Identity Threat Detection and Response with Clear Skye + ServiceNow

Identity Threat Detection + Response (ITDR) is an Essential Line of Defense

Identity is the foundation of access management, due to the decreasing importance of the perimeter, making visibility into identity-related attack activity one of the most essential lines of defense.

Traditional Identity Governance and Administration (IGA) solutions focus on authorization and governance – making sure the right people have access to the right resources, which helps guard against overprovisioned access that can expose credentials to an attacker.

But taking the data created by Clear Skye IGA's identity lifecycle management processes, and analyzing patterns, provides visibility into potential identity-related attack activity. This provides a powerful method of intrusion detection.

Clear Skye + Security Incident Response = ITDR Capabilities

Clear Skye's identity warehouse data resides natively on the Now Platform, coupled with ServiceNow's Security Incident Response application, unlocks Identity Threat Detection and Response capabilities.

Chris Krebs, former Director of the Cybersecurity and Infrastructure Security Agency (CISA) has been on the speaking circuit stressing that the true crown jewels of any company are identities and credentials. For example, one of the most vulnerable environments is Active Directory – which is involved in 90% of the attacks investigated by Mandiant.

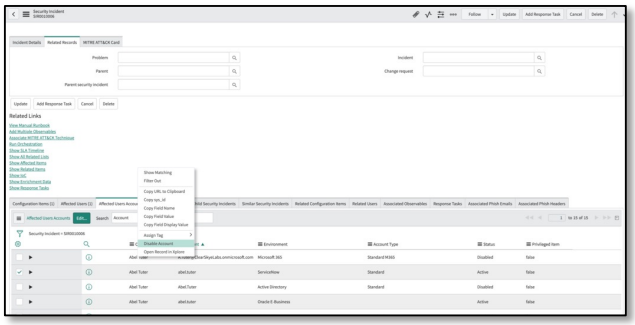
According to Krebs: "It is about identity lifecycle management. It's about good hygiene steps, it's about detection, it's about response, it's about cultivating from cradle to grave the identity. You don't want to be the Ronco oven of security services. It's not set it, forget it. It's constant monitoring, detection and management of identity."

Clear Skye IGA + ServiceNow SecOps

How Clear Skye Enhances ServiceNow SecOps Capabilities

- Augments security incidents with identity context
- Expedites remediation of incidents with just-in-time access
- Mitigates risk of incidents by disabling and selectively restoring access
- Attaches audit evidence for security incidents that includes identity actions and remediations

Harness Clear Skye's identity information + ServiceNow's security playbooks to identify malicious attacks such as ransomware or risky access that may be exploited to exfiltrate data



Identity data belongs on the Now Platform

With Clear Skye, you can build the following into your Security Incident Response processes using native ServiceNow functionality.

Identity Security Orchestration, Action & Response (SOAR) playbook actions

- Aggregate affected accounts and access
- Disable accounts and access that are part of security incidents
- Retrieve and document configuration Items with potential exposure, based on access
- Analyze identity data patterns to generate incidents in Security Incident Response when the following are detected:
    - Foreign changes
    - Compromised accounts with elevated privileges are creating new accounts in your environment
    - Terminated users with access

Visit our website to watch a demo or request more info clearskye.com