What is SIEM? A Beginner's Guide

DATA SECURITY

SIEM is now a $2 Billion industry, but only 21.9% of those companies are getting value from their SIEM, according to a recent survey.

SIEM tools are an important part of the data security ecosystem: they aggregate data from multiple systems and analyze that data to catch abnormal behavior or potential cyberattacks. SIEM tools provide a central place to collect events and alerts – but can be expensive, resource intensive, and customers report that it is often difficult to resolve problems with SIEM data.

Guide: 5 Ways Your SIEM is Failing You (And What to Do About It)

First Name* First Name

Last Name* Last Name

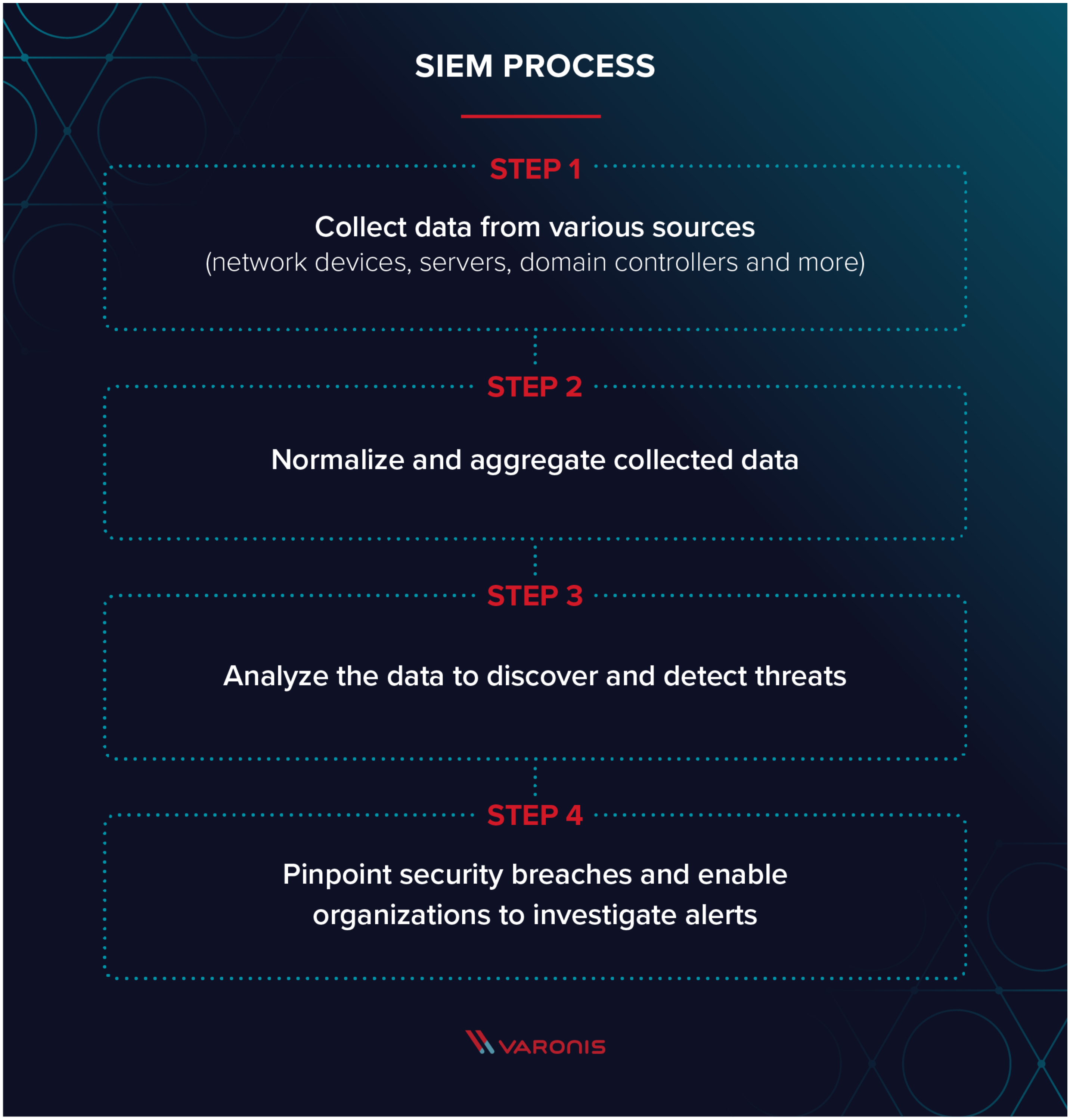
Email* Email

☐ I agree to receive communications from Varonis.*

You can unsubscribe from these communications at any time. For more information on our privacy practices, and how we're committed to protecting your information, please review our privacy policy.

