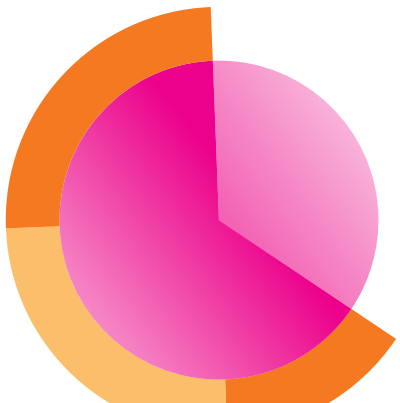
The Essential Guide to **Security Data**

splunk>

Time-Series Data. Streaming Data. The Rise of Data.

It's no secret that data remains underused and undervalued in most organizations all over the world. Despite the constant talk of data-driven decisions, organizations of all sizes are still missing the mark on how to effectively capture and use the troves of data being generated every day, whether it comes from users, outside industry resources, or their own networked devices. And yet, cybercriminals are realizing that data is at times more valuable than oil, because similar to oil, data can be refined and turned into a commodity to the highest bidder. Security teams are dealing not only with the rise of data and expanded perimeters within the organization, but the rise of sophisticated cyber attacks. They need visibility and contextual insights to effectively investigate and respond to security incidents across their on-prem, hybrid, and multicloud environments.

In fact, 73% of organizations are enriching their security analytics with other data sources, by turning to analytics tools. Important insights across IT, security and your organization lie hidden in this data. Data holds the definitive record of all activity and behavior of your customers and users, transactions, applications, servers, networks, mobile devices and more. Critical information on everything from configurations, APIs, message queues, diagnostic outputs, sensor data of industrial systems and more is all there — you just have to tap into it the right way.



With the right approach, data makes it simple to:

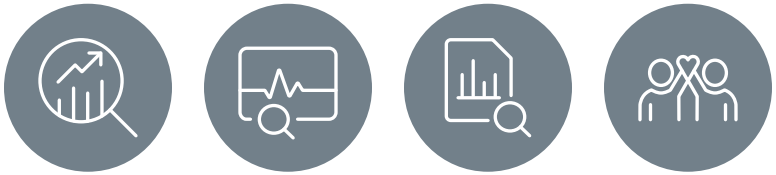
- Make better informed decisions about every part of your business.
- Run your operations more efficiently.
- Optimize user and customer experiences.
- Detect fraud, or prevent it altogether.
- Uncover potential disasters before they happen.
- Find hidden trends that help your company leapfrog the competition.
- Make everyone who uses it look like a hero.
- … and so much more.

The challenge with leveraging the vast quantity of data that most companies collect is that it comes in a dizzying range of formats that traditional data monitoring and analysis tools aren't designed to handle. Many tools can't keep up with the varying data structures, sources or time scales. And it goes well beyond just machine data as well. But the upside to tapping into your data is tremendous, and this is where Splunk® comes in.

With Splunk, you can bring data to every question, decision and action in your organization to create meaningful outcomes. Unlike any other platform, Splunk is truly able to take any data from any source and drive real action to benefit the business — from IT infrastructure and security monitoring to DevOps and application performance monitoring and management.

A Data Platform For A Hybrid World

Use data to:



The organizations that get the most value out of their data are those able to take disparate data types, enrich them and extract answers. But not knowing what data to ingest can stop businesses before they begin to realize success.

Familiarizing yourself with general use cases in security, IT operations, business analytics, DevOps, the Internet of Things (IoT) and more — including the data types and sources involved — can get you on track right away.

Here's an example:

1. A customer's order didn't go through
2. The customer called support to resolve the issue
3. After too much time on hold, the customer gave up and tweeted a complaint about the company

What Does Machine Data Look Like?

Figure 1: Data can come from any number of sources, and at first glance, can look like random text.

Machine Data Contains Critical Insights

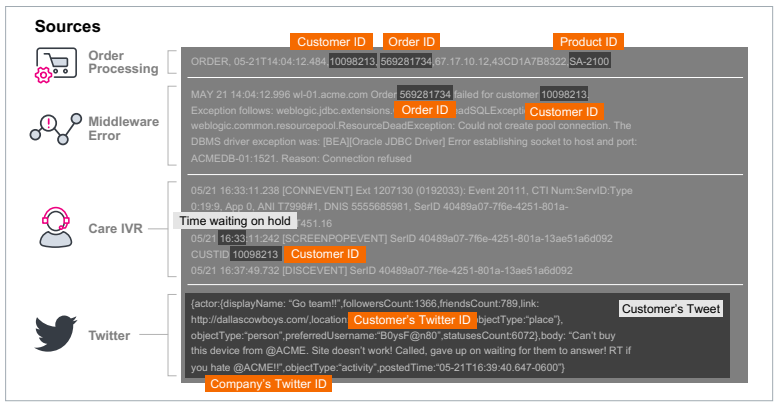


Figure 2: The value of data is hidden in this seemingly random text.

