelligence repurposes to

BERNICIA

At a Glance

Industry

Services

Location

United Kingdom

Challenge

Protect customer's personal identifiable information against data exfiltration by proactively detecting and swiftly responding to potential anomalous behavior

Products and Services

ArcSight Intelligence for CrowdStrike

Success Highlights

- 100+ million security events distilled to a handful of targeted threat leads
- Seamless integration with CrowdStrike for a zero-footprint cloud deployment
- Data visualization to easily spot trend development
- Improved processes in high-risk applications
- Nuanced behavioral analysis to detect lateral movement and data exfiltration

> **"ArcSight Intelligence highlighted interesting behaviors in some of our applications that provided valuable intelligence. Having a deep insight into how our staff use the environment gives us the opportunity to spot anomalous behaviors and hopefully stop a malicious actor in their tracks."**
>
> **Adam Watson**
> Head of Security and Infrastructure
> Bernicia Homes

find sophisticated anomalies which would otherwise go unnoticed. We did not have to worry about deploying more endpoint agents, as the CrowdStrike data was already there in the cloud, giving us a zero-footprint deployment option. We simply set up the integration with ArcSight Intelligence in the CrowdStrike store."

Over a proof of concept of 45 days, ArcSight Intelligence analyzed over 100 million security events from hundreds of endpoints. The management of this data is where ArcSight Intelligence stood out from the competition, as far as Adam was concerned: "ArcSight Intelligence gave us a user-friendly interface that makes it easy to find the information we need. We are a small team, and the cybersecurity threat hunting service that complements ArcSight Intelligence was invaluable to us. We received an executive report with a manageable number of qualified potential anomalous behaviors. The data was presented visually, and it was very easy to spot trends over a period of time. Upon closer investigation, we thankfully found nothing serious and certainly nothing malicious, but ArcSight Intelligence highlighted interesting behaviors in some of our applications that provided valuable intelligence. Having a deep insight into how our staff use the environment gives us the opportunity to spot anomalous behaviors and hopefully stop a malicious actor in their tracks."

Comprehensive Threat Hunting Reduces Alert Fatigue

Following the successful proof of value, the Bernicia team seamlessly transitioned into production with ArcSight Intelligence. Adam and the team were introduced to the cybersecurity threat hunting team and agreed on a working practice going forward. A weekly touchpoint discusses high-level findings, while a workflow was set up to manage critical alerts that need to be actioned by Bernicia straight away. ArcSight Intelligence will detect, connect the dots, and visualize an attack path. With this context, ArcSight Intelligence can highlight attacks as they unfold. In this case, Bernicia is immediately alerted with incident visualizations and workflows to enable efficient validation, investigation, and response. Adam comments: "ArcSight Intelligence gives us the tools and the peace of mind to know we can protect our customers and employees against malicious intent."

He concludes: "Today, the risk of a compromised user account or a sophisticated cyberattack is higher than ever before. ArcSight Intelligence complements our existing cyber defense solutions perfectly and is exactly what we need right now. The comprehensive threat hunting service reduces alert fatigue and enables us to focus our resources."

Connect with Us
www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.