Get the free guide

"Seeing the context for when and how security events sped up our investigations by a factor of 3."



SIEM PROCESS

STEP 1

Collect data from various sources
(network devices, servers, domain controllers and more)

STEP 2

Normalize and aggregate collected data

STEP 3

Analyze the data to discover and detect threats

STEP 4

Pinpoint security breaches and enable organizations to investigate alerts

Security Information and Event Management (SIEM) is a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure.

SIEM collects security data from network devices, servers, domain controllers, and more. SIEM normalizes, aggregates, and applies analytics to that data to discover trends, detect threats, and enable organizations to investigate any alerts.

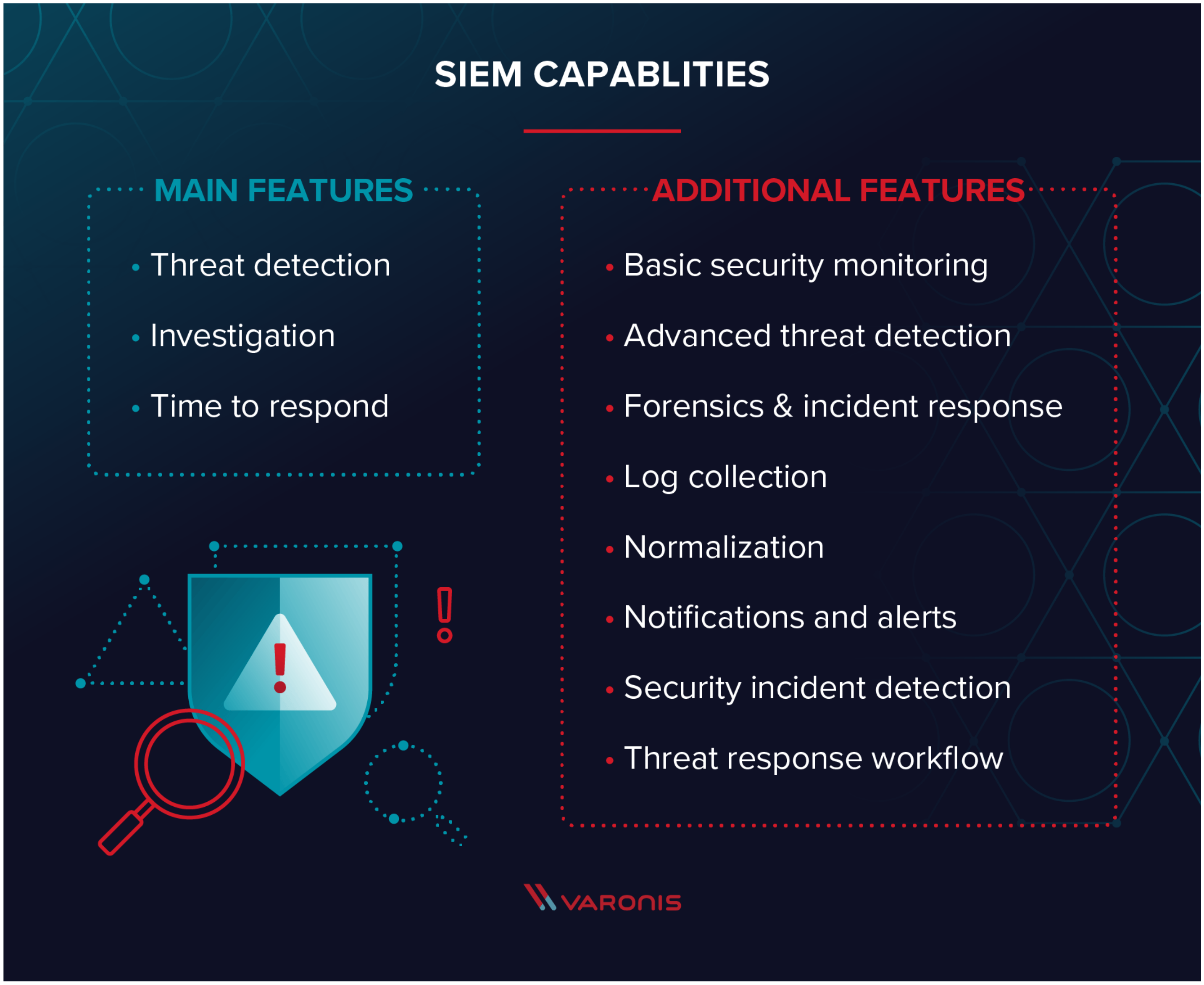
How Does SIEM Work?