Machine Data Contains Critical Insights

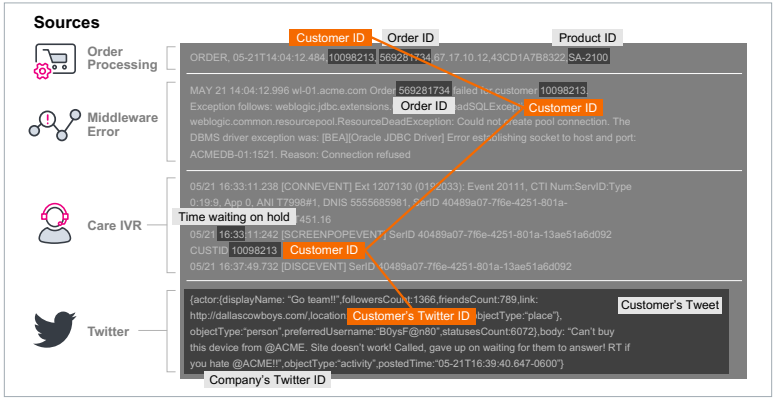


Figure 3: By correlating different types of data together, you can start to gain real insight into what's going on in your infrastructure, see security threats or even use the insights to drive better business decisions.

By taking all the data involved in the process — i.e., pulling information from order processing, middleware, interactive voice response systems and Twitter — an organization can get a full view of the customer experience problem.

Security Data

Organizations must use every available resource to stay ahead of cyberattacks because of the persistent nature of advanced threats and the ease with which malware can cripple an entire network. Security analysts are overwhelmed with the speed and volume of security alerts. Analysts cannot address every alert every day, and this leads to slow investigation and response times. Furthermore, SOCs are short-staffed, with a shortage of qualified security analysts to fill positions around the globe.

These challenges are only going to grow as we enter a digital age with the complexity of cloud migration, networks moving from 4G to 5G, as the number of connected devices nears 80 billion, and as automation becomes more ingrained in our lives.

One of the most important — and often overlooked — resources that organizations can tap into to solve these security challenges is data. Data is everywhere and it can be used to to stay ahead of the latest cyberthreats.

The companies that are able to harness the power of these transformations and the data they create are going to be more efficient, profitable, innovative and ultimately more secure.

This book showcases how three companies are leveraging data to protect themselves against the latest cyberthreats, and in many cases, to address IT operations, IoT, DevOps and business analytics challenges as well.

Security and Compliance

IT Ops, App Delivery and DevOps

Table of Contents

Transforming Intel's Security Posture With Innovations in Data Intelligence

Industry

- Technology

Splunk Use Cases

- Security
- Cybersecurity Incident Response Management
- Security Monitoring
- Application Monitoring

Challenges

- Shift to a data-centric business model increases data value, but also vulnerability
- Legacy SIEM no longer fit for purpose
- Multiple, disconnected data siloes and teams delivering different data analysis interpretations

Business Impact

- Transformed information security management and control
- Detects sophisticated threats in minutes or hours, versus days or weeks
- Delivers a collaborative, unified approach to managing cybersecurity
- Delivers a cyber intelligence platform for Intel's entire InfoSec organization

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security
- Splunk IT Service Intelligence (ITSI)
- VictorOps
- Splunk Mission Control

"We see the potential, and because we see the potential, we're investing time, energy and resources. We want Splunk to be successful because we think it will help us fulfill our mission."

— Brent Conran, Chief Information Security Officer, Intel

Executive Summary

It would be difficult to overestimate the impact and importance of Intel's technology contributions on society. The company's engineering expertise is helping secure, power and connect billions of devices and the infrastructure of the smart, connected world. Equally difficult to overestimate would be the significance of secure data as an organization's most protected asset.

With Splunk® and Apache Kafka as its foundation, Intel IT developed a new Cyber Intelligence Platform that is transforming its approach to information security by:

- Speeding data analysis and reducing time to detect and respond to advanced threats
- Enabling a collaborative organization with a common language and work surface
- Providing streams processing and machine learning tools that deliver business value in additional areas, such as security operations and system health

Data is everything

Intel has changed from a PC-centric company to a data-centric company. The company is developing new products, entering new markets and engaging new customers in innovative ways.

"Data is everything; data is king. It's powering our business; it's powering everything," says Brent Conran, chief information security officer at Intel. "It's transforming traditional industries and born-in-the-cloud industries. The ability to gain insights from data is the difference between a successful business or one that falls away."

This greater emphasis and reliance on data required Intel's Information Security (InfoSec) organization to build and maintain a comprehensive "defense-in-depth" strategy. The team automated prevention and detection tools at many levels — including the perimeter, network, endpoints, applications and data layer — to handle 99% of threats across Intel's environment.

Hunting the one percent

Advanced threats continue to grow in frequency and sophistication. And the organization was burdened with a legacy SIEM that no longer met the needs of the organization. Only a handful of experts knew how to use this legacy SIEM, which couldn't scale with the ever-increasing demand for more types of data.

