VARONIS UBA THREAT MODELS

Varonis User Behavior Analytics (UBA) threat models analyze and detect suspicious activity and prevent data breaches – using deep analysis of metadata, machine learning, and advanced UBA.

WHY VARONIS USER BEHAVIOR ANALYTICS?

- Defend your data against cyberattacks, ransomware, insider threats, and more
- Get meaningful insights into user and data patterns, security risks, and social connections
- Build context around the content of data and activity with collected metadata
- Monitor critical assets for suspicious activity and unusual behavior
- Reduce the amount of time it takes to find and assess a real issue, with forensics on compromised assets
- Integrate with SIEM and other UBA systems
- Recover from potential security breaches more quickly

HOW DOES IT WORK?

Varonis addresses security issues and automates threat detection with threat models that map suspicious activity to a kill chain, and monitor and alert on attacks through the entire lifecycle of a breach.

Reconnaissance: Attackers scope the system, looking for vulnerabilities and intel.

Intrusion: malware and other dangerous files are sent to the system to gain entry.

Exploitation: Perimeter security is breached; the attackers get into to the system and install additional malicious tools.

Privilege Escalation: Attackers gain elevated access to resources, getting even further into the system with added privileges.

Lateral Movement: Credentials are compromised, the attackers are now moving between systems.

Obfuscation (anti-forensics): Attackers mask their activity to avoid detection.

Denial of Service: Network and data infrastructure is targeted, resources become unavailable for legitimate users.

Exfiltration: Data is moved out of the system for potential release and further exploitation.

WHAT CAN YOU DO WITH VARONIS UBA THREAT MODELS?

- Find things that don’t belong: exploitation tools, ransomware, crypto intrusion, and more
- Monitor for suspicious activity, including unusual access to sensitive data and abnormal user behavior and file activity
- Track attempts to damage system infrastructure
- Analyze policy changes, membership changes, and account modifications to protect against potential exploitation

VARONIS UBA THREAT MODELS DETECT AND FIGHT BACK AGAINST:

- Insider threats
- Outsider threats
- Malware activity
- Suspicious behavior
- Potential data breaches
- Compromised assets