F5 LABS

USING F5 LABS

APPLICATION THREAT INTELLIGENCE

How Threat Intelligence Can Be The
Game Changer For Your Security Program

January 2017

By Ray Pompon and Sara Boddy

TABLE OF CONTENTS

Despite All Our Advances, We're Still Falling Behind 03

- Change Is Accelerating 03
- Data Is Beyond Our Ability to Manage 04
- Threats Are Evolving 04
- Apex Predators Have Emerged 05
- Applications Are in the Crosshairs 05
- Most Authentication Security Is Pathetic 06
- New Regulations Keep Piling On 06
- Nobody Cares, They Just Want Us to Fix It 06

WhadaYaGonnaDo? 08

- Compliance Is No Help 09
- Isn't There Something We Can Buy to Make This Go Away? 09

Enter Threat Intelligence 09

- Machine-to-Machine Threat Intelligence 09
- Human-to-Human Threat Intelligence 11
- Human Threat Intelligence Is What Most People Really Want 12

Why Threat Intelligence is a Game Changer 13

Introducing F5 Labs 14

- F5 Labs' Mission: To Help Secure the Internet 14
- What the F5 Labs Threat Research and Intelligence Team Does 14
- What You'll Find at F5 Labs 15
- F5 Labs Threat Intelligence Assets 16

DESPITE ALL OUR ADVANCES, WE'RE STILL FALLING BEHIND

Cyber security has been a work in progress for decades. As security pros, we've learned a lot about how to defend our networks. We have more tools at our disposal than ever before. And for the first time in history, we are receiving tangible support from upper management for security work. We've never had it so good, right? Yet, we feel more helpless than ever. Most of the time, we're overwhelmed and feel like we're perpetually playing catch up.

CHANGE IS ACCELERATING

One reason is because everything is happening too fast. Technology is moving fast—mobile consumer technology, cloud-dispersed data and apps, global remote workforce, constellations of identities, galaxies of applications, big data silos, the Internet of Things (IoT). Entire new paradigms of technology usage are washing over our culture at break-neck speed. A new technology-driven service disrupts the status quo, and then we quickly see everyone copycatting the service in different sectors. First, Amazon, and then the Amazonification of everything. And the same with Uber, and now the Uber-of-X. From Myspace to Facebook to social networking everywhere. The quick move to the web, and cloud, and now mobile. As soon as consumers begin to lean into a new technology, it soaks into everyday use in a matter of months. Even our foundational infrastructure is morphing under our feet. It's hard to remember a time when an operating system remained current for more than a few years.

If we just ignore the new technology and new ways of applying it, we cannot ignore the sheer mass of people and devices being assimilated into the global collective every second.

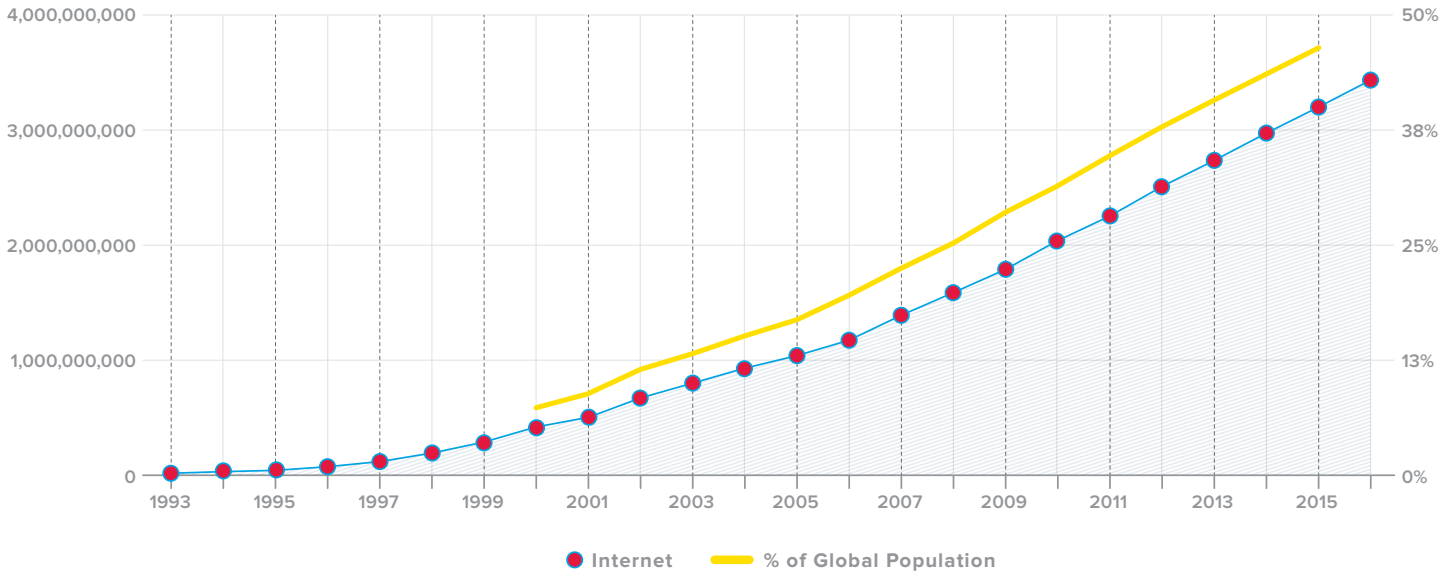


Figure 1: Internet users with percentage of global population[1]

[1] http://www.Internetlivestats.com/Internet-users

DATA IS BEYOND OUR ABILITY TO MANAGE

Then there is the nature of data itself. With every new net citizen and every new device comes a multitude of new data streams. There are the data streams themselves, then metadata streams describing the data streams, and then the saved data analysis of the data streams and metadata. It's all being generated, crunched, transmitted, stored, and backed up somewhere.

And let's not forget how IT actually works; all data transfers imply a perfect copy of the original. Every byte we send has been duplicated numerous times along its journey from sender to receiver. Consider an email sent from your mobile device: a copy is saved locally, a copy is saved on the mail farm where the mailbox lives (and all its backups), and then this is all repeated for each receiver of that email. Data is everywhere and it's snowballing at an exponential rate.

