

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

cident Details Related Records	MITHE ATTACK Card									
	Problem		Q.			Incident			۹.	
	Parent		9,			Change request			9,	
Parent se	ecurity incident		٩,							
Update Add Response Task	Cancel Delete									
lated Links										
how SLA Yeneline how All Related Lists										
ov Related Items Includ ov Enrichment Data ov Response Tasko	ees [2] Affected Users Acc	Show Matching Filter Out Copy URL to Clipboard Copy Sys., M	hild Security incidents	Similar Security incidents	Related Configuration Rems Related	Users Associated Observables	Response Tasks	Associated Phish Emails	Associated Phish Headers	
ow Related Terms social social Terchment Data social Response Techn		Filter Out Copy URL to Clipboard	kild Security Incidents	Similar Security Incidents	Related Configuration Roms - Related I	Users Associated Observables	Response Tables	Associated Phich Emails		n B 4B ≻ >> 5
ov Robited terms NHLIG sov Twickment Table ov Reporter Table Configuration Items (1) Affected Liv	Search Account	Filter Out Copy URL to Clipboard Copy syn_Jd Copy Field Name Copy Field Name		Smilar Security incidents	Related Configuration News Indeed (Users Associated Observables	Reporte Tasks	Associated Phich Emails		n B 4'B → >> (
oor Andread terms see 2005 wee Terchment Zalia wee Terchment Zalia Configuration Terms (10) Affected Str Configuration Terms (10) Affected Str Affected Stress Accounts (14)	Search Account	Filter Out Copy URL to Clipboard Copy Sp. Jd Copy Field Name Copy Field Name Copy Field Dayley Value Ausign Tag 2 Duable Assumt		Smilar Security Incidents III Environment		Users Associated Observables	Response Taolo	Associated Phish Emails		10 15 of 15 → >> 1
en Anland Lenns Sec 312 en Marconset Table en Fitzconse Table Configuration Nerres (1) Athende Liv III Athende Livers Accounts (1) Security Incident + 5000000	A Seach Account	Filter Out Copy LIR. In Clipboard Copy Yes/ Marce Copy Field Name Copy Field Name Copy Field Dapley Water Assign Tag Constite Assount Come Second In Miller		Environment.			Response Taulos			10 IS of IS → 5 > 5
hos-shided tens hex.200 hex.200 hex.201 Configuration herm (10) Affected to Affected tens Accounts Configuration herm (10) Affected tens Accounts Affected tens Accounts Configuration herm (10) Affected tens Accounts Configuration herm (10) Affected tens Accounts Configuration herm (10) Affected tens Accounts Affected tens Affected tens Accounts Affected tens Accounts Affected tens Accounts Affected tens Affec	Search Account os Q. III () Account	Filter Out Copy LIR. In Clipboard Copy Yes/ Marce Copy Field Name Copy Field Name Copy Field Dapley Water Assign Tag Constite Assount Come Second In Miller	et a	Environment.		■ Account Type	Response Taolos	II tone	HE H 1	10 IS # IS ► ►> 5
Security incident + \$1803200	search Account os () At () At	Filter Out Copy URL to Clipboard Copy Stick Stand Copy Stick Stame Copy Stick Stame Copy Stick Stame Copy Stick Stame Copy Stick Stame Copy State Association Copy State Association Association Conference Association Copy State As	ert a gebra-Skyetabu onmicro	Environment ant.com Microarit.365		₩ Account Type Standard M365	Response Taolo	III Status Disabled	<< < 1 If Philapel tem false	w 15 of 15 ▷ ▷ ▷ 5

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 <u>clearskye.com</u>