Intel InfoSec needed a strategy to detect sophisticated threats attempting to penetrate the organization's environment — what Intel InfoSec calls hunting the one percent. This strategy inspired Intel's Cyber Intelligence Platform (CIP), which is centered on leading-edge technologies, including Splunk and Apache Kafka. With high-performance servers based on Intel® Xeon® Platinum processors, Intel 3D NAND Solid State Drives (SSDs) and Intel® Optane™ SSDs, the new CIP platform ingests over 12 terabytes of data per day and stores 15 petabytes of data. The data flows from hundreds of sources to a Kafka message bus, then into the Splunk platform, where users perform over 1.3 million searches per week.

With Splunk's Data-to-Everything™ Platform and hundreds of third-party tools, the InfoSec organization now has context-rich visibility and a common work surface, which improves the effectiveness of the entire InfoSec organization. The team now detects and responds to threats within hours or minutes — compared to weeks or hours previously.

Scaling Intel's Cyber Intelligence Platform

CIP's results led to additional data sources, new use cases and many more data models. Soon, use of the CIP expanded to teams like vulnerability management, compliance and enforcement, risk management and beyond, which placed additional demands on the infrastructure while requiring even faster compute and storage. To maximize the platform's performance, Intel's security solution architect and engineers needed a deeper understanding of the Splunk platform and Intel technologies.

> **"We built CIP to handle tens, and eventually hundreds, of terabytes of data per day, and to support hundreds of users building ad hoc searches, scheduled searches, data model accelerations and machine learning models. To be performant at scale, we needed servers with Intel's Xeon Scalable processors and Intel SSDs for high-performance compute and storage. Seconds matter when your mission is 'make it safe for Intel to go fast.'"**
>
> — Jac Noel, Security Solution Architect, Intel

A collaborative Splunk and Intel team developed a joint reference configuration to help guide CIP's expansion across compute, memory and storage using the latest Intel products and technologies. Splunk and Intel are now sharing their success with IT peers, helping others scale their Splunk and Apache Kafka deployments to more effectively convert raw data into operational, business and security intelligence.

Providing value for today and tomorrow

Intel's InfoSec team is expanding its use of Splunk and Kafka. The analysts and data scientists are transforming, enriching, joining, filtering and operating on data in stream. The team is also adding more machine learning tools for everything from incident response, operations and system health to workflow orchestration and alerts. In collaborating with Splunk, Intel is unlocking value for today and tomorrow.

"Intel Information Security is much more agile than we've ever been in the past," says, Conran. "We put in a brand-new Splunk data lake and we modernized our tools. By putting data in the right place and reskilling our people, we created a force multiplier. We are using machine learning to significantly increase the depth and speed of our cyber intelligence."

NewYork-Presbyterian Battles the Opioid Crisis With Splunk

Industry

- Healthcare

Splunk Use Cases

- Security

Challenges

- Needed to track data from electronic health records, electronic prescription of controlled substances platforms, pharmacy dispensing systems and other sources in order to see if drugs are being diverted for potentially illegitimate purposes.
- Unable to monitor access to electronic PHI in real time, resulting in reduced security and protection of patient records.

Business Impact

- Safeguards against the diversion of opioids and high-cost medications, such as certain anti-cancer drugs that can be priced at tens of thousands of dollars per month.
- Monitors IT security operations to ensure controlled substances and other medications aren't being used or prescribed illegally.
- Creates possibilities for peer institutions to bring the same monitoring and diversion techniques to their hospitals.

Data Sources

- Audit logs
- Application data
- EPIC
- Cerner
- Allscripts
- athenahealth

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security (ES)

Executive Summary

As one of the nation's most comprehensive and integrated academic healthcare delivery systems, NewYork-Presbyterian is dedicated to providing the highest quality, most compassionate care to patients in the New York metropolitan area, nationally and across the globe. NewYork-Presbyterian is consistently recognized as a leader in medical education, groundbreaking research and innovative, patient-centered clinical care.

By wielding the power of Splunk technology, NewYork-Presbyterian has built a platform to closely safeguard controlled substances and other medications, ultimately benefiting the greater healthcare community. Thanks to Splunk, NewYork-Presbyterian can now:

- Audit access to patient records, and share data to authorized users to glean insights
- Help reduce the diversion of opioids and other controlled substances
- Comply with the Health Insurance Portability and Accountability Act (HIPAA) and other disclosure requirements
- Ensure the privacy of Protected Health Information (PHI) data and patient privacy

Protecting patient data and privacy

Initially, NewYork-Presbyterian turned to Splunk to fulfill a variety of security use cases, including preventing phishing attacks, bolstering account security and automating critical security workflows. "Fast-forward a couple of months, and we started building our security operations center [SOC]," says Jennings Aske, senior vice president and chief information security officer at NewYork-Presbyterian. "Now, we have a team of six individuals that spend all day looking at dashboards and visualizations that integrate all the data sources we need for security," says Aske.

But that was just the beginning. "In the course of building our SOC, we realized we needed to think about business problems related to patient privacy. In particular, we wanted to have a platform to help us make sure people weren't snooping, looking at too many records or accessing the wrong records," continues Aske. "So I said, 'Let's go talk to Splunk and suggest that we build a privacy platform for us and other Splunk customers that would integrate with clinical systems like EPIC.'"