All of this data, and it's gushing in and out faster than ever before. As a result, the Internet is constantly growing, with "high" (100 Mbps) bandwidth circuits becoming increasingly available at ever more affordable rates in first-world countries, and the expansion of Internet services into countries that a few years ago barely had connectivity.

Even if cyber security tools and techniques could keep pace with the threats, the sheer volume of new technologies, data sources, and rivers of new data is becoming too much to reasonably defend. The expansion of security tools, trained security personnel, and cyber-savvy law enforcement is growing nowhere nearly as fast. The only thing that is keeping pace with the rapid growth of technology is the threats.

THREATS ARE EVOLVING

The threat landscape has evolved from the early days of hacking for fun or fame, to hacking for profit. Once capitalism got tangled up in hacking, the market for cybercrime really took off. Suddenly we saw organized crime, boutique cybercrime, cybercrime entrepreneurs, and long-tail hacking schemes.

Note that with each step of the evolution, all the previous incarnations still exist. The Internet ecosystem is full of parasites, young and old.

MOTIVE	SCHEME	EXAMPLES
Self-education, fun, fame ("Look what I can do!")	Self-propagating malware as vandalism	Morris worm, Melissa virus
Personal politics ("We hate you so we'll take you down.")	Malware vandalism adds a denial-of-service component	Blaster, SQL Slammer, MafiaBoy, DDoS
Simple data plunder from organizations (direct grab of data that's easily liquidated)	Credit card fraud, ID theft	Russian hackers Ivanov and Gorshkov

Long tail profiteering (make pennies a day from thousands of infected hosts)	Spam relay, click-jacking, PayPer-Install fraud, Bitcoin mining, bot herding	Maxwell (donttrip) botnet
Direct consumer fraud (fraud that goes undetected)	Trick home users out of their money	Fake anti-virus programs
Consumer extortion (easier, pays faster)	Demand money from home users to get their data back	Crypto ransom
Organizational extortion (bigger pay-offs that pay faster)	Demand money from organizations	Crypto ransom of file shares, DDoS protection racket
Relay platform (“getaway car”)	Use stolen resources to aid in larger, more complex crimes	Phishing platforms, malware C&C servers, SEO injection of fake news, malware attack drones
Espionage, IP theft for economic gain	Stolen credentials to steal intellectual property for resale	Spear phishing attacks, low-and-slow network penetrate and pivot

APEX PREDATORS HAVE EMERGED

Like a savvy hunter of wild game, the modern attacker selects and stalks his prey and then after making the kill, makes effective use of every part of the carcass. Every component of a victim’s compromised machine is exploited: the credentials, the resident data, the network access, and the stored trust relationships.

If the criminals weren’t enough of a threat, cyber attacks are now another weapon in the arsenal of modern warfare and espionage. If a government or well-funded non-government entity isn’t doing the dirty work themselves, they could be hiring hacker mercenaries to do their privateering for them. Organizations that aren’t the direct target often become part of the collateral damage, finding their networks rummaged through or torn open by attackers on their way to get to someone else or their data. Innocent organizations can also be knocked out in the “blast radius” of large-scale distributed denial-of-service attacks because of the sheer size and imprecision of such attacks. If they’re using the same Internet services (whether web hosting platform, DDoS protection service, or DNS provider) as the DDoS target, they’re offline just as fast and as long as the victim is.

APPLICATIONS ARE IN THE CROSSHAIRS

In most of these attacks, the Internet applications are the target because that’s where the data resides that attackers are after. Since infrastructure technology is the slowest to evolve, our defense tools are strongest and most reliable at the network perimeter. So attackers, being cunning and motivated, shift their threat vectors to the “softer” parts: the applications.

Not only are applications changed out and updated constantly, but many are bespoke to the organizations using them. A custom web application that powers an Internet start-up is often hammered together at the last minute, designed for maximum desirable features and attractiveness. If it sticks, it'll be secured—eventually. In the meantime, it's barely security-tested and quite vulnerable.

MOST AUTHENTICATION SECURITY IS PATHETIC

Even the strongest of applications require users to log in and use them. Users gain access by authenticating themselves, usually with a username and password. Most of the time, the username is the user's email address, trivially discoverable. The password is not as bad, but pretty close. So-called best practices like "use 8 characters with upper/lower case and a number" are not cutting it. Especially when many users simply type in passwords like these:

A compromised identity can be the easiest way in the front door, and studies have shown it's the most common weakness is cyber security.

How are passwords stored within organizations? Recent large-scale breaches of millions of usernames and passwords have shown the answer to be: *not very securely*. Secure practices recommend that each password be cryptographically hashed with a unique salt. However, the headlines have proved that a majority of organizations overlook this crucial protection[2], resulting in mother lodes of usernames and passwords lying around for crooks to plunder. Given that users frequently reuse usernames and passwords from one system to another, this further degrades the value of this type of authentication.

NEW REGULATIONS KEEP PILING ON

With all the headlines of huge breaches and outages, our lawmakers are ramping up what they do best: creating more paperwork and rules for us to follow. Nearly every major country and business sector is in the process of rolling out new cyber security regulations to define how and what we need to do in defending our networks. Civil class action suits are starting to multiply as lawyers smell blood in the water from the shipwrecks of breached companies.

