State and Local Government

"No other technology provides insights and behavioral model customization like Exabeam. They pioneered user and entity behavior analytics (UEBA)."

- SOC Manager, The Missing Link

Cyberattacks targeting state and local governments are on the rise

With state and local government agencies touching so many aspects of their constituents' lives, disruptions or data breaches can have a significant impact on the community. With more than 2,000 incidents in 2022, it's clear that local governments are prime targets for attackers. Tight budgets and staffing shortages often force government agencies to rely on outdated security systems and limited backups, making them attractive targets for hackers. These attackers also seek notoriety through media coverage of government attacks, providing free publicity for their software and services.

Compromising user credentials is one of the most common ways attackers infiltrate victims' systems. Consequently, officials must either pay ransoms or bear the costs of downtime, lost revenue, and direct expenses for restoring their systems — often at taxpayers' expense. Meanwhile, government employees and citizens must deal with crippled systems, such as emergency services or police departments, for critical operations.

Protect government data with modern security tools

With public safety, finances, sensitive information, and trust at stake, it's necessary that state and local government agencies implement solutions that enable security teams to quickly and accurately detect, investigate, and respond to cyberthreats. Exabeam helps agencies keep critical systems up and running and protect citizens' valuable personal data. The Exabeam Security Operations Platform empowers security teams to improve threat detection and achieve faster investigation and response times, upscaling speed, productivity, accuracy, and outcomes.

With Exabeam, security teams can:

- Securely ingest, parse, store, and search data at scale
- Utilize behavioral analytics to establish a baseline of normal behavior for users and devices
- Automate triage and forensic investigations with machine-built incident timelines that automatically gather context and activity before and after an alert

Detect credential-based attack activity

New threat permutations crop up frequently, rendering traditional detection approaches less effective in providing timely detection or visibility into the full scope of an attack. One of the top patterns for this type of breach is miscellaneous errors, with employees being seven times more likely to cause compromise through a mistake than a malicious act.

Unfortunately, agencies and offices often lack the staff, time, or budget to manually monitor and tune their security tools to keep pace with the onslaught of threats. As a result, state and local governments find themselves increasingly vulnerable to attacks.

Modern tools allow security teams to leverage user and behavior entity analytics (UEBA) to detect these rapidly changing threats. The Exabeam Security Operations Platform provides complete coverage to protect against these threats, including:

- Security log management using cloud-scale architecture to ingest, parse, store, and search data at lightning speed
- Behavioral analytics using histograms to baseline the normal behavior of users and devices, detecting, prioritizing, and responding to anomalies based on risk
- An automated investigation experience across the threat detection, investigation, and response (TDIR) workflow, offering a complete picture of threats, automating manual routines, and simplifying complex work.

Enable rapid response

Once a system is compromised, security analysts must be able to quickly identify and respond to the behavior of attackers infiltrating the network before files are encrypted and ransomware is activated. Astoundingly, the average time required to identify a breach is 280 days. Security teams facing talent shortages often lack sufficient resources to move quickly enough to disrupt the attack.

Exabeam offers security orchestration, automation, and response (SOAR)-powered playbooks that facilitate rapid responses that can disrupt the ransomware kill chain. These playbooks string together complex workflows, such as detonating a file in a sandbox, and based on the results, quarantine affected endpoints or block access to command and control servers. Security analysts can define triggers to automatically activate a playbook as soon as ransomware is detected, disrupting the kill chain and containing infections within minutes.