Together, NewYork-Presbyterian and Splunk made this vision a reality, creating a platform that allows for immediate investigation by alerting privacy officers if patient records are inappropriately accessed. Yet the hospital soon realized that the platform's potential extended far beyond what they initially envisioned.

Battling opioids on a global scale

Soon, NewYork-Presbyterian realized that the same Splunk capabilities of correlation and machine learning that helped power the patient platform could also help identify opioid diversion — a critical contributor to the opioid epidemic ravaging the United States.

"When we think about the role that hospitals play in terms of the opioid crisis, we have employees who actually suffer from higher addiction rates than the general public," says Aske. "We know from looking at CDC statistics that at certain points in time, hospitals have been a primary source of some drugs on the street. One year, about 25% of the street's OxyContin came from hospitals. We have an ethical and moral obligation to not simply rely on manual auditing, but to build a platform to help catch potential diversion."

Helping fulfill this mission, the medication analytics platform will allow NewYork-Presbyterian to track data from electronic health records (EHRs), Electronic Prescription of Controlled Substances (EPCS) platforms, pharmacy dispensing systems and other sources, delivering insights to guard against the diversion of these medications. For example, the platform will immediately alert NewYork-Presbyterian if a physician prescribes a controlled substance to a patient who isn't in the care of the hospital, or if a pharmacy technician uses an automated dispensary cabinet more often than his or her peers.

"Ultimately, we thought that building this platform with Splunk means it could be easily leveraged by peer institutions across the country. It's safe to say that Splunk is used by all 20 of the *U.S. News*' top 20 hospitals. That's the sort of strength in numbers that could allow for these platforms to play a major role in improving care and public health."

— Jennings Aske, Senior Vice President and Chief Information Security Officer at NewYork-Presbyterian

"When I think about the medication analytics platform, I think about the fact that if you go outside of your or your family's six degrees, you can find family members affected by this," says Aske. "I think about when I've been offered opioids for gum surgery and didn't need it. I have a young daughter, and I want to make sure that if she's ever in a situation in which opioids are prescribed, it's for a legitimate reason, and they're not diverted."

A promising future

As NewYork-Presbyterian continues to provide compassionate care around the world, it's exploring new uses for Splunk across the hospital system, including potentially leveraging Splunk to faster detect issues with insurance coding and better investigate denied reimbursement claims. "Splunk is a platform that leverages and explores data in ways that might not be obvious," says Aske. "By bringing Splunk to more questions like insurance billing, we could potentially save the hospital millions of dollars."

With Splunk and NewYork-Presbyterian working together, "the possibilities are pretty much limitless in terms of how we can think about the hospital's data," says Aske. "We want to double down on our use of Splunk to really push this partnership — not only for us, but for healthcare organizations around the country."

Bringing Threat Intelligence to Security Playbooks

Why Recorded Future customers choose Splunk Platform

Industry

- Technology

Splunk Use Cases

- Security
- Cybersecurity
- Security Orchestration Automation and Response
- Incident Response Management
- Security Monitoring
- Application Monitoring

Challenges

- Clients conducting operations manually
- Redesigning processes for individual clients

Business Impact

- Clients able to identify threats 10% faster
- Clients able to events 63% quicker
- Observed a 32% increase in overall efficiency

Splunk Products

- Splunk SOAR
- Splunk Enterprise Security

> **"Without using automation and orchestration, I don't see how companies are going to be able to face the challenges that they have today. With everything that's going on, companies are overwhelmed. Humans can't do it by themselves."**
>
> — Seth Whitten, VP of Integrations and Strategic Partnerships

Around 40,000 security professionals across 22 industries and six continents depend on Recorded Future for best-of-breed threat intelligence. Recorded Future collects and analyzes vast amounts of data to deliver relevant cyber threat insights in real time. This intelligence allows their customers to improve detection and response, which helps their security teams make better decisions faster.

Meet Seth Whitten, VP of integrations and strategic partnerships at Recorded Future. We sat down with him to talk about the Splunk and Recorded Future partnership, and how the Splunk® SOAR integration has made an impact. "Our largest integration right now is Splunk® Enterprise," he says. "For us, it was natural to move into SOAR. We have a lot of clients who are driving events out of their SIEM tools, and want to be able to better act on them."

Why SOAR

Prior to SOAR, Recorded Future clients would conduct their operations manually. "They would have to go into our platform, pull out the information they were looking for, and make a decision on whether or not to move forward when investigating an alert or triaging things in their environment," Seth says.

With SOAR, Recorded Future customers can automate those otherwise manual, repetitive security operations tasks. Security alerts that previously took minutes or hours to resolve, now only take seconds with SOAR's automation capabilities. As a result, Recorded Future customers have increased their operational efficiency and significantly reduced response time to security events.

Seth says his favorite part of SOAR is the way his team can structure playbooks. "It's easier for us to work with SOAR in the field because we have the predefined playbooks that we can get up and running for clients a lot quicker, without taking them through the redesigning process," he says.