SIEM provides two primary capabilities to an Incident Response team:

- Reporting and forensics about security incidents
- Alerts based on analytics that match a certain rule set, indicating a security issue

At its core, SIEM is a data aggregator, search, and reporting system. SIEM gathers immense amounts of data from your entire networked environment, consolidates and makes that data human accessible. With the data categorized and laid out at your fingertips, you can research data security breaches with as much detail as needed.

Security Information and Event Management Capabilities



SIEM CAPABLITIES

MAIN FEATURES

- Threat detection
- Investigation
- Time to respond

ADDITIONAL FEATURES

- Basic security monitoring
- Advanced threat detection
- Forensics & incident response
- Log collection
- Normalization
- Notifications and alerts
- Security incident detection
- Threat response workflow

Gartner identifies three critical capabilities for SIEM (threat detection, investigation and time to respond) — there are other features and functionality that you commonly see in the SIEM market, including:

- Basic security monitoring
- Advanced threat detection
- Forensics & incident response
- Log collection
- Normalization

- Threat response workflow

Top SIEM Tools

These are some of the top players in the SIEM space:

Splunk

Splunk is a full on-prem SIEM solution that Gartner rates as a leader in the space. Splunk supports security monitoring and can provide advanced threat detection capabilities.

Varonis integrates with Splunk through the Varonis DatAlert App for Splunk.

IBM QRadar

QRadar is another popular SIEM that you can deploy as a hardware appliance, a virtual appliance, or a software appliance, depending on your organization's needs and capacity.

QRadar can integrate with Varonis to add Advanced Threat Detection capabilities. Look for the Varonis App for QRadar

LogRhythm

LogRhythm is a good SIEM for smaller organizations. You can integrate LogRhythm with Varonis to get threat detection and response capabilities.

SIEM in the Enterprise

Some customers have found that they need to maintain two separate SIEM solutions to get the most value for each purpose since the SIEM can be incredibly noisy and resource intensive: they usually prefer one for data security and one for compliance.

Beyond SIEM's primary use case of logging and log management, enterprises use their SIEM t purposes. One alternate use case is to help demonstrate compliance for regulations like HIPAA, PCI, SOX, and GDPR.

planning world, data is key, and understanding your current usage and trends over time allows you to manage growth and avoid large capital expenditures as a reactionary measure versus prevention.

Limitations of SIEM Applications as a Full Data Security Ecosystem

SIEM applications provide limited contextual information about their native events, and SIEMs are known for their blind spot on unstructured data and emails. For example, you might see a rise in network activity from an IP address, but not the user that *created* that traffic or **which** files were accessed.

In this case, context can be everything.

What looks like a significant transfer of data could be completely benign and warranted behavior, or it could be a theft of petabytes of sensitive and critical data. A lack of context in security alerts leads to a ‘boy that cried wolf’ paradigm: eventually, your security will be desensitized to the alarm bells going off every time an event is triggered.

SIEM applications are unable to classify data as sensitive or non-sensitive and therefore are unable to distinguish between *sanctioned* file activity from *suspicious* activity that can be damaging to customer data, intellectual property, or company security.

