AT&T Threat Hunting Program

A proactive approach to countering cybersecurity attacks

Benefits

The AT&T Threat Hunting Program is designed to help your business:

- Establish a threat hunting process and lifecycle
- Create a hunting schedule
- Scope the hunt: identify objectives, outcomes, and data sources
- Encourage junior staff to participate
- Establish metrics and success criteria
- Document the hunts and the lessons learned
- Identify and address visibility and capability gaps

A new approach to cybersecurity

Unlike most cybersecurity countermeasures, the AT&T Threat Hunting Program goes on the offensive to track down infiltrations. By evaluating existing security vulnerabilities, the AT&T Cybersecurity Consulting Team adopts a hypothesis-based approach to testing weaknesses and eliminating threats.

The cybersecurity threat landscape presents businesses with evolving challenges. Ransomware attacks on are the rise and destructive malware continues to disrupt business operations. Better tools are required to minimize damage caused by increasingly sophisticated techniques.

AT&T Threat Hunting Program is a combination of strategies and proactive countermeasures that help businesses identify security weaknesses and reduce the time unauthorized users go undetected. The key lies in its unique strategic approach to anticipating and identifying vulnerabilities and verifying infiltrations. Threat hunting is the proactive analysis of network and system artifacts to identify suspicious, malicious, and unusual activity that is otherwise ignored by detection technologies. It's not a technology or a tool, but a set of protocols and methodical approaches that helps businesses lessen the impact of unauthorized access to critical systems and data.

By evaluating a business's network and cloud resources, the AT&T Threat Hunting Program formulates hypotheses about which resources are most at risk, then examines those assets to determine whether unathorized users have indeed penetrated security measures. These insights are then collected and used to refine future hypotheses and improve the prediction process. The goal is to intercept unauthorized access and limit the time users spend undetected, a factor known as dwell time.

A goal-based method for minimizing dwell time

The Threat Hunting Program team begins each project by examining the existing environment, including people, processes, and capabilities. These efforts start with interviews with stakeholders and include collecting documentation concerning requirements, standards, current state, and future state goals for the AT&T Threat Hunting Program. The team then performs an assessment of an organization to help formulate hypotheses about which assets are most vulnerable to attack.

The assessment includes:

- Threat profile and industry vertical
- Business risk identification related to cyber threats
- Threat intelligence sources and applications
- Enterprise visibility

Once the initial assessment is completed, AT&T Cybersecurity begins work on developing the individual organization's Threat Hunting Program. This includes a program framework, processes, and procedures for establishing a Threat Hunting lifecycle. At the conclusion of each engagement, the team issues a report documenting the overall program, capabilities, and outputs.

These documents will help the organization perform the following security goals:

- Integrate threat hunting into their overall security program
- Establish a threat hunting cadence and reporting
- Develop dashboarding, reporting, and KPIs to measure effectiveness
- Knowledge transfer

Discover how the AT&T Threat Hunting Program can enhance your cybersecurity. Contact your service representative for additional information.

About AT&T Cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.