Recorded Future and SOAR

SOAR playbooks automate a sequence of security actions at machine speed, enabling clients to create customized and repeatable security workflows. For example, a SOAR playbook can instruct your sandbox to detonate a file, or tell your endpoint security tool to quarantine a device. With more than 100 predefined, out-of-the-box playbooks, SOAR helps customers ensure that they have a repeatable and auditable process around security operations.

"We use natural language processing and artificial intelligence to correlate data and make it available for clients to use when solving problems."

— Seth Whitten, VP of Integrations and Strategic Partnerships

"Our clients want to be able to get through all of their alerts. They want to prioritize them. They want to act. They want to drive outcomes. SOAR was a natural place for us to put our data to help drive action around those outcomes."

— Seth Whitten, VP of Integrations and Strategic Partnerships

The integration with Recorded Future gives those playbooks access to threat intelligence data. When an alert is passed over to SOAR — either from Splunk® Enterprise Security or as a new artifact — a playbook is invoked, which is automatically enriched with risk scores and associated context from Recorded Future. The playbook's decision logic can determine if the alert needs to be escalated to a human analyst if it's risky, or passed over if it's not. As SOAR helps remove false positives from the flow, human analysts have more time to focus on larger problems.

Top Three Benefits

- Identify threats 10% faster
- Respond to events 63% quicker
- 32% increase in overall efficiency

Authentication Data

Use Cases: Security and Compliance, IT Operations, Application Delivery

Examples and Data Sources: Active Directory, LDAP, Identity Management, Single-Sign On

Authentication data provides insight into users and identity activity. Common authentication data sources include:

- **Active Directory:** A distributed directory in which organizations define user and group identities, security policies and content controls.
- **LDAP:** An open standard defined by the Internet Engineering Task Force (IETF) and is typically used to provide user authentication (name and password). It has a flexible directory structure that can be used for a variety of information such as full name, phone numbers, email and physical addresses, organizational units, workgroup and manager.
- **Identity Management:** Identity management is the method of linking the users of digital resources — whether people, IoT devices, systems or applications — to a verifiable online ID.
- **Single Sign-On (SSO):** A process of using federated identity management to provide verifiable, attestable identities from a single source to multiple systems. SSO significantly increases security by tying user credentials to a single source, allowing changes to user rights and account status to be made once, and reflected in every application or service to which the user has access. SSO is particularly important for users with elevated security rights such as system or network administrators that have access to a large number of systems.

Use Cases

Security and Compliance: For security, authentication data provides a wealth of information about user activity, such as multiple login failures or successes to multiple hosts in a given time window, activities from different locations within a given amount of time, and brute force activities. Specifically:

- Active Directory domain controller logs contain information regarding user accounts, such as privileged account activity, as well as the details on remote access, new account creation and expired account activity.
- LDAP logs include a record of who, when and where users log in to a system and how information is accessed.
- Identity Management data shows access rights by user, group and job title (e.g., CEO, supervisor or regular user). This data can be used to identify access anomalies that could be potential threats — for example, the CEO accessing a low-level networking device or a network admin accessing the CEO's account.

IT Ops and Application Delivery: Authentication data supports IT operations teams as they troubleshoot issues related to authentication. For example, application support can be tied to logins, enabling IT operations to see whether users are struggling to log in to applications. For IT operations teams that support Active Directory, logs can be used to troubleshoot and understand the health of Active Directory.

USER DATA

Antivirus

Use Cases: Security and Compliance

Examples: Kaspersky, McAfee, Norton Security, F-Secure, Avira, Panda, Trend Micro

The weakest link in corporate security are individuals, and antivirus is one way to protect them from performing inadvertently harmful actions. Whether it's clicking on an untrustworthy web link, downloading malicious software or opening a booby-trapped document (often one sent to them by an unsuspecting colleague), antivirus can often prevent, mitigate or reverse the damage.

So-called advanced persistent threats (APTs) often enter through a single compromised machine attached to a trusted network. While not perfect, antivirus software can recognize and thwart common attack methods before they can spread.

Use Cases

Security and Compliance: Antivirus logs support the analysis of malware and vulnerabilities of hosts, laptops and servers; and can be used to monitor for suspicious file paths. It can help identify:

- Newly detected binaries, file hash, files in the filesystem and registries.
- When binaries, hash, or registries match threat intelligence.
- Unpatched operating systems.
- Known malware signatures.

Mail Server

Use Cases: Security and Compliance, IT Operations

Examples: Exchange, Office 365

Email remains the primary form of formal communication in most organizations. As such, mail server databases and logs are some of the most important business records. Due to their size and tendency to grow without bounds, email data management typically requires both data retention and archival policies so that only important records are held and inactive data is moved to low-cost storage.

Use Cases

Security and Compliance: Mail server data can help identify malicious attachments, malicious domain links and redirects, emails from known malicious domains, and emails from unknown domains. It can also be used to identify emails with abnormal or excessive message sizes, and abnormal email activities times.