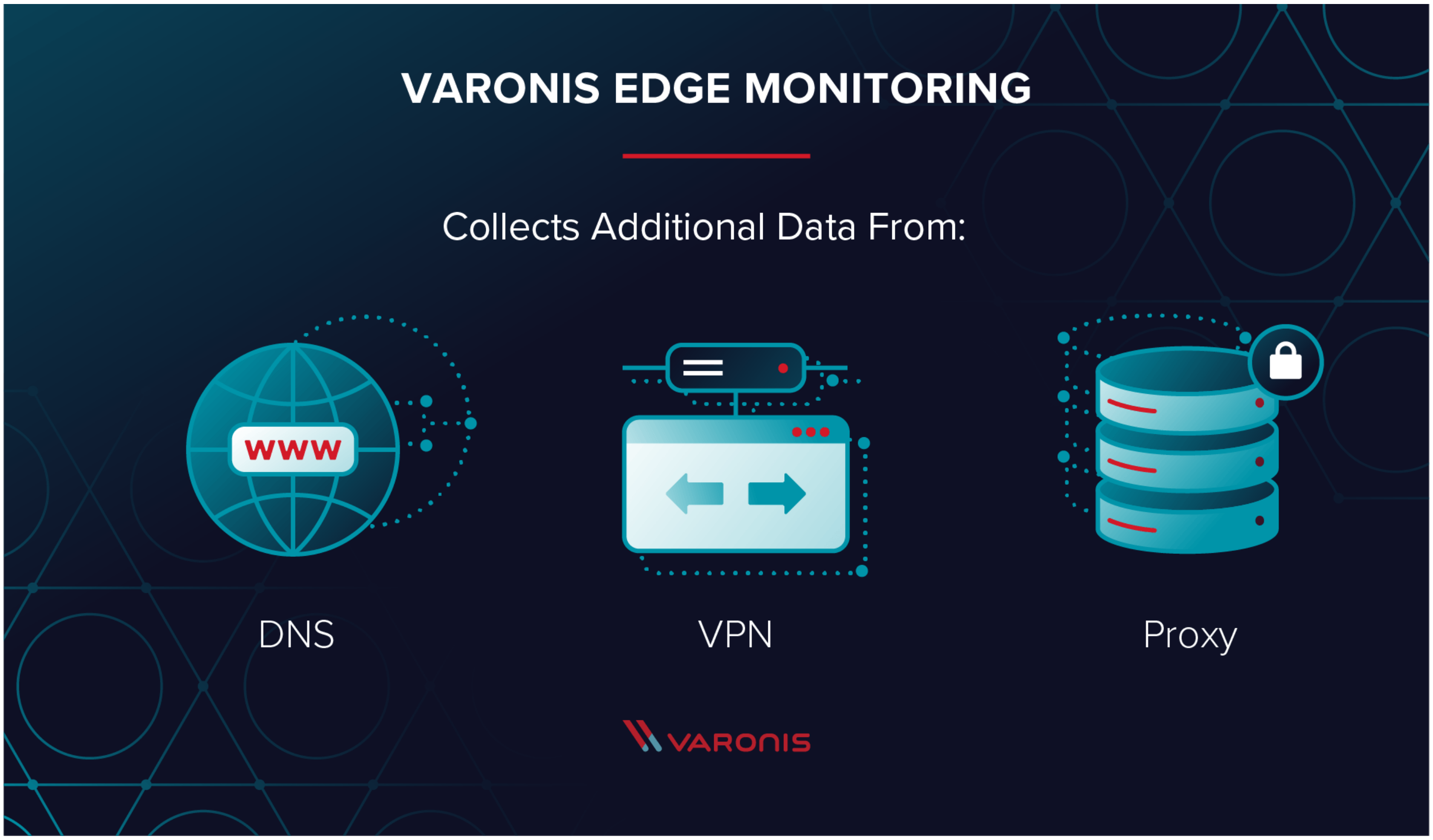
Ultimately, SIEM applications are only as capable as the data they receive. Without additional context on that data, IT is often left chasing down false alarms or otherwise insignificant issues. Context is key in the data security world to know which battles to fight.

The biggest issue we hear from customers when they use SIEM is that it’s extremely difficult to diagnose and research security events. The volume of low-level data and the high number of alerts cause a ‘needle in a haystack’ effect: users get an alert but often lack the clarity and context to act on that alert immediately.