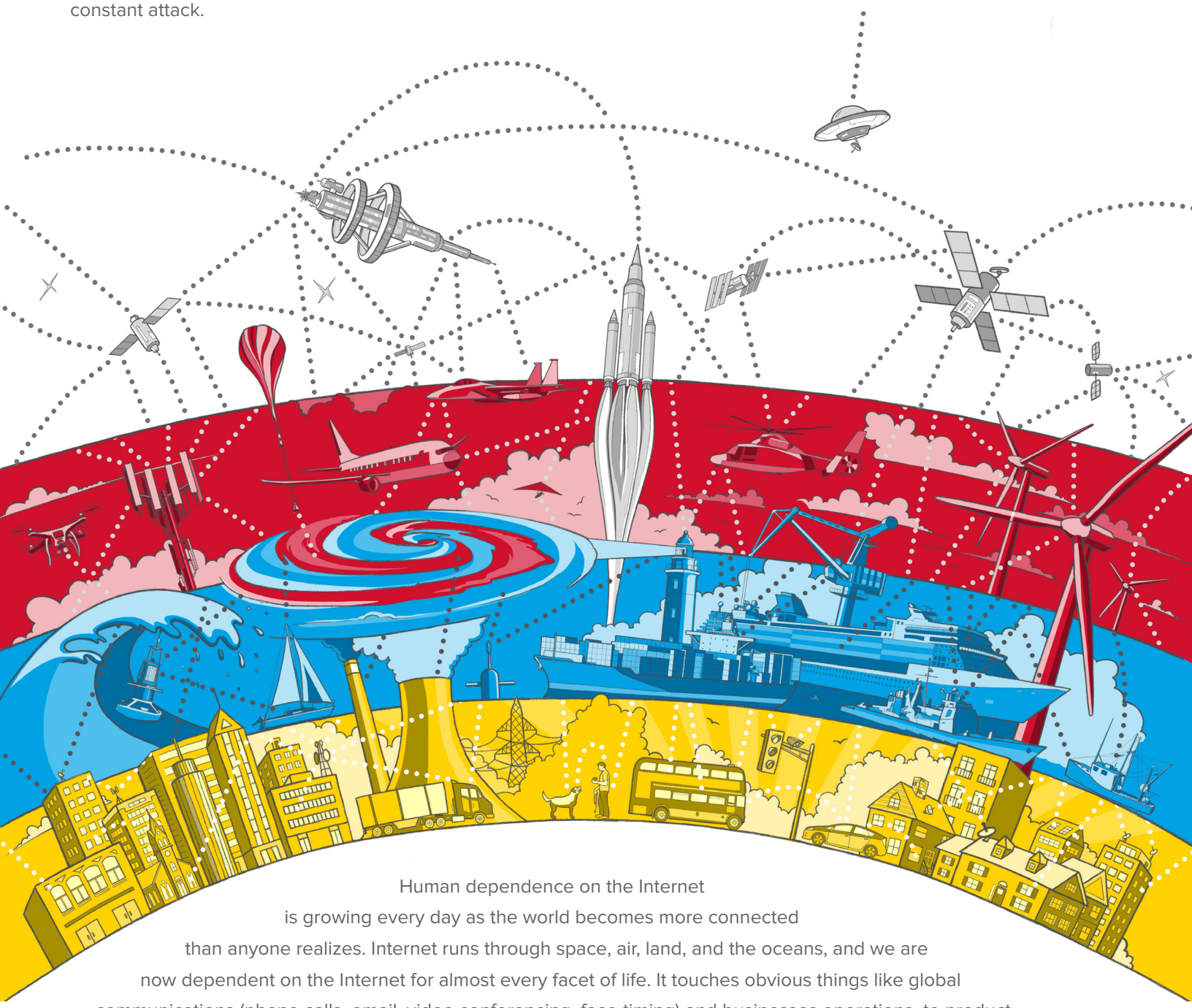
NOBODY CARES, THEY JUST WANT US TO FIX IT

There are so many attackers and so many ways our systems can be attacked. The security team cannot protect everything at once. Worse, the users push back when too much security is imposed, making it harder for them to get things done. In the end, the users just need their applications to be running as expected with no interference from either hackers or the security team. Many feel that if a solution is judged to be "insecure" then it's security's job to make it secure and leave them alone. And things can never, ever go down.

Depending on the industry sector (financial, medical), some users care a lot about the integrity and confidentiality of their data. It is a truth universally acknowledged that a critical system in possession of users must be in want of a near perfect

[2] https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet#Use_a_cryptographically_strong_credential-specific_salt

uptime. *The applications we run must stay up when under attack.* Uptime in some environments is so important that even when a system is compromised, it must still be available. This adds to the overloaded work stack of making applications highly available, even while supporting incident response. And, by the way, most of our Internet applications are under constant attack.



Human dependence on the Internet is growing every day as the world becomes more connected than anyone realizes. Internet runs through space, air, land, and the oceans, and we are now dependent on the Internet for almost every facet of life. It touches obvious things like global communications (phone calls, email, video conferencing, face-timing) and businesses operations, to product purchases (point-of-sale, online, Apple Pay), and navigation systems (Google Maps, air traffic control systems). It is also embedded in our infrastructure that runs our faucets and farms, our power grids, the 911 system, and digital signage guiding us on the freeway or to our gate at the airport. We've reached the point where it's becoming infeasible for most of us to live "off the grid."

WHADAYAGONNADO?

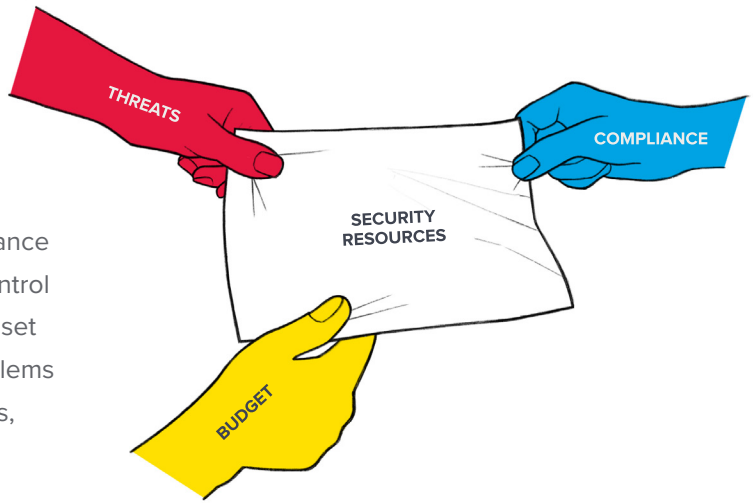
In cyber security, the question is always which of these thousand things should we be doing right now? What is our biggest threat at this moment? Many of us have the big known threats covered and are keeping our defenses running this way:

- Implement least privilege and zero trust. Basic email should not be trusted. Basic Internet browsing should not be trusted. Filter, test, and segment.
- Train users to be on the alert and report suspicious activity so you can block attacks before they spread. Reality is that humans are easy to exploit, and hackers are going phishing in an overstocked pond.
- Assume breach and remember that data is the goal, applications are the targets. Firewalls that can't protect applications are as useless as a tennis racket in a rainstorm.
- Learn what is going on in your organization and keep up to date. An intrusion detection system is useless unless you have someone with the right mindset and training who's looking at the output all the time.
- Protect the perimeter, yes, but remember applications and identities pass freely and often invisibly through that perimeter.
- Encrypt whatever possible, both in flight and at rest. Encrypt with care because bad encryption looks just like good encryption. Right up until it breaks.
- Have an effective vulnerability management program. Scan, test, and scan again. Vulnerabilities are never a point-in-time occurrence; you must have a continual testing process aligned to your development cycles and patch releases of your vendors.
- If you can't do it yourself, get help. Security-as-a-service is powerful when it comes to effectively managing high risk controls that require 24x7 rapid response by highly skilled engineers.
- Manage user identities. Use federation and single sign-on where possible to keep things organized and improve authentication.
- Gain visibility into your SSL/TLS data stream and manage it. Remember, the bad guys use encryption tools. Their malware is hiding in SSL/TLS passing right through your perimeter and landing in your users' browsers.
- Have a DDoS response worked out. Whether you consider yourself a target or not, the odds are you will experience DDoS effects.

If we're doing all of these things, we've met the minimum bar for basic survival against most of the common Internet threats.

But, then what?

COMPLIANCE IS NO HELP



Having to adhere to compliance requirements is a double-edged sword. On the positive side, it forces management to give us the resources we need to deal with the threats. But compliance can also force us to adopt controls to deal with irrelevant threats and leave us with no support for critical risks. Most compliance requirements are nothing more than pre-computed risk control measures based on estimations of the actual threat and asset coverage. In other words, they will cover some of our problems but will be a poor fit for others. For many security programs, they are just another requirement tugging away at already stretched resources.

Best practices are not much help, either. There are so many of them and most are vaguer than compliance requirements in terms of fitting your needs.

ISN'T THERE SOMETHING WE CAN BUY TO MAKE THIS GO AWAY?

We wish. There are lots of solutions for lots of threats. More now than ever, but we can't possibly implement them all. After all, we've got limited resources. So, how many control implementations can we reasonably deploy? Consider all the big IT projects that are overpromised and poorly fitted to the problem at hand. We need to choose carefully before we start buying new tools.

We know we can do this. What we know we need to do is align our security resources to reflect the threats to your organization. We need to know what applications and data are targeted. This problem cannot be unsolvable or unachievable. But we also know if that if we go it alone, we might be in over our heads.

ENTER THREAT INTELLIGENCE

Threat Intelligence—the concept of collecting, contributing to, and sharing global attack and exploit activity—isn't new, but it is a hot topic in the cyber security world today. Vendor booths at security trade shows seemed to be all about threat intelligence. This is both a good thing—because threat intelligence is a powerful tool in managing security—but also a bad thing—because the market is over-saturated with dozens of vendors reporting on the same threats and information.

First, let's be clear about what we're talking about. There are two kinds of threat intelligence. Both kinds have been around for a long time and are now experiencing a re-emergence with slicker interfaces and more powerful capabilities.

MACHINE-TO-MACHINE THREAT INTELLIGENCE

The most common contemporary type is a machine-consumable data feed of known threat indicators. This kind of automated feed, consumed by intelligence analysis engines, combines external threat data with internally observed

events. Correlation between the two sets of data can yield new insights on potential internal threats to an organization. For a simple example, an external threat intelligence feed could provide a list of known malware filenames and associated botnet-controlled IP addresses. This could be cross-referenced against firewall usage logs to see if any internal users have been visiting known dangerous sites. The prevailing format for this kind of threat feed is the Structured Threat Information eXpression (STIX™)[3].