IT Ops: Email messages and activity logs can be required to maintain compliance with an organization's information security, retention and regulatory compliance processes. Mail server transaction and error logs also are essential debugging tools for IT problem resolution and also may be used for usage-based billing.

Vulnerability Scanning

Use Case: Security and Compliance

Examples: ncircle IP360, Nessus

An effective way to find security holes is to examine infrastructure from the attacker's point of view. Vulnerability scans probe an organization's network for known software defects that provide entry points for external agents. These scans yield data about open ports and IP addresses that can be used by malicious agents to gain entry to a particular system or entire network.

Systems often keep network services running by default, even when they aren't required for a particular server. These running, unmonitored services are a common means of external attack, as they may not be patched with the latest OS security updates. Broadscale vulnerability scans can reveal security holes that could be leveraged to access an entire enterprise network.

Use Cases

Security and Compliance: Vulnerability scans yield data about open ports and IP addresses that can be used by malicious agents to gain entry to a particular system or entire network. The data can used to identify:

- System misconfiguration causing security vulnerability.
- Outdated patches.
- Unnecessary network service ports.
- Misconfigured filesystems, users or applications.
- Changes in system configuration.
- Changes in various user, app or filesystem permissions.

APPLICATION DATA

Web Server

Use Cases: Security and Compliance, IT Operations, Application Delivery

Examples: Java J2EE, Apache, Application Usage Logs, IIS logs, nginx

Web servers are the backend application behind every website that delivers all content seen by browser clients. Web servers access static HTML pages and run application scripts in a variety of languages that generate dynamic content and call other applications such as middleware.

Web servers can vary widely, and can include:

- **Java – J2EE:** Java is the most popular programming language due to its versatility, relative ease of use and rich ecosystem of developer tools. Via the J2EE platform, which includes APIs, protocols, SDKs and object modules, Java is widely used for enterprise apps including web applets, middle-tier business logic and graphic front ends. Java is also used for native Android mobile apps.

- **Apache:** Apache is one of the oldest and most-used web servers on the internet, powering millions of enterprise, government and public sites. Apache keeps detailed records of every transaction: every time a browser requests a web page, Apache log details include items such as the time, remote IP address, browser type and page requested. Apache also logs various error conditions such as a request for a missing file, attempts to access a file without appropriate permissions or problems with an Apache plug-in module. Apache logs are critical in debugging both web application and server problems, but are also used to generate traffic statistics, track user behavior and flag security attacks such as attempted unauthorized entry or DDoS.

- **Application Usage Logs:** Like Apache web logs, collecting application usage can provide valuable information to multiple stakeholders including developers, IT, sales and marketing. Depending on how granular the measurement, usage tracking can assist developers in identifying application features that are most and seldom used, those that users have trouble with and areas for future enhancement. For customer-facing applications, usage logs provide sales and marketing teams insight into the effectiveness of online and app-based sales channels and promotions, data about sell-through and transaction abandonment, and information for potential cross-sales promotions.

Use Cases

Security and Compliance: Web logs record error conditions such as a request to access a file without appropriate permissions and also track user activity that can flag security attacks such as attempted unauthorized entry or DDoS. It can also help to identify SQL injections and support correlating fraudulent transactions.

- Since Java apps frequently access network services and sensitive databases, security teams can use log data to vet the integrity of J2EE apps, identify suspicious application behavior and application vulnerabilities.
- Apache web logs can alert to security attacks such as attempted unauthorized entry, XSS, buffer overflows or DDoS.
- Like web logs, generic application usage logs can alert security teams to unauthorized access such as someone consuming more resources than normal, or using applications at odd hours.

IT Ops and Application Delivery: Web logs are critical in debugging both web application and server problems, but also are used to generate traffic statistics that are useful in capacity planning. Web server data can provide varying information for IT operations teams:

- J2EE data can help operations teams diagnose problems with three-tier applications that involve the interaction between web, middleware and database servers.
- In aggregate, Apache web logs can show activity of a web service. Drilling into details can reveal infrastructure bottlenecks and indicate downstream issues.
- Application usage logs can help IT operations teams with infrastructure capacity planning, optimization, load balancing and usage-based billing by providing detailed records of resource consumption.

MIDDLEWARE DATA

Firewall

Use Cases: Security and Compliance, IT Operations

Examples: Palo Alto, Cisco, Check Point

Firewalls demarcate zones of different security policies. By controlling the flow of network traffic, firewalls act as gatekeepers collecting valuable data that might not be captured in other locations due to the firewall's unique position as the gatekeeper to network traffic. Firewalls also execute security policy and thus may break applications using unusual or unauthorized network protocols.

Use Cases

Security and Compliance: Firewall logs provide a detailed record of traffic between network segments, including source and destination IP addresses, ports and protocols, all of which are critical when investigating security incidents. The data may also reveal gaps in security policy that can be closed with tighter construction of firewall rules. Firewall data can help identify and detect:

- Lateral movement
- Command and Control traffic
- DDoS traffic
- Malicious domain traffic
- Unknown domain traffic
- Unknown locations traffic

IT Ops: When network applications are having communication problems, network security policies may be the culprit. Firewall data can provide visibility into which traffic is blocked and which traffic has passed through — helping identify if you have an app or network issue.