How Varonis Complements SIEM

The context that Varonis brings to SIEM can be the difference between a snipe hunt or preventing a

And that's where Varonis comes in. Varonis provides additional context to the data that a SIEM collects: making it easier to get more value out of a SIEM by building in-depth context, insight, and adding threat intelligence into security investigations and defenses.



Varonis captures file event data from various data stores – on-premises and in the cloud – to give the who, what, when, and where of each file accessed on the network. With Varonis Edge monitoring, Varonis will also collect DNS, VPN, and web proxy activity. You'll be able to correlate the network activity with the data store activity to paint a complete picture of an attack from infiltration through file access to exfiltration.

Varonis classifies unstructured files based on hundreds of possible pattern matches, including PII, government ID numbers, credit card numbers, addresses, and more. That classification can be extended to search for company-specific intellectual property, discover vulnerable, sensitive information, and help meet compliance for regulated data. Varonis reads files in place without any impact to end users.

Varonis also performs user behavior analytics (UBA) to provide meaningful alerts based upon behavior patterns of users, along with advanced data analysis against threat models that inspect patterns for insider threats (such as exfiltration, lateral movement, account elevation) and outsider

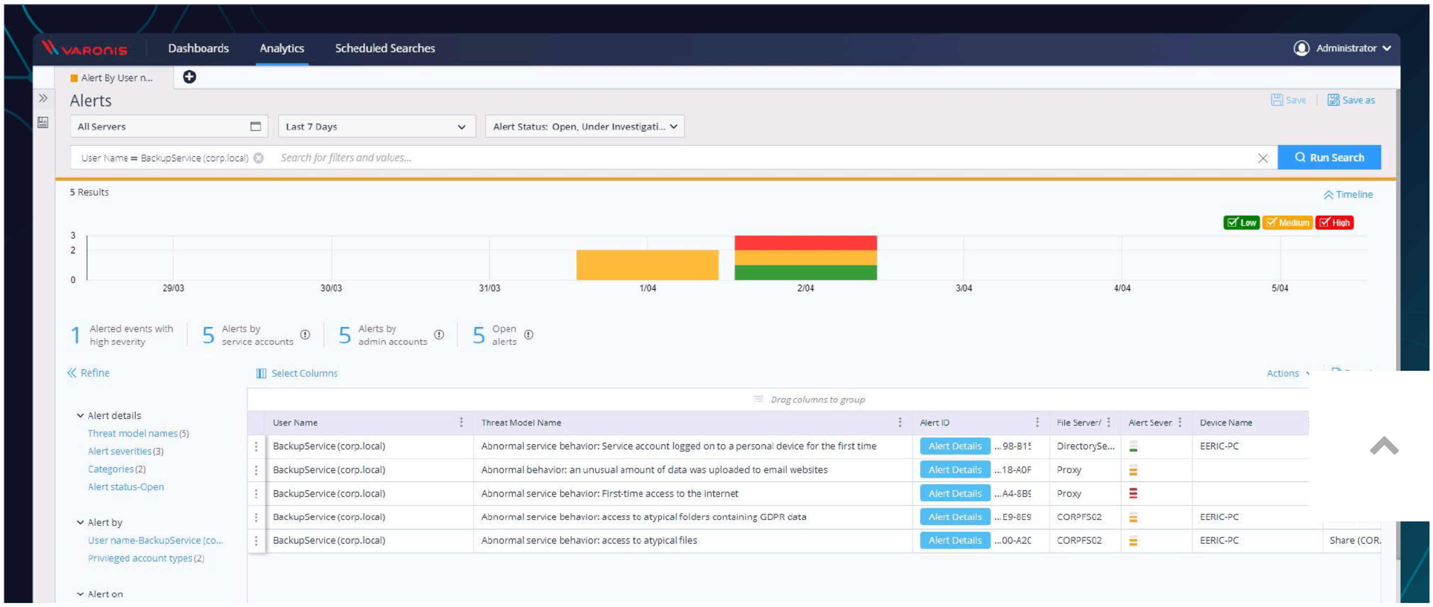
Integration Highlights

Varonis integrates with SIEM applications to give security analytics with deep data context so that organizations can be confident in their data security strategy. Benefits include:

- Out of the box analytics
- Integrated Varonis dashboards and alerts for streamlined investigation
- Alert specific investigation pages
- Critical information highlighted at a glance, with actionable insights and rich context
- Integration into your SIEM workflow

How to Investigate an Attack with SIEM and Varonis

This contextual data that Varonis brings gives security teams meaningful analysis and alerts about the infrastructure, without the additional overhead or signal noise to the SIEM. SOC teams can investigate more quickly by leveraging SIEM with Varonis and get insight into the most critical assets they need to protect: unstructured data and email. With the added visibility provided by Varonis, you get an at-a-glance overview of what's happening on your core data stores – both on-premises and in the cloud. You can easily investigate users, threats, and devices – and even automate responses.



All Servers

Last 7 Days

Alert Status: Open, Under Investigati...

User Name = BackupService (corp.local)

Search for filters and values...

5 Results

1 Alerted events with high severity

5 Alerts by service accounts

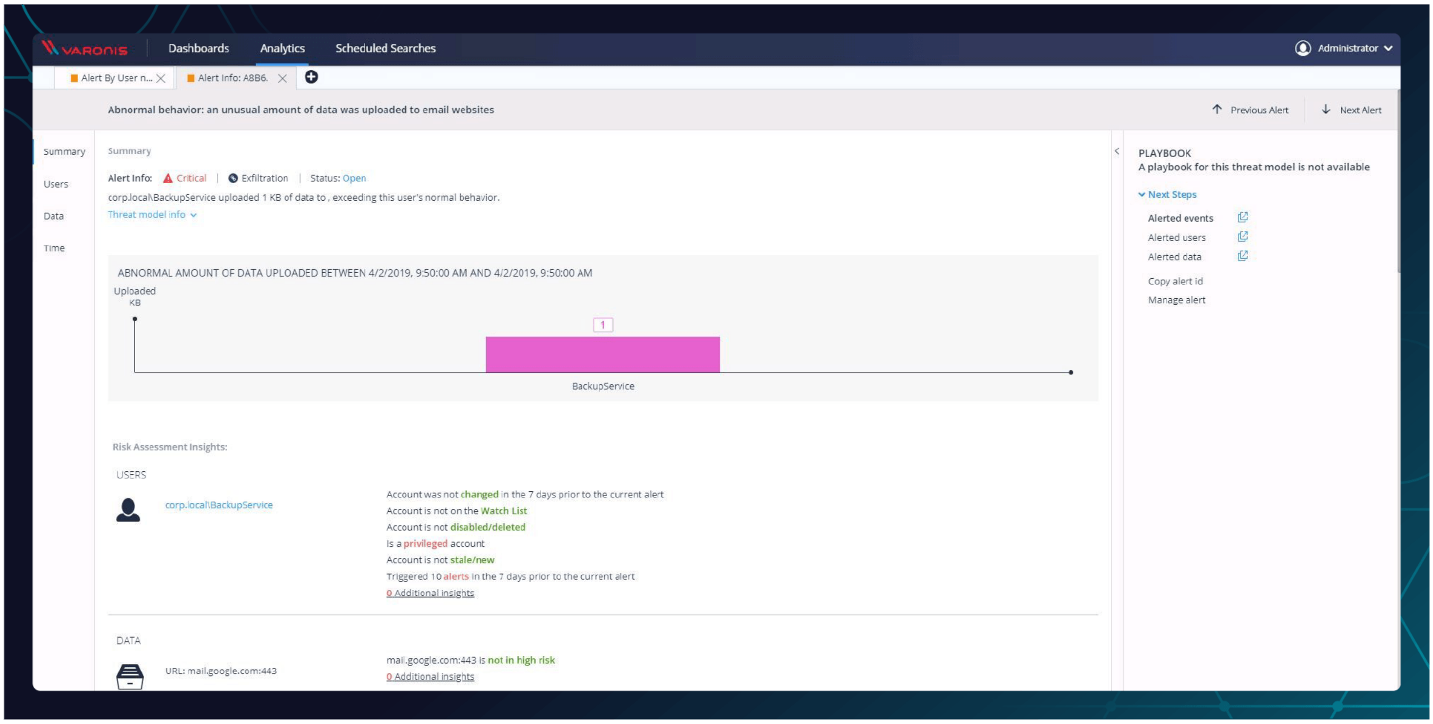
5 Alerts by admin accounts

5 Open alerts

User Name	Threat Model Name	Alert ID		File Server/	Alert Sever.	Device Name	
BackupService (corp.local)	Abnormal service behavior: Service account logged on to a personal device for the first time	Alert Details	...98-B15	DirectorySe...		EERIC-PC	
BackupService (corp.local)	Abnormal behavior: an unusual amount of data was uploaded to email websites	Alert Details	...18-A0F	Proxy			