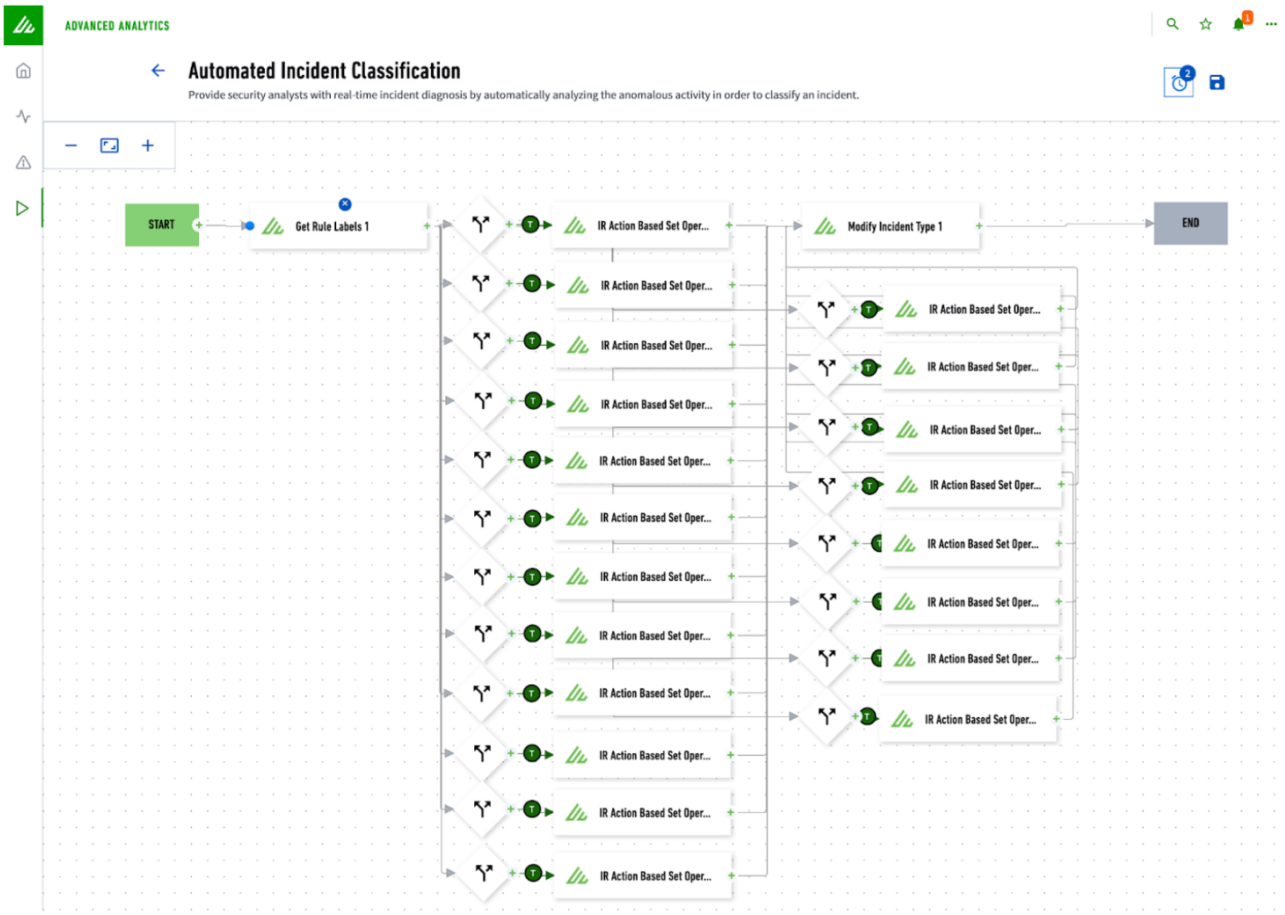

Figure 1.
The Exabeam Turnkey Playbook for Threat Intelligence automatically extracts files and links from an email, then obtains the IP, domain, URL, file, and email sender reputation from a threat intelligence service. Using conditional logic, the playbook automatically escalates the incident if it finds anything suspicious

Determining normal vs. abnormal behavior

Since most breaches involve compromised credentials, discerning normal from abnormal behavior can be challenging. Acquired credentials enable attackers to move seamlessly throughout an agency's networks, often going undetected. This seemingly legitimate access can take weeks or even months to discover, resulting in more extensive damage and expense.

Exabeam helps security teams outsmart adversaries using compromised credentials by providing automation and use case content across the entire analyst workflow, from collection to response. By leveraging machine learning and UEBA to establish a baseline for normal behavior for every user, device, and peer group, Exabeam automatically detects anomalous behaviors indicative of a compromised account, regardless of the attacker's techniques. These pre-built detection models do not require security engineers to create complex correlation rules.

Automate triage and investigations

While traditional security tools help public sector agencies meet compliance requirements, they are not designed to support security operations center (SOC) workflows for incident investigation. When attacks occur, analysts using legacy tools often spend many cycles with tedious, manual queries that consume precious time during an attack, meaning systems containing sensitive constituent data may be affected before adequate response measures can be implemented.

Exabeam automates the more tedious, time-consuming portions of the investigation workflows, enhancing analyst productivity and saving valuable time while an attack is in progress. Exabeam automatically reconstructs an attack kill chain using machine-built Smart Timelines™ to gain visibility into the full scope of an incident, identifying which systems and assets were infected. With automated, rapid investigations, teams can use these timelines to quickly review the entire attack chain and spend less time performing manual searches, focusing instead on complete and timely responses.

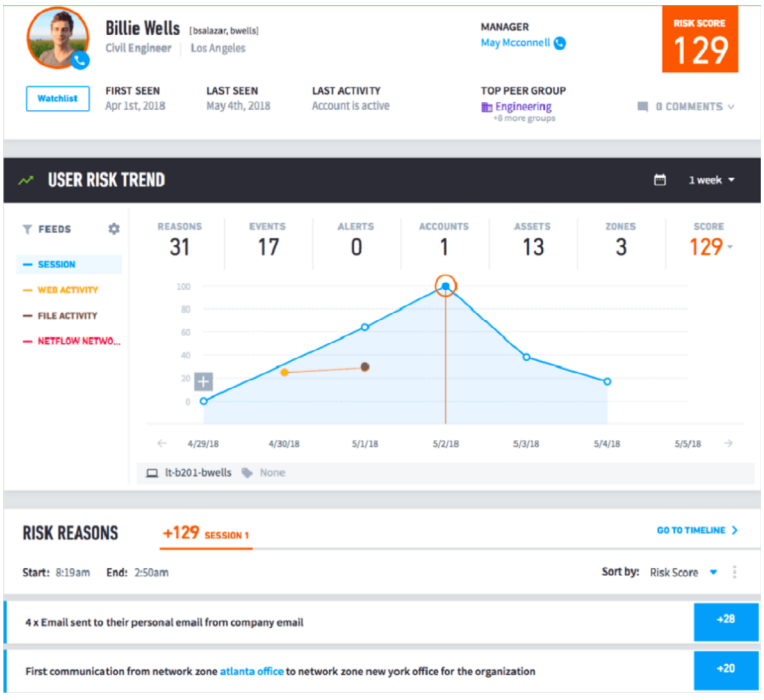

Figure 2.
Smart Timelines provide an event chronology along with descriptions and potential risk scores

Manage regulatory requirements

State and local governments are often required to adhere to various federal and state regulations, such as HIPPA, FERPA, and PCI DSS. Compliance with these regulations requires the implementation of specific cybersecurity controls and processes. These range from logging requirements for orchestration, standardization, and storage to behavior monitoring, which can be overwhelming to teams and resources. However, tools like the Exabeam Security Operations Platform can effectively manage compliance, streamlining the process for government agencies. Although compliance alone cannot prevent, detect, or remediate attacks, the right security solution can.

About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM™ for advancing security operations. We Detect the Undetectable™ by understanding normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

Learn more about Exabeam today

Get a Demo Now →