Proofpoint Threat Intelligence Solutions for the Federal Government

Products

- Proofpoint Emerging Threats Intelligence
- ET Pro Ruleset
- Proofpoint Threat Intelligence Services
- Proofpoint Takedown

Key Benefits

- APIs, IDS/IPS rule sets, highly curated and high-confidence threat feeds, takedown services to protect your brand
- US analyst support
- US-based analysis for government customers
- Supports CMMC Level 2 and 3 requirements
- Supports four Zero Trust Pillars for DoD and CISA standards

Government agencies are under constant attack. These assaults can come from a wide array of adversaries. And though they may take many different forms, more than 90% of them begin with a single vector—email. The email vector serves as the initial link, at the far left of the attack chain. Unfortunately, it also represents one of the biggest intelligence gaps, or blind spots, for the US Department of Defense (DoD), the intelligence community and other federal agencies.

Proofpoint can help. This solution brief describes the Proofpoint threat intelligence stack of offerings for federal agencies. Our solution set provides focused and relevant threat intelligence on email and network visibility. It delivers focused recommendations to mitigate threats. And it helps you turn threat intelligence into a strategic tool you can use to cultivate well-trained users, establish thoughtful security architectures and implement robust intelligence plans. With our help, you can come to see email not just as a communication tool with security issues, but as a primary source of early threat intelligence that can help you get ahead of emerging threats.

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.

One of the most important services at our organization defending against initial compromise.

— Intelligence community customer

Emerging Threats Intelligence

Proofpoint Emerging Threats Intelligence is the most timely and accurate source of threat security intelligence. It helps you with threat discovery, security enforcement and incident response as well as enriches other solutions. It combines actionable information, such as up-to-the-minute IP and domain reputation feeds, with a database of globally observed threats and malware analysis.

Emerging Threats Intelligence is the gold standard for threat researchers. It offers 100% verified threat intelligence from one of the world's largest malware exchanges. It integrates seamlessly with your security tools. And it helps you understand the deeper, historical context of the origins and authors of threats. Unlike other intelligence sources that report only domains or IP addresses, our intel includes a 10-year history and proof of conviction. It covers more than 40 threat categories and related IPs, domains and samples as well as historical CVE exploitation and malware activity observed on our worldwide sensor network.

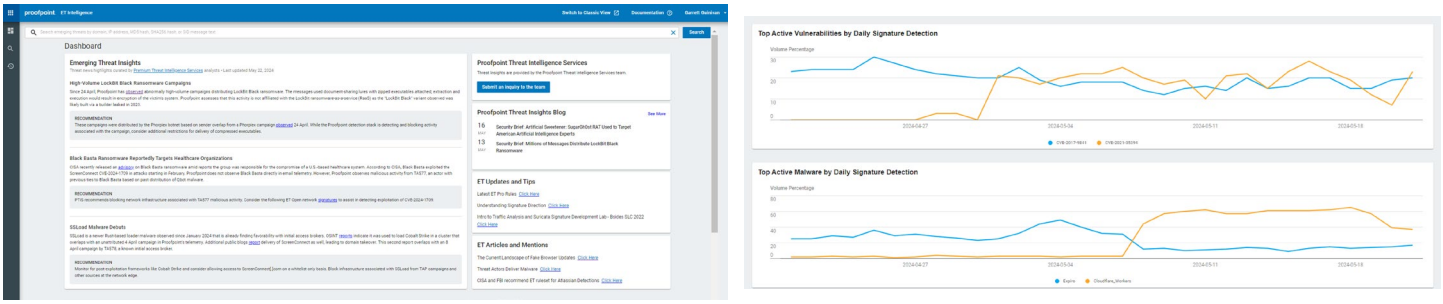

Figure 1: Emerging threats dashboard snapshots allow all users to know what the top threats are in the landscape.

Emerging Threats Pro Ruleset

Proofpoint Emerging Threats Pro Ruleset is a timely and accurate rule set that detects and blocks threats using your existing network security appliances. Examples of these appliances may include next-generation firewalls, network intrusion detection systems (IDS) and intrusion prevention systems (IPS). Emerging Threats Pro Ruleset is updated daily. And it is available in SNORT and Suricata formats. It covers more than 40 different categories of network behaviors, malware command and control, denial of service (DoS) attacks, botnets, informational events, exploits, vulnerabilities, SCADA network protocols and exploit kit activity.