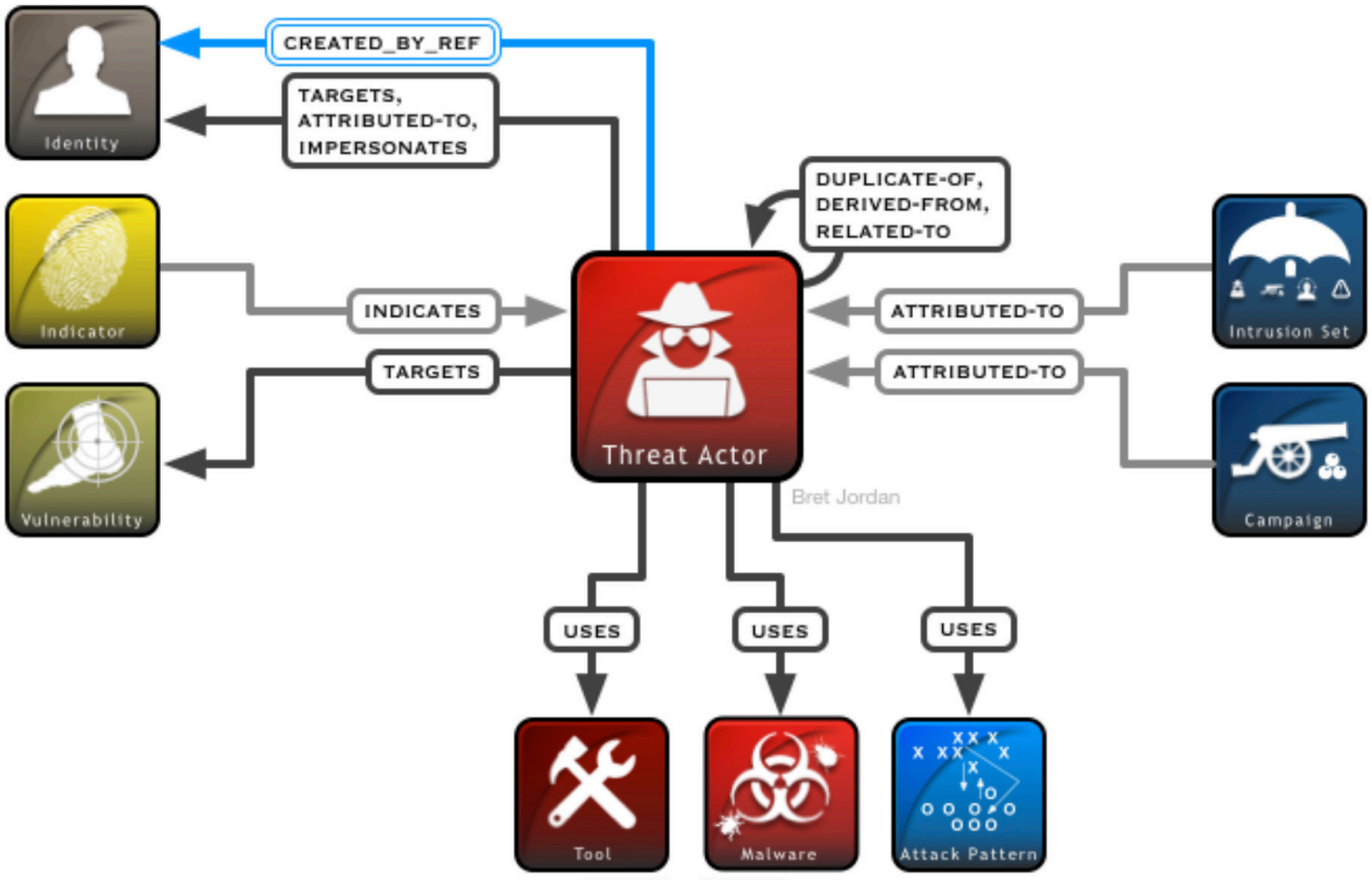


Figure 2: STIX 2.0 Threat Actor Relationships[4]

Leveraging these kinds of feeds is both a science and an art. Automated feeds must be weighted for data quality and trustworthiness. If threat intelligence feeds are consumed unfiltered, untrained security administrators can become swamped with misleading alerts and false positives. In cases where threat feeds are linked to automated traffic-blocking devices, such as firewalls, some users have issues with legitimate traffic being blocked.

---

[3] http://stixproject.github.io/getting-started/whitepaper/

[4] https://freetaxii.github.io/stix2-object-relationships.html

When feeds are used to just alert or block without applying analysis, this becomes what Marcus Ranum calls "Enumerating Badness," which is one of the "Six Dumbest Ideas in Computer Security... because sometime around 1992 the amount of Badness in the Internet began to vastly outweigh the amount of Goodness."[5] It's a bit distressing that after all these decades, the security industry is still using the same ineffective techniques.

The problem with enumerating badness is that if the bad guys aren't known yet by your threat intelligence feed, they're going to be undetected. Even mature threat feeds, such as malware URL lists that have been common security controls for decades, are failing to keep up with the rapid flux of compromised websites. Some threat intelligence feeds have also been found to contain circular data, meaning their threat data is sourced from another feed. So, if we're combining feeds to try to verify something, we'd only end up being misled by bad data.

On the whole, machine-to-machine threat intelligence is useful to a degree, but to do anything truly innovative with it requires resources and expertise. Otherwise, it's just an enhancement to your virus or IDS signatures.

HUMAN-TO-HUMAN THREAT INTELLIGENCE

The other kind of threat intelligence is as old as warfare itself. Every major era of human conflict has necessitated the collection of information about potential enemy activity. Even George Washington has his Culper Ring of spies to relay information about the British army.

This form of intelligence is created by humans and meant to be consumed directly by humans, which means it is verbal or written, sometimes with accompanying graphics and diagrams. All security professionals, whether they are consuming automated threat feeds or not, consume basic open-source intelligence in the form of blogs, articles, podcasts, videos, and reports from threat researchers, their favorite news outlets, and their vendors.

This kind of threat intelligence is one of the primary sources of useful information that can be used to shape security program design, budgeting, and to control deployment. The word most commonly associated with this is *actionable*. That means the information received is relevant to your situation and based on that, you can make choices that affect future outcomes. If you are the head of security for a community medical facility, for example, threat intelligence about the infection details of ransomware targeting DICOM file repositories is actionable for you. You can now look at additional protection for those infection vectors. Threat intelligence about the command and control networks for password-stealing Trojan malware for an online banking site is not as actionable for you since it doesn't directly apply to you.

The concept of controls appropriate to risk has been around for ages, but it's often implemented haphazardly. Far too often, application front doors are left open via a web application vulnerability or by placing the access keys in the hands of an untrained employee that is easy to spear phish. We spend far too much time implementing a full-scale security program, spending time and money in areas that aren't at risk (low likelihood of exploit and low impact), and not enough time in areas that are frequently targeted, have a high rate of success, and a large impact when a does happen. Threat intelligence should be the evidence driving the prescription of your security controls, what they are targeting, at what strength.

[5] http://www.ranum.coity/computer_security/editorials/dumb/

HUMAN THREAT INTELLIGENCE IS WHAT MOST PEOPLE REALLY WANT

Knowing what kinds of threats are approaching your organization is the kind of guidance you need to bolster defenses and allocate resources. This information can be used to build a meaningful and powerful risk management system to withstand the barrage of attacks a typical organization experiences. This kind of threat intelligence can answer questions like:

- Who is targeting my data and services and why?
- What exploits, out of the hundreds released every week, should I be concerned about?
- How does the newest malware move through my network?
- Where should I look for nefarious activity?
- When should I approach upper management about additional funding for new dangers?
- To quote security analyst and risk management specialist Dan Geer, "Intelligence is that which enables decision making, and in turn, which improves outcomes."[6]