Intrusion Detection/ Prevention

Use Case: Security and Compliance

Examples: Tipping Point, Juniper IDP, Netscreen Firewall, Juniper NSM IDP, Juniper NSM, Snort, McAfee IDS

IDS and IPS are complementary, parallel security systems that supplement firewalls — IDS by exposing successful network and server attacks that penetrate a firewall, and IPS by providing more advanced defenses against sophisticated attacks. IDS is typically placed at the network edge, just inside a perimeter firewall, although some organizations also put a system outside the firewall to provide greater intelligence about all attacks. Likewise, IPS is typically placed at the network perimeter, although it also may be used in layers at other points inside the network or on individual servers. IPS usually works by dropping packets, resetting network connections and blacklisting specific IP addresses or ranges.

Use Cases

Security and Compliance: IDS logs provide security teams detailed records of attacks including the type, source, destination and port(s) used that provide an overall attack signature. Special signatures may trigger alarms or other mitigating actions. IPS provide the same set of attack signature data, but also may include a threat analysis of bad network packets and detection of lateral movement. This data can also detect command and control traffic, DDoS traffic, and malicious or unknown domain traffic.

NETWORK DATA

Network Access Control (NAC)

Use Case: Security and Compliance

Examples: Aruba ClearPass, Cisco ACS

Network access or admission control is a form of client/endpoint security that uses a locally installed software agent to pre-authorize connections to a protected network. NAC screens client devices for contamination by known malware and adherence to security policies such as running an approved OS with the most recent patches. Clients failing NAC screens are rerouted to an isolated quarantine network until any detected problems are corrected.

Use Cases

Security and Compliance: NAC software collects data about the connecting clients such as an inventory of installed client software, compliance with security policies, OS and application patch versions, accessibility by remote access clients and user access to protected networks. NAC logs provide security teams with a detailed profile of a client's state and activity. It can provide details into unauthorized device connections and be used to correlate users/IP to a physical network location.

Network Switches

Use Cases: Security and Compliance, IT Operations

Examples: Ethernet Switch, Virtual Switches

Switches are network intersections, places where packets move from one network segment to another. In their purest form, switches work within a particular IP subnet and can't route Layer 3 packets to another network. Modern data center designs typically use a two-tier switch hierarchy: top-of-rack (ToR) switches connecting servers and storage arrays at the edge and aggregation or spine switches connecting to the network core. Although ethernet switches are far more widespread, some organizations also use fiber channels or infiniband for storage area networks or HPC interconnects, each of which has its own type of switch.

Use Cases

Security and Compliance: Switch data, often captured as NetFlow records, is a critical data source for flagging advanced persistent threats, analyzing traffic flows for unusual activity and identifying potential data exfiltration. As a wire-level data source, switch statistics are almost impossible to spoof and thus a crucial source of security data. This data can also be used to correlate users or IP addresses to a physical network location.

IT Ops: Operations teams use switch logs to see the state of traffic flow, such as source and destination, class of service and causes of congestion. Logs also can show traffic statistics in the aggregate, by port and by client, and whether particular ports are congested, failing or down.

Proxies

Use Cases: Security and Compliance, IT Operations

Examples: Blue Coat, Fortinet, Juniper IDP, Netscreen Firewall, Palo Alto Networks, Palo Alto Networks config, Palo Alto Networks system, Palo Alto Networks threat, Palo Alto Networks traffic, nginx

Network proxies are used in several ways in IT infrastructure: as web application accelerators and intelligent traffic direction, application-level firewalls, and content filters. By acting as a transparent 'bump-in-the-wire' intermediary, proxies see the entire Layer 7 network protocol stack, which allows them to implement application-specific traffic management and security policies.

Use Cases

Security and Compliance: Security teams are interested in proxies as application-layer firewalls. Here, proxy records can identify details about specific content traversing network control points including file names, types, source and destination, and metadata about the requesting client such as OS signature, application and username/ID (depending on the proxy implementation). The data can also be used to help detect command and control traffic, malicious domain traffic and unknown domain traffic.

Web proxies and some next generation firewalls may act in a transparent or explicit mode communicating with HTTP(S) servers on behalf of a client. Using a number of related technologies, the request and response can be inspected and permitted, or blocked, based on user role, site or resource category or attack indicator. Data logged in the events can potentially be used in detective correlation.

IT Ops: Operations teams often use proxies embedded in an application delivery controller (ADC), a more advanced, Layer 7-aware version of a load balancer. In this context, proxy logs can provide information about incoming requests and traffic distribution among available resources.

System Logs

Use Cases: Security and Compliance, IT Operations, Application Delivery

Examples: Unix, Windows, Mac OS, Linux

Every OS records details of its operating conditions and errors, and these time-stamped logs are the fundamental and authoritative source of system telemetry. Depending on the OS, there may be separate logs for different classes of events, such as routine informational updates, system errors, boot loader records, login attempts and debug output. Error logs often aggregate records from multiple subsystems and OS services or daemons, and, thus, are a definitive source of troubleshooting information.