BackupService (corp.local)	Abnormal service behavior: First-time access to the internet	Alert Details	...A4-8B9	Proxy			
BackupService (corp.local)	Abnormal service behavior: access to atypical folders containing GDPR data	Alert Details	...E9-8E9	CORPFS02		EERIC-PC	
BackupService (corp.local)	Abnormal service behavior: access to atypical files	Alert Details	...00-A2C	CORPFS02		EERIC-PC	Share (COR.

(Click to Zoom)

When you click on the Varonis Alert Event in your SIEM, you are taken to the Varonis Alert Dashboard for the alert you are investigating. From here, you can see that this alert is related to four other alerts. Any one of them is troublesome, but since they are all connected, it's a much clearer and well laid out picture of a cyberattack.



Abnormal behavior: an unusual amount of data was uploaded to email websites

Summary

Alert Info: Critical | Exfiltration | Status: Open

corp.local\BackupService uploaded 1 KB of data to , exceeding this user's normal behavior.

Threat model info

ABNORMAL AMOUNT OF DATA UPLOADED BETWEEN 4/2/2019, 9:50:00 AM AND 4/2/2019, 9:50:00 AM

Risk Assessment Insights:

USERS

corp.local\BackupService

Account was not changed in the 7 days prior to the current alert
Account is not on the Watch List
Account is not disabled/deleted
Is a privileged account
Account is not stale/new
Triggered 10 alerts in the 7 days prior to the current alert
0 Additional insights

DATA

URL: mail.google.com:443

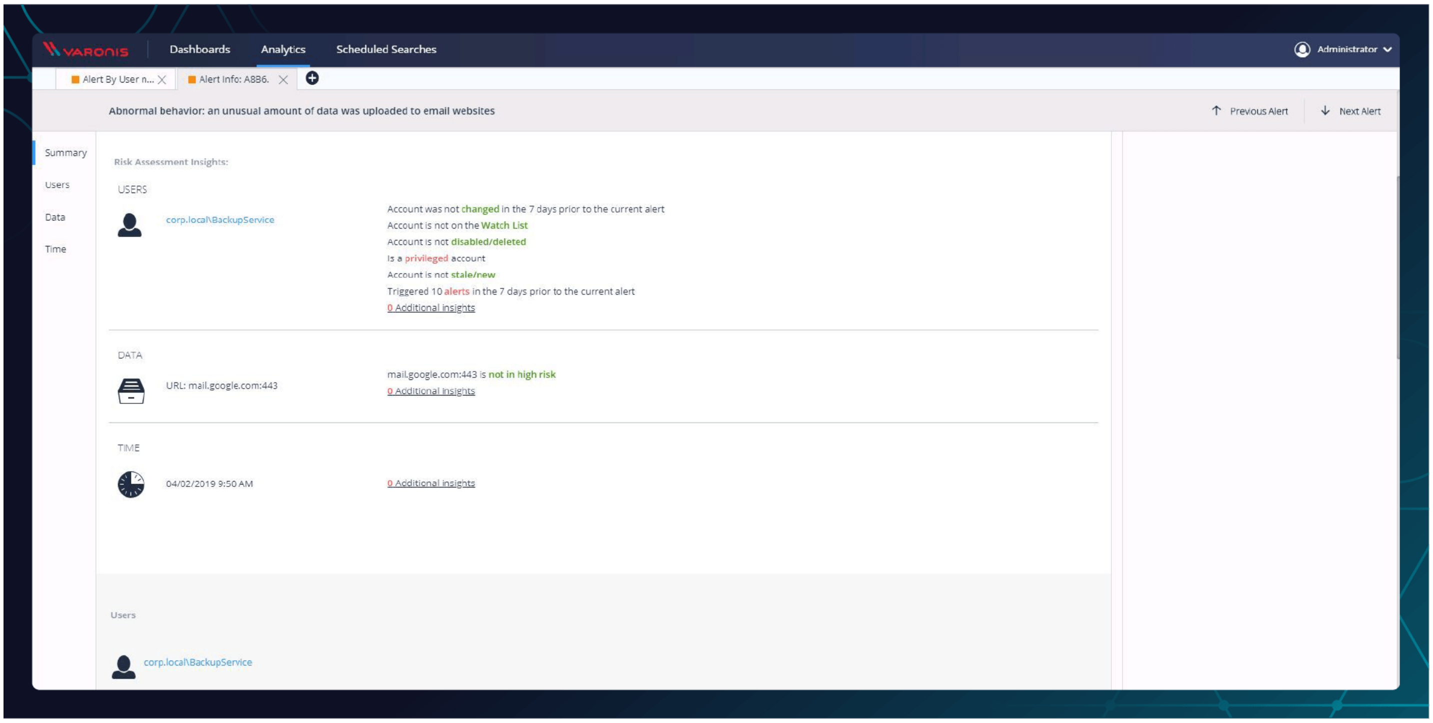
mail.google.com:443 is not in high risk
0 Additional insights