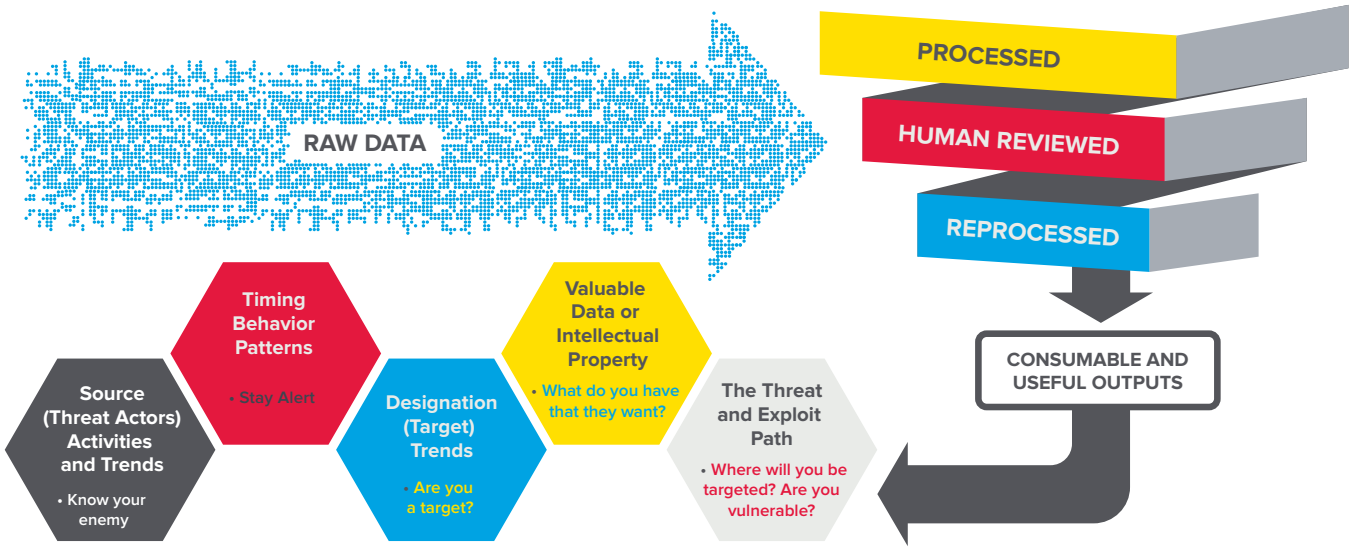


Figure 3: How raw threat data gets processed into actionable intelligence

The downside of human threat intelligence is that the production of it requires advanced skills, proper perspective, and relevant data. Most of all, the recipient of the intelligence must trust that what the source is telling them is real and appropriate. Although there is a lot of threat intelligence to choose from and consume, it is not always easy to determine the trustworthy and relevant sources. Like everything else, you don't have time to read through thousands of articles to find the handful of actionable jewels that will inform your decisions.

---

[6] http://geer.tinho.net/geer.recordedfuture.7x15.txt

WHY THREAT INTELLIGENCE IS A GAME CHANGER

To really understand threat intelligence, we need to look at how our organizations are attacked. One of the common models for this is to look at the entire timeline of a cyber attack.

Simplified, this attack timeline involves a run-up of reconnaissance of a target. This is a long period of increasing reconnaissance that includes probing, scanning, searching for vulnerabilities, collecting email addresses, and poking at servers. Finally, when the attackers have enough, they plan their tactics for penetration and then move swiftly and decisively. The actual attack takes place in hours or days and then the attackers are gone. On average, it takes the victim weeks or months to detect and clean up after the attack. Mapped out, here's what that looks like as a linear sequence with a typical 50-day attack timeframe:

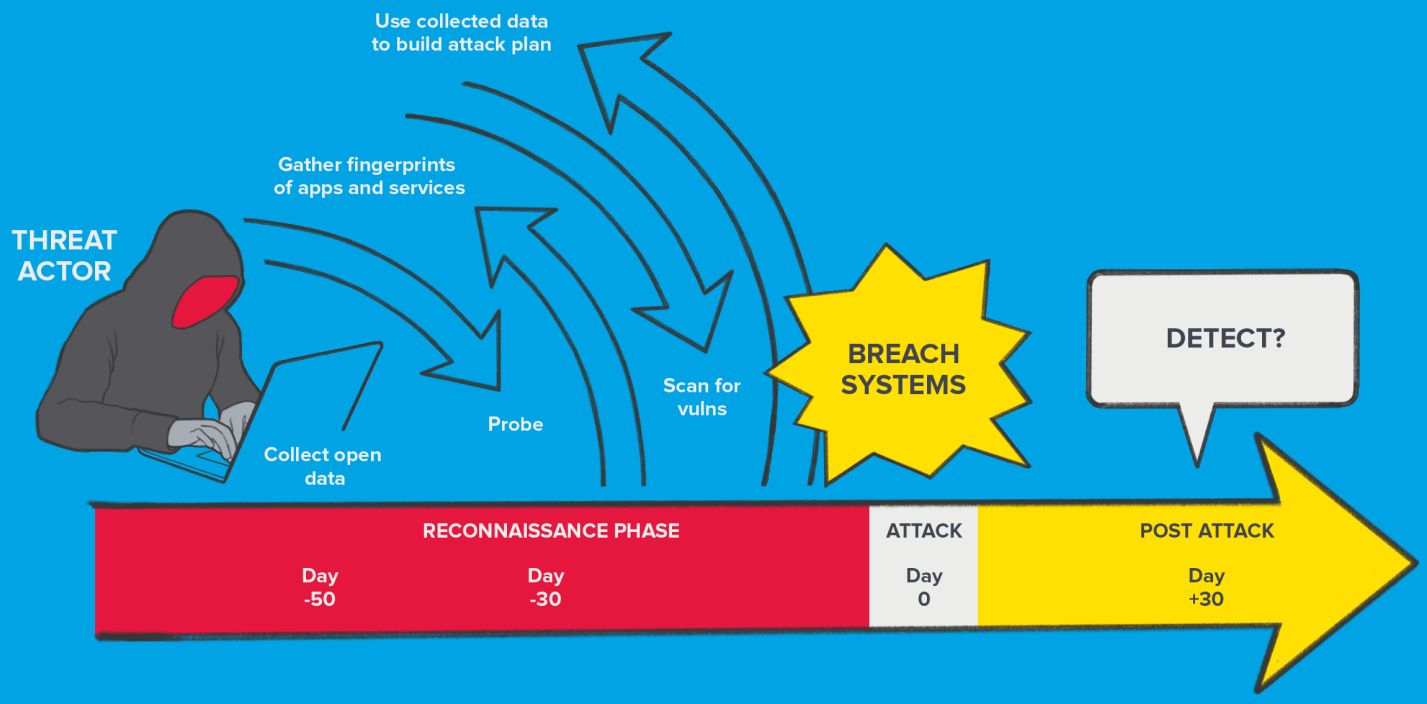


Figure 4: Threat Intelligence gives advanced insight into a hacker's recon phase—the value is before an attack.