Use Cases

Security and Compliance: System logs include a variety of security information such as attempted logins, file access and system firewall activity. These entries can alert security teams to network attacks, a security breach or compromised software. They also are an invaluable source of information in forensic analysis of a security incident. For example, the data can be used to identify changes in system configurations and commands executed by users or privileged users.

IT Ops and Application Delivery: System logs often are the first place operations teams turn when troubleshooting system problems, whether with the OS, hardware or various I/O interfaces. Since a particular problem often manifests itself with errors in multiple subsystems, correlating log entries is one of the best ways of identifying the root cause of a subtle system failure.

Server Logs

Use Cases: Security and Compliance, IT Operations, Application Delivery

Server operating systems routinely record a variety of operational, security, error and debugging data such as system libraries loaded during boot, application processes open, network connections, file systems mounted and system memory usage. The level of detail is configurable by the system administrator; however, there are sufficient options to provide a complete picture of system activity throughout its lifetime. Depending on the subsystem, server logs are useful to system, network, storage and security teams.

Use Cases

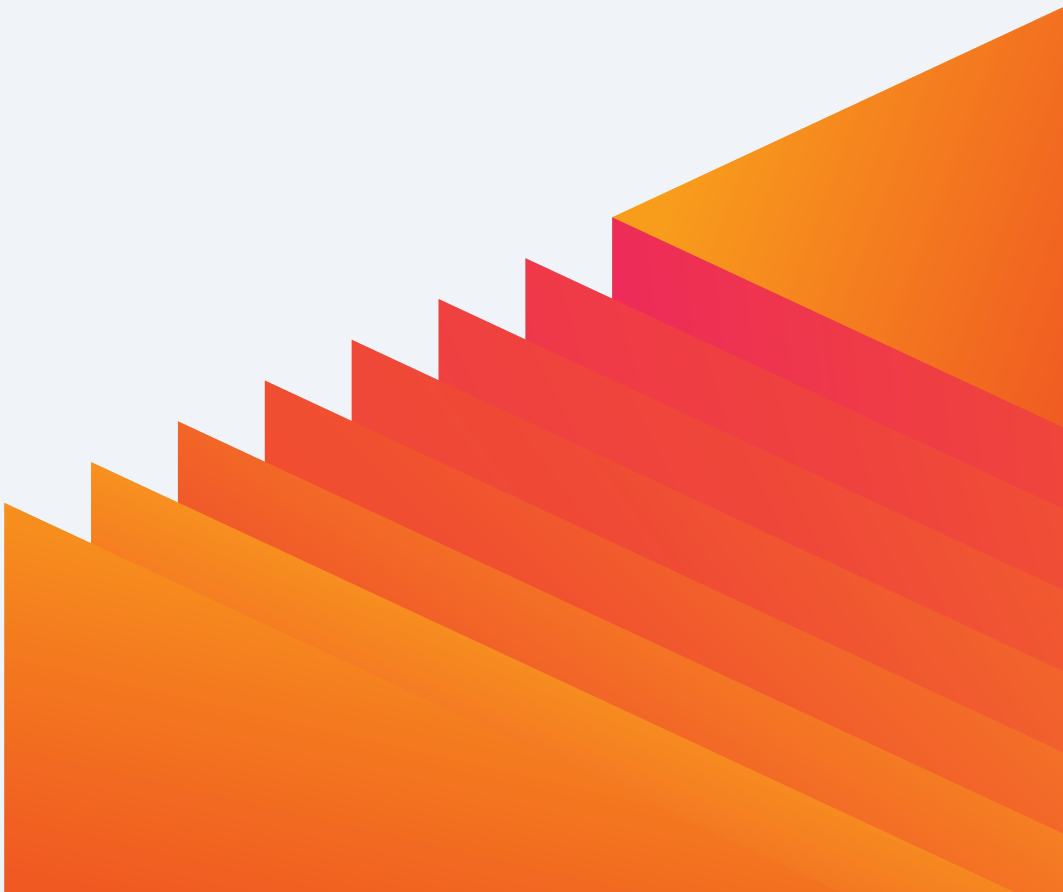
Security and Compliance: Server logs include data from security subsystems such as the local firewall, login attempts and file access errors that security teams can use to identify breach attempts, track successful system penetrations and plug vulnerabilities. Monitoring server logs such as file access, authentication and application usage can help secure infrastructure components.

IT Ops and Application Delivery: Server logs provide a detailed record of overall system health, and forensic information about the exact time of errors and anomalous conditions that are invaluable in finding the root cause of system problems.

About **Splunk.**

Splunk turns data into doing with the Unified Security and Observability Platform. Splunk technology is designed to investigate, monitor, analyze and act on data at any scale. Join millions of passionate users by trying Splunk for free.

Free Trial



splunk>

23-251635-Splunk-theessentialguidetosecuritydata-EB-102