Preempt Threat Hunter

Fast, Powerful Investigations to Surface Hidden and Non-Obvious Threats

Preempt's Threat Hunter capabilities puts the raw power of the Preempt Platform at your fingertips. With unified visibility of accounts and access across all platforms, analysts can quickly query across any combination of attributes tracked by Preempt to find exactly what they are looking for in context. Instead of constantly pivoting between tools, analysts can now drive smart and integrated investigations that correlate across user and device attributes, access and authentication methods, account changes, time, location, and more. This ability to query across the full scope of Preempt Platform provides the freedom to dive into any level of detail and ask the open-ended questions that reveal hidden problems in the enterprise.

Key Benefits

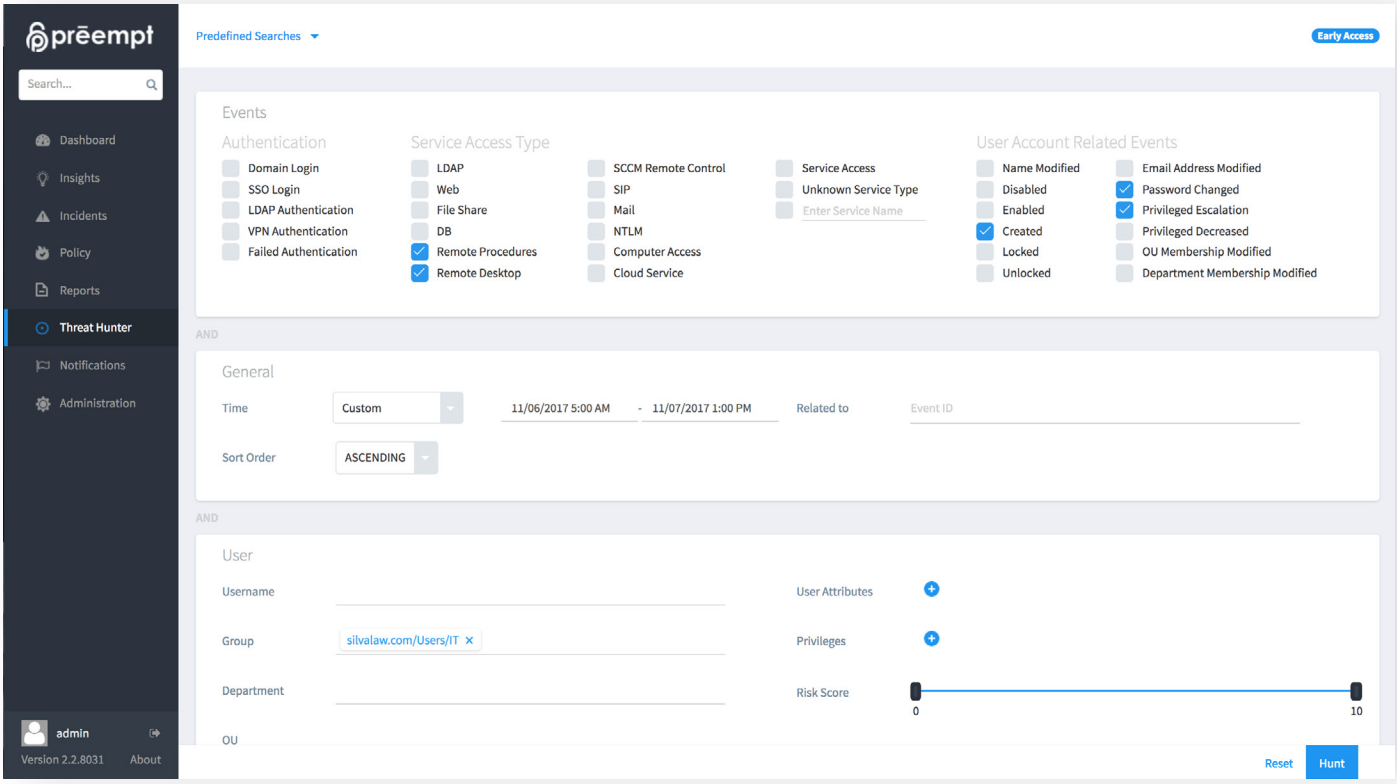
- Vastly accelerate threat hunts
- Easily correlate across any number of entity traits and behaviors
- Reduce investigation and dwell time
- Empower open-ended investigations based on identity, behavior, and risk
- Find attack progression and scope by seeing related events in context

Powerful Query Interface

The Threat Hunter app begins with a powerful interface that lets analysts search across any attribute in the Preempt Platform. Instead of crafting arduous string-based queries, analysts can simply select the attributes they are interested in and go. This lets analysts dial in exactly what they are looking for and quickly test hypotheses without getting bogged down crafting queries and pouring over logs.

Searches can include but are not limited to:

- Authentication Type (e.g. LDAP, SSO)
- Service Access Type (e.g. Fileshare, Remote Desktop)
- Account Events (e.g. Privilege Escalation, Locked Account)
- Time Range
- User Attributes (e.g. High Risk, Weak PW)
- Privileges
- Location (e.g. CIDR, Site, Geo)



Digging Deeper

Once a query is run, Threat Hunter lets the analyst dive into any level of detail and pivot into related events. For example, when investigating a failed login, an analyst can see the user and host details, the host OS down to the build number, as well as detailed failure reasons and counts. Analysts can then easily expand to see related events and a chronology of exactly what happened before and after the event in question. This allows staff to intuitively follow the thread of their investigation and pivot without constantly crafting new queries. This combination of simple searching and detailed results, ensures staff can go from open-ended questions to hard answers quickly and easily.

preempt

Preempt protects organizations by eliminating security threats. Threats are not black or white and the Preempt Platform is the only solution that preempts threats with continuous threat prevention that automatically adapts based on identity, behavior and risk. This ensures that both security threats and risky employee activities are responded to with the right level of security at the right time. The platform easily scales to provide comprehensive identity based protection across organizations of any size.

www.preempt.com info@preempt.com