Up until now, all of our security controls—firewalls, intrusion detection systems, two-factor tokens, anti-virus—have been focused solely on the attack and post-compromise period. That's the short far-right part of the timeline. That means we have tools to protect us for that brief moment when our networks are actively being ripped open and looted. We have more tools like forensics and log analysis to help us figure out what happened after everything terrible has happened.

Threat intelligence is the first tool that now let's look into that long run-up before the attack happens. Only threat intelligence offers us a way to anticipate an attack coming and prepare for it. We can get ready to dodge, deceive, or defeat it before the attackers make their move. What might this look like?

"My threat intelligence says that this particular threat actor, the Fruit Cup Gang, is working for the Eastern Moofian government, which has targeted drone technology as a potential interest. We're seeing IP addresses known to be associated with the Fruit Cup Gang harvesting our websites to get information about our drone project. We know our sites mention two of our engineers, plus there have been news articles mentioning two other engineers. Let's get those folks in a briefing room and warn them about possible spear phishing attacks."

For the first time, we can move up the timeline to get ready before the trouble begins and stop the attackers in their tracks before we experience any loss or damage. There has never been a tool like this before in security's arsenal.

INTRODUCING F5 LABS

At F5, we care about security; we always have. We know how hard it is to defend an enterprise.

With our history of managed security services and with our teams of security researchers around the globe making continual enhancements to our security products and managed services, F5 has actionable threat intelligence lying around like sawdust in a lumber mill. F5 made the bold decision to formalize and build a team fully dedicated to sharing the rich set of application threat data with the security community. Thus, F5 Labs was born.

The core members of the F5 Labs team were hand-picked from senior cyber security positions at large organizations that had complex security and regulatory needs. The F5 Labs team believes that the Internet exists as a collective whole—its own ecosystem—in which all of us defenders need to join forces. Regardless of our respective organizations, we're all in this security fight together. A breach of one us weakens all of us. Every time a major provider or service is hacked and our user credentials are compromised, all of our networks are at greater risk, productivity is lost, and hundreds of millions of dollars go to clean-up. Meanwhile, our cyber insurance premiums go up, while policy coverage goes down.

F5 LABS' MISSION: TO HELP SECURE THE INTERNET

Many of us work in this field because we love technology and can see the power it wields to solve complex problems. We know that security gets in the way of productive work, but we also know that hacking and breaches are even more counter-productive. We want to see cyber insurance costs go down, fraud to abate, and users to trust their systems and data. We want our friends and families to have secure and reliable home systems, be able to access the resources they want, and feel reassured in buying new technology. We want the Internet to enable new business ideas, new scientific advances, and bring new opportunities to those who have never had them before. We know that cyber security professionals collectively can do better, learn from each other's mistakes, and help each other. We all chose to work in cyber security. We know it's an extremely difficult challenge and we still go ahead and fight every day. We know that if no one does anything, the situation will spiral out of control to the point where the Internet becomes unusable. We want to help.

WHAT THE F5 LABS THREAT RESEARCH AND INTELLIGENCE TEAM DOES

F5 Labs provides the security community with actionable threat intelligence about current cyber threats and future trends so we can all stay at the forefront of the security game. We bring together the expertise of skilled security researchers with the breadth of threat data we collect from multiple sources, including internal research teams, trusted third parties, and our customers. We look at threat actors, the nature and source of attacks, tools and tactics, evolving techniques, and we provide post-attack analysis of significant incidents. Our goal is create a comprehensive, 360 degree view of the threat landscape—the same way our customers experience it. With relevant intelligence, you can focus on specifically where the danger is threatening your network, applications, people, and processes.

WHAT YOU'LL FIND AT F5 LABS

Staying ahead of the game is our goal. We can help you understand what is valuable to attackers so you can map this to your assets and understand what is at stake. We can show you what attackers are doing and why, so you can look for their behavioral patterns within your networks. We'll show you how they attack and what kinds of damage they do so you can prepare your incident response playbook.

What distinguishes F5 Labs from others is that we process our threat intelligence into Who, What, When, Why, How, and What's Next. But it's not just basic, it's actionable, it's usable.

The questions we seek to answer for you are:

- **What:** What are the current threat trends and projections over the next 1, 3, or 5 years? And what are people doing about it? What are common threats to your industry? What are common threats to your country or geography? What types of systems and processes are targeted the most? What are the primary ways hackers are getting in, regardless of industry or geo location? What were the root causes of some of the most damaging hacks, most importantly, in your industry? What are attack trends by target and type? What is it about your organization that makes it a potential target for data breaches and attacks?
- **Who:** General threat actor trends; groups and/or individual actors. Geo trends by IP address, country, ASN, and regional registry. What do you know about the individuals that can conduct attacks on your organization?
- **When:** Timing trends: continual, seasonal, time of day, day of week. Location and Time: timeline of attack
- **How:** Trends by targets: identities and apps
- **Why:** Financial, espionage, notoriety and warfare motives, and what is the risk to your assets? Are they being protected adequately? What is everyone else doing? Why you and not someone else?
- **What's Next:** Attack trends and spikes are early indicators of new exploits and predictions. What should you do?

F5 LABS THREAT INTELLIGENCE ASSETS

By combining our experience and industry perspective, F5 Labs delivers threat intelligence that is both accurate to your needs and precise enough to be actionable. As David Akin says in his first law of spacecraft design[7], analysis without numbers is only an opinion, so we provide data and facts to back up our conclusions. When it comes to actions, we focus on solution-level recommendations that map to common security controls.

In the spirit of the lively 2016 U.S. presidential campaign and the rise of "fake news," the sample threat news headlines on the next page are hypothetical, but the control actions are real and provide a taste of what you can expect from F5 Labs.