PLAYBOOK
A playbook for this threat model is not available

Next Steps

(Click to Zoom)

This alert tells us that this BackupService account uploaded data to an external email website.



Abnormal behavior: an unusual amount of data was uploaded to email websites

Risk Assessment Insights:

USERS

corp.local\BackupService

Account was not changed in the 7 days prior to the current alert
Account is not on the Watch List
Account is not disabled/deleted
Is a privileged account
Account is not stale/new
Triggered 10 alerts in the 7 days prior to the current alert
0 Additional insights

DATA

URL: mail.google.com:443

mail.google.com:443 is not in high risk
0 Additional insights

TIME

04/02/2019 9:50 AM

0 Additional insights

Users

corp.local\BackupService

(Click to Zoom)

This alert tells us that the BackupService account has never accessed the internet before, making the fact that the account uploaded data to email much more suspicious.

That's just the beginning of investigating cybersecurity alerts with Varonis and your SIEM. Varonis can kick off a script to disable the user account and shut down the attack as soon as it's detected – in which case, that hacker might not have been able to get to the payroll files at all!

With the context you have at your disposal, you can quickly respond to – and manage – the alerts that you receive in your SIEM.

Security analysts spend countless hours to get meaningful alerts from SIEM: fine-tuning use cases, building rules, and adding in data sources – Varonis gives a head start with out-of-the-box analytics models, intuitive dashboards, and intelligent alerting.

OK, I'm Ready to Get Started!

If you're already using a SIEM, it's simple to add Varonis and get more out of your SIEM invest you're looking to start your data security plan, start with Varonis, and then add your SIEM.

make Varonis and your SIEM better able to correlate and store data for analysis and auditing.

Check out a Live Cyberattack Webinar to see how Varonis brings context to your SIEM data.

JEFF PETTERS

Jeff has been working on computers since his Dad brought home an IBM PC 8086 with dual disk drives. Researching and writing about data security is his dream job.

—— RELATED POSTS ——

DATA SECURITY

Attack lab: Spear Phishing with Google Drive Sharing

DATA SECURITY

Threat Update 27 – Concentrations of Power

DATA SECURITY

Your Primer to Third-Party Risk Management

Français
Deutsch
日本語
Русский
Português

SOLUTIONS
Remediation & Governance
Security Analytics
Data Classification
Ransomware
Insider Threats
External Threats

PLATFORM
How It Works
How to Buy
How to Use It
Real Results
ROI
Integrations

COMPANY
About Varonis
Varonis Life
Careers
Customers
Investor Relations
Brand
Contact Us

RESOURCES
Free Security Training
Analyst Reports
Whitepapers
Guides
Videos
Events

PARTNERS
Technology Partners
Channel Partners
Partner Portal