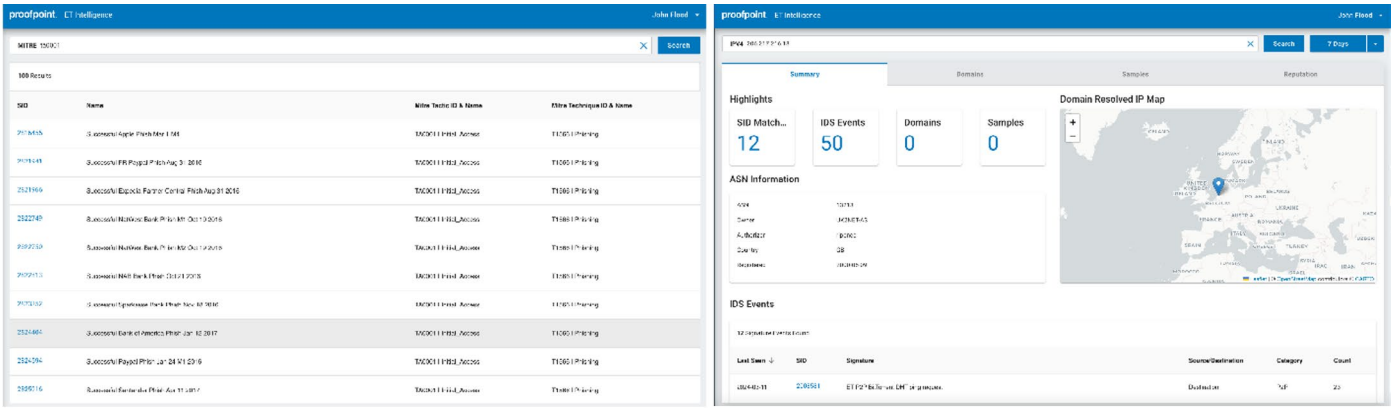

Figure 2: ET Intelligence portal snapshots showcasing a major ET rule with accompanying rules, impacts, MITRE techniques and further intelligence around the alert.

Proofpoint threat intel meetings give the teams a chance to get together internally, communicate amongst each other and focus together on security.

— Member at civilian agency

Proofpoint Threat Intelligence Services

Proofpoint Threat Intelligence Services provide deep situational understanding of the threat landscape and your organization's place in it. This can help you better prioritize your security decisions. Threat Intelligence Services offer:

- Direct access to our industry-leading US threat researchers for RFIs
- Monthly custom threat reports
- Advanced warning for emerging threats through access to our analyst logbooks
- Deep dive and landscape reporting finished intelligence through a searchable portal
- Monthly briefings from a dedicated threat analyst

The services can help you retain hard-to-find security analyst staff by reducing the number of manual processes and allowing them to focus on the most critical issues. Our researchers have more than a combined 100 years of experience within federal agencies like the NSA, the US Cyber Command and service branches.

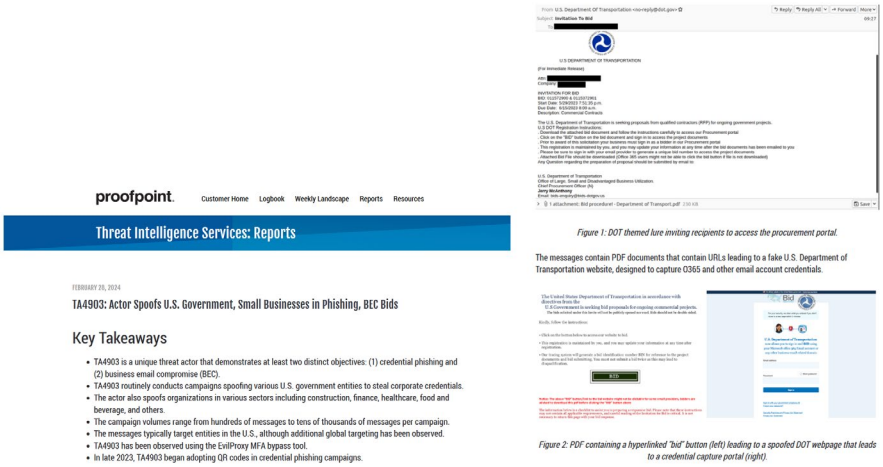

Figure 3: Threat intelligence portal snapshots of TA4903, an actor that spoofs US government customers.

Proofpoint Takedown

With Proofpoint Takedown, you get a dedicated team of analysts to help manage takedowns of malicious sites that target your company or customers. The service involves threat investigation and a double-action mitigation process that comprises both blocklist and a takedown actions.

Customers submit sites to the Takedown team for investigation and review. The team's analysts then investigate that site and pull pieces of evidence to make a case for a mitigation action on your behalf. Once malicious activity is confirmed and evidence requirements are met, the Takedown team immediately blocklists the site throughout all Proofpoint traffic and automates the blocklist reporting to our partner providers. These blocklist partners block malicious sites on different levels, including web, DNS and email. This action typically takes effect within 24 to 48 hours. This provides rapid protection while the Takedown team assists further with the takedown action.

In the takedown action, the team's analysts contact providers attached to the domain, provide the evidence and request mitigation steps to protect your company and internet users. These providers typically include the registrar, hosting provider, top-level domain (TLD) provider and more. A successful takedown can include suspension of the domain and the responsible user, removal of the domain registration or removal of various content or services attached to the domain.

Government Framework Support

This Proofpoint threat intelligence solution set provides the tools and staffing that help support the Cybersecurity Maturity Model Certification (CMMC) and Zero Trust frameworks for both the US Cybersecurity and Infrastructure Security Agency (CISA) and the DoD.

Cybersecurity Maturity Model Certification

This solution set supports CMMC Levels 2 and 3, focusing on the following domains:

- Situational Awareness
- Security Assessment
- Risk Management
- Risk Assessment
- Incident Response
- Awareness and Training

Zero Trust Alignment

This solution set aligns with the following Zero Trust pillars:

- DoD
  - Visibility and Analytics—Target and Advanced
- CISA
  - Applications and Workloads—Advanced
  - Networks—Advanced
  - Identity—Advanced
  - Data

LEARN MORE

For more information, visit **proofpoint.com**.