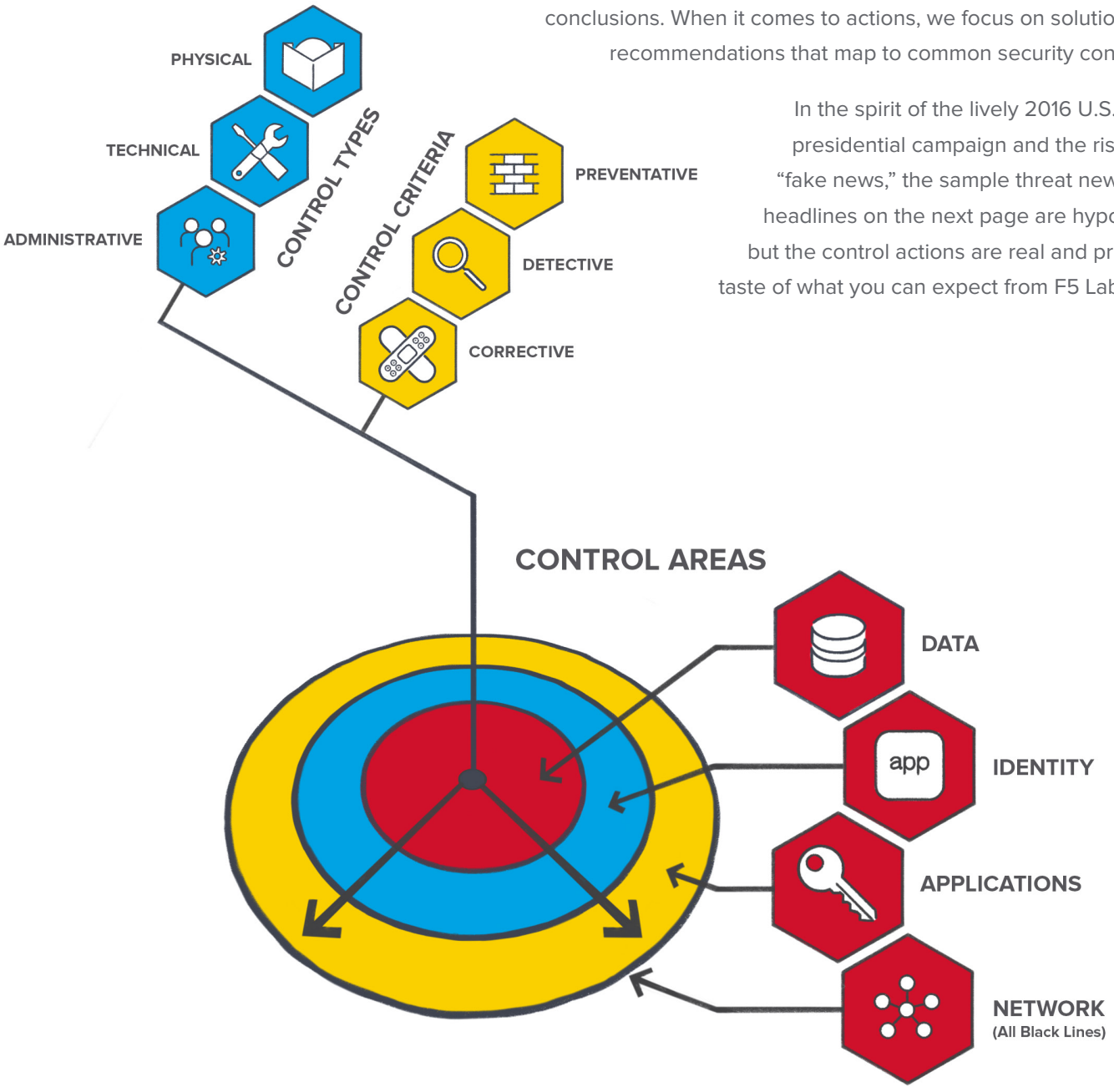


Figure 5: Actionable insights tied to common security controls

[7] http://spacecraft.ssl.umd.edu/akins_laws.html

HYPOTHETICAL HEADLINE	ACTION
"Richard Sherman Calls DDoS Attacks 'Pedestrian,' but They Hit You at Rates Only Service Providers Can Take"	Define your DDoS strategy: on-premises, hybrid, or cloud?
	Sign up with a DDoS cloud scrubbing service.
"Give Up on Usernames and Passwords: Yeehaw Hacked, One Zillion Records Lost!"	Implement SSO to reduce password fatigue.
	Force a reset on all user identities.
	At a minimum, encrypt your identity credential stores with a Hash+Salt.
"Data is the Goal, Applications are the Targets, and Identities are the Exploit Path"	Ensure access to high value datasets is properly controlled at both a user and system communication level.
	Implement a robust application vulnerability detection and remediation process within your software development life cycle.
"Getting Pwnd through XSS Moved from Possible to Likely, so Stop Treating It as Medium Risk"	Train your developers in secure coding, at least annually.
	Implement hack-a-thon days with your development staff once a quarter to tackle vulnerability remediation.
"Brute-Force, Schmoot-Force! User = Admin, Password = Password?"	Enforce strong password requirements.
	Enforce password reset upon initial login.
"Properly Managing Vulnerabilities is a Pipe Dream if You Try to Do It Alone"	Implement a bug bounty program and/or wall of fame.
	Implement a WAF to automate vulnerability patching and bridge the gap between detection and remediation.

“Hackers Go Phishing in an Overstocked Pond with Fake C-Level Emails”	Train your entire staff on phishing—regularly. There’s no such thing as too much awareness.
	Implement MFA to ensure compromised credentials don’t result in a breach of your network.
“Hackers Keep Their Exploits Private Using Your Encryption”	Implement decryption devices to provide visibility back to your security monitoring systems.
	Implement an effective web filtering solution to prevent infected machines from phoning home to malware sites.

From the newest malware variants to zero-day exploits and attack trends, F5Labs.com is where you’ll find the latest insights from F5’s threat research and intelligence team.

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